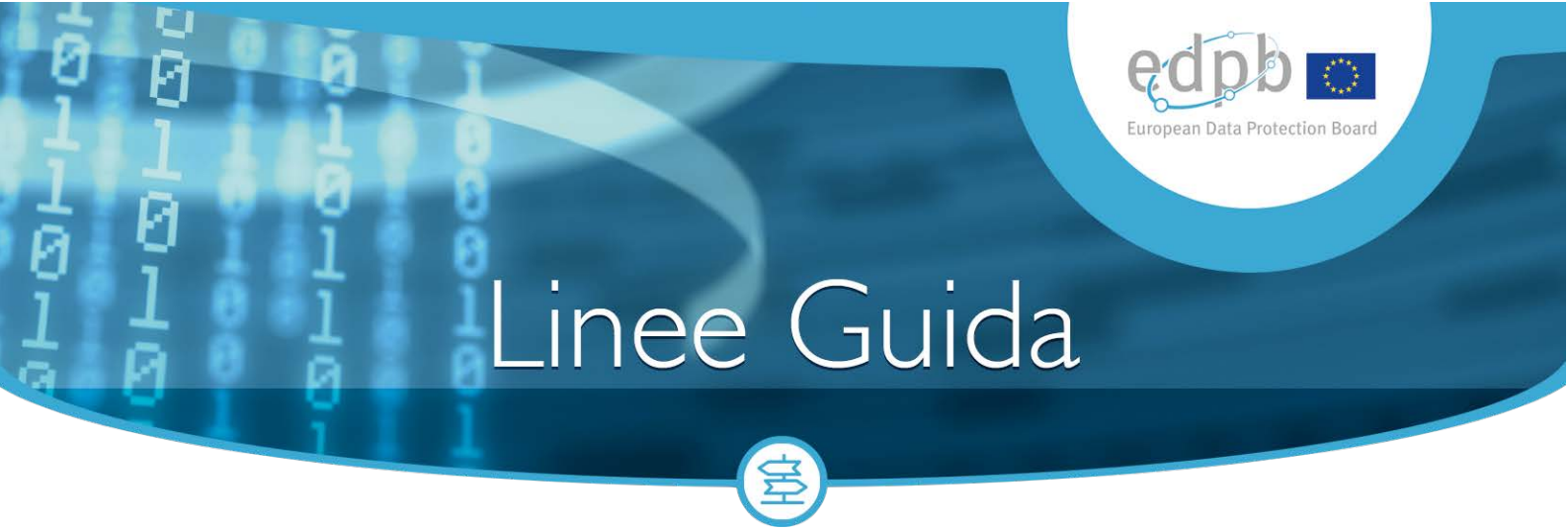

Linee-guida 04/2020 sull'uso dei dati di localizzazione e degli strumenti per il tracciamento dei contatti nel contesto dell'emergenza legata al COVID-19

Adottate il 21 aprile 2020

Cronologia delle versioni

Versione 1.1	5 maggio 2020	Piccole correzioni
Versione 1.0	21 aprile 2020	Adozione delle Linee-guida

Sommario

Il comitato europeo per la protezione dei dati

Visto l'articolo 70, paragrafo 1, lettera e), del 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 (in prosieguo "RGPD"),

Visto l'accordo SEE, in particolare l'allegato XI e il protocollo 37, modificato dalla decisione del Comitato misto SEE n. 154/2018 del 6 luglio[1] 2018,

Visti l'articolo 12 e l'articolo 22 del suo regolamento,

ADOTTA LE SEGUENTI LINEE-GUIDA:

1 INTRODUZIONE & CONTESTO

1. Governi e soggetti privati si stanno orientando verso l'uso di soluzioni basate sui dati nell'ambito della risposta alla pandemia causata dal COVID-19, e ciò suscita numerose preoccupazioni in materia di tutela della vita privata.
2. Il Comitato europeo per la protezione dei dati sottolinea che il quadro giuridico in materia di protezione dei dati è stato concepito per essere flessibile e, in quanto tale, è in grado di conseguire una risposta efficace per limitare la pandemia e proteggere i diritti umani e le libertà fondamentali.
3. Il Comitato è fermamente convinto che, ove sia necessario ricorrere al trattamento di dati personali per gestire la pandemia causata dal COVID-19, la protezione dei dati è indispensabile per generare un clima di fiducia, creare le condizioni per l'accettabilità sociale di qualsiasi soluzione e garantire, pertanto, l'efficacia di tali misure. Poiché il virus non conosce confini, appare preferibile sviluppare un approccio comune europeo in risposta alla crisi attuale, o almeno realizzare una cornice di interoperabilità.
4. Il Comitato ritiene, in via generale, che i dati e le tecnologie utilizzati per contribuire alla lotta al COVID-19 debbano servire a dare maggiori strumenti alle persone, piuttosto che a controllarle, stigmatizzarle o reprimerne i comportamenti. Inoltre, mentre i dati e le tecnologie possono essere strumenti importanti, essi hanno limiti intrinseci e non possono che far leva sull'efficacia di altre misure di sanità pubblica. I principi generali di efficacia, necessità e proporzionalità devono guidare qualsiasi misura adottata dagli Stati membri o dalle istituzioni dell'UE che comporti il trattamento di dati personali per combattere il COVID-19.
5. Le presenti linee-guida chiariscono le condizioni e i principi per l'uso proporzionato dei dati di localizzazione e degli strumenti di tracciamento dei contatti, in due ambiti specifici :
   - Utilizzo dei dati di localizzazione a supporto della risposta alla pandemia tramite la definizione di modelli della diffusione del virus, al fine di valutare l'efficacia complessiva di misure di isolamento e quarantena;
   - Utilizzo del tracciamento dei contatti per informare le persone che sono probabilmente entrate in contatto ravvicinato con soggetti successivamente confermati positivi, al fine di interrompere tempestivamente la trasmissione del contagio.
6. L'efficienza del contributo che le app per il tracciamento dei contatti possono fornire alla gestione della pandemia dipende da molti fattori (ad esempio, percentuale di persone che dovrebbero installarle; definizione di "contatto" in termini di prossimità e durata). Inoltre, tali applicazioni

1 I riferimenti agli "Stati membri" contenuti nel presente documento vanno intesi come riferimenti agli "Stati membri del SEE".

devono far parte di una strategia globale in materia di sanità pubblica per combattere la pandemia, compresi, tra l'altro, la sperimentazione e il successivo tracciamento manuale dei contatti ai fini dell'eliminazione di casi dubbi. La loro diffusione dovrebbe essere accompagnata da misure di sostegno volte a garantire che le informazioni fornite agli utenti siano contestualizzate e che le segnalazioni possano essere utili al sistema sanitario pubblico. In caso contrario, queste applicazioni potrebbero non esplicare appieno la propria efficacia.

7. Il Comitato sottolinea che il regolamento generale sulla protezione dei dati (RGPD) e la direttiva 2002/58/CE (la "direttiva relativa alla vita privata e alle comunicazioni elettroniche", direttiva e-privacy) contengono norme specifiche che consentono l'uso di dati anonimi o personali per sostenere le autorità pubbliche e altri soggetti, a livello nazionale e dell'UE, nel monitoraggio e nel contenimento della diffusione del virus SAR-CoV-2[2].

8. A tale riguardo, il Comitato si è già pronunciato sul fatto che il ricorso alle app per il tracciamento dei contatti dovrebbe essere volontario e non dovrebbe basarsi sulla tracciabilità dei movimenti individuali, bensì sulle informazioni di prossimità relative agli utenti.[3]

2 UTILIZZO DEI DATI RELATIVI ALL'UBICAZIONE

2.1 Fonti dei dati relativi all'ubicazione

9. Per la modellizzazione della diffusione del virus e dell'efficacia complessiva delle misure di confinamento, esistono due principali fonti di dati relativi all'ubicazione:
   - dati relativi all'ubicazione raccolti da fornitori di servizi di comunicazione elettronica (come gli operatori di telecomunicazioni mobili) nel corso della prestazione del loro servizio; e
   - dati relativi all'ubicazione raccolti da fornitori di servizi della società dell'informazione, la cui funzionalità richiede l'uso di tali dati (ad esempio, navigazione, servizi di trasporto, ecc.).

10. Il Comitato ricorda che i dati relativi all'ubicazione[4] raccolti dai fornitori di comunicazioni elettroniche possono essere trattati solo entro i limiti di cui agli articoli 6 e 9 della direttiva relativa alla vita privata e alle comunicazioni elettroniche. Ciò significa che tali dati possono essere trasmessi alle autorità o a terzi solo se sono stati resi anonimi dal fornitore oppure, per i dati indicanti la posizione geografica dell'apparecchiatura terminale di un utente, che non sono dati relativi al traffico, con il consenso previo degli utenti[5].

11. Per quanto riguarda le informazioni, compresi i dati relativi all'ubicazione, raccolte direttamente dall'apparecchiatura terminale, si applica l'articolo 5 (3) della direttiva relativa alla vita privata e alle comunicazioni elettroniche. Pertanto, l'archiviazione di informazioni sul dispositivo dell'utente o l'accesso alle informazioni già archiviate sono consentiti solo se i) l'utente ha prestato il consenso[6] o ii) la memorizzazione e/o l'accesso sono strettamente necessari al servizio della società dell'informazione esplicitamente richiesto dall'utente.

12. Sono tuttavia possibili, a norma dell'articolo 15 della direttiva relativa alla vita privata e alle comunicazioni elettroniche, deroghe ai diritti e agli obblighi previsti quando tali deroghe costituiscono una misura necessaria, adeguata e proporzionata all'interno di una società democratica per determinati obiettivi[7].

13. Per quanto riguarda il riutilizzo dei dati di localizzazione raccolti da un fornitore di servizi della società dell'informazione a fini di modellizzazione (ad esempio attraverso il sistema operativo o alcune applicazioni precedentemente installate), devono essere soddisfatte ulteriori condizioni. In effetti,

---

[2] Si veda la precedente dichiarazione del Comitato europeo per la protezione dei dati sul focolaio di COVID-19.
3 https://edpb.europa.eu/sites/edpb/files/files/file1/edpbletterecadvisecodiv-appguidance fines.pdf
[4] Cfr. articolo 2, lettera c), della direttiva relativa alla vita privata e alle comunicazioni elettroniche.
[5] Cfr. articoli 6 e 9 della direttiva relativa alla vita privata e alle comunicazioni elettroniche.
[6] La nozione di consenso nella direttiva relativa alla vita privata e alle comunicazioni elettroniche coincide con quella di cui al RGPD e deve soddisfare tutti i requisiti previsti dal consenso di cui all'articolo 4 (11) e all'articolo 7 del RGPD.
[7] Per l'interpretazione dell'articolo 15 della direttiva e-privacy, cfr. anche la sentenza della Corte di giustizia dell'Unione europea del 29 gennaio 2008 nella causa C-275/06, Productores de Musica de España (Promusicae) c. Telefonica de Espana SAU.

quando i dati sono stati raccolti in conformità all'articolo 5 (3) della direttiva relativa alla vita privata e alle comunicazioni elettroniche, essi possono essere trattati ulteriormente solo con il consenso supplementare dell'interessato o sulla base di una normativa dell'Unione o di uno Stato membro che costituisce una misura necessaria e proporzionata, in una società democratica, per salvaguardare gli obiettivi di cui all'articolo 23 (1) del RGPD.[8]

2.2 Utilizzo di dati anonimizzati relativi all'ubicazione

14. Il Comitato sottolinea che, per quanto riguarda l'utilizzo dei dati relativi all'ubicazione, occorre sempre privilegiare il trattamento di dati anonimi piuttosto che di dati personali.

15. L'anonimizzazione fa riferimento all'uso di una serie di tecniche finalizzate a eliminare la possibilità di collegare i dati a una persona fisica identificata o identificabile con uno sforzo "ragionevole". Questo "test di ragionevolezza" deve tenere conto sia degli aspetti oggettivi (tempi, mezzi tecnici) sia di elementi di contesto che possono variare caso per caso (rarità di un fenomeno alla luce, per esempio, della densità di popolazione, la natura e il volume dei dati). Se i dati non superano tale test, non sono anonimizzati e pertanto rientrano nel campo di applicazione del regolamento generale sulla protezione dei dati.

16. La valutazione della robustezza della tecnica di anonimizzazione adottata dipende da tre fattori: (i) individuabilità (*singling out*) (possibilità di isolare una persona all'interno di un gruppo sulla base dei dati); (ii) correlabilità (possibilità di correlare due record riguardanti la stessa persona); (iii) inferenza (possibilità di dedurre, con probabilità significativa, informazioni sconosciute relative a una persona).

17. Il concetto di anonimizzazione tende ad essere frainteso e spesso confuso con la pseudonimizzazione. Mentre l'anonimizzazione consente di utilizzare i dati senza restrizioni, i dati pseudonimizzati rientrano nel campo di applicazione del regolamento generale sulla protezione dei dati.

18. Esistono molte opzioni per conseguire un'anonimizzazione efficace[9], ma con un *caveat*. I dati non possono essere resi anonimi isolatamente, il che significa che solo intere serie o interi insiemi di dati sono passibili di anonimizzazione. In tal senso, qualsiasi intervento su un dato isolato o sulla serie storica di dati riferibili a un singolo interessato (mediante cifratura o altre trasformazioni matematiche) può essere considerato, nel migliore dei casi, una pseudonimizzazione.

19. I processi di anonimizzazione e i tentativi di re-identificazione sono oggetto di numerosi studi e ricerche. È fondamentale che ogni titolare che implementi soluzioni di anonimizzazione si mantenga aggiornato sugli sviluppi recenti in questo campo, in particolare per quanto riguarda i dati relativi all'ubicazione (provenienti da operatori delle telecomunicazioni e/o da servizi della società dell'informazione) che sono notoriamente difficili da anonimizzare.

20. In effetti, un ampio corpus di ricerche ha dimostrato[10] che *dati relativi all'ubicazione ritenuti anonimi* possono di fatto non esserlo. Le tracce di mobilità dei singoli individui sono caratterizzate intrinsecamente da forte correlazione e univocità. Pertanto, in determinate circostanze possono essere vulnerabili ai tentativi di re-identificazione.

21. Un'unica serie di dati che consenta di rintracciare l'ubicazione di un individuo lungo un arco di tempo significativo non può essere pienamente anonimizzata. Questa affermazione resta valida se non si riduce in misura sufficiente la precisione delle coordinate geografiche registrate, o se non si eliminano dettagli del percorso di tracciamento, e anche se si mantiene solo l'ubicazione dei luoghi in cui l'interessato permane per un tempo considerevole. E vale anche in caso di insufficiente aggregazione dei dati relativi all'ubicazione.

22. Al fine di conseguire l'anonimizzazione, i dati relativi all'ubicazione devono essere trattati con attenzione per soddisfare il test di ragionevolezza. In tal senso, il trattamento deve prendere in

---

[8] Si veda la sezione 1.5.3 delle Linee-guida 1/2020 sul trattamento dei dati personali nel contesto dei veicoli connessi.
[9] (de Montjoye et al., 2018) "On the privacy-conscientious use of mobile phone data".
[10] (de Montjoye et al., 2013) "Unique in the Crowd: The privacy bounds of human mobility" e (Pyrgelis et al., 2017) "Knock Knock, Who's There? Membership Inference on Aggregate Location Data".

considerazione gli insiemi di dati di ubicazione nel loro complesso, e riguardare dati di una serie ragionevolmente ampia di individui utilizzando tecniche di anonimizzazione disponibili e con caratteristiche robuste, implementandole in modo adeguato ed efficace.

23. Infine, data la complessità dei processi di anonimizzazione, si raccomanda con forza di garantire la trasparenza per quanto riguarda la metodologia di anonimizzazione utilizzata.

3 APP PER IL TRACCIAMENTO DEI CONTATTI

3.1 Analisi giuridica generale

24. Il monitoraggio sistematico e su larga scala dell'ubicazione e/o dei contatti tra persone fisiche costituisce una grave interferenza nella vita privata. Essa può essere legittimata solo facendo affidamento su un'adozione volontaria da parte degli utenti per ciascuno dei rispettivi scopi. Ciò implica, in particolare, che le persone che non intendono o non possono utilizzare tali applicazioni non dovrebbero subire alcun pregiudizio.

25. Per garantire il rispetto del principio di responsabilizzazione, dovrebbe essere definita chiaramente la titolarità del trattamento di un'eventuale app per il tracciamento di contatti. Il Comitato ritiene che le autorità sanitarie nazionali possano essere i titolari di tale trattamento[11]; si possono comunque prendere in considerazione altre configurazioni di titolarità. In ogni caso, se il processo di diffusione delle app per il tracciamento dei contatti coinvolge diversi attori, devono essere definiti con chiarezza e fin dall'inizio i ruoli e le responsabilità rispettive e di tutto ciò devono essere informati gli utenti.

26. Inoltre, per quanto riguarda il principio della limitazione delle finalità, le finalità devono essere sufficientemente specifiche così da escludere trattamenti ulteriori per scopi non correlati alla gestione della crisi sanitaria causata da COVID-19 (ad esempio, per fini commerciali o per le attività di contrasto di matrice giudiziaria o di polizia). Una volta definita con chiarezza la finalità, sarà necessario garantire che l'uso dei dati personali sia adeguato, necessario e proporzionato.

27. Nel contesto di un'app per il tracciamento dei contatti, occorre prestare particolare attenzione al principio di minimizzazione e ai principi della protezione dei dati fin dalla progettazione e per impostazione predefinita (*data protection by design and by default*):
    - le app per il tracciamento dei contatti non necessitano del tracciamento della posizione dei singoli utenti. Occorre invece utilizzare i dati di prossimità;
    - poiché le app per il tracciamento dei contatti possono funzionare senza l'identificazione diretta delle persone, dovrebbero essere adottate misure adeguate per prevenire la reidentificazione;
    - le informazioni raccolte dovrebbero risiedere nell'apparecchiatura terminale dell'utente e dovrebbero essere raccolte solo le informazioni pertinenti e solo ove strettamente necessarie.

28. Per quanto riguarda la liceità del trattamento, il Comitato rileva che le app per il tracciamento dei contatti comportano la memorizzazione e/o l'accesso a informazioni già archiviate nell'apparecchiatura terminale dell'utente, che sono soggette all'articolo 5 (3) della direttiva ePrivacy. Se tali operazioni sono strettamente necessarie per consentire al fornitore dell'app di rendere il servizio esplicitamente richiesto dall'utente, il trattamento non richiede il consenso di quest'ultimo. Per le operazioni che non sono strettamente necessarie, il fornitore dovrebbe richiedere il consenso dell'utente.

29. Inoltre, il Comitato osserva come la circostanza per cui l'uso di app per il tracciamento dei contatti avvenga su base volontaria non implichi che il trattamento dei dati personali debba necessariamente basarsi sul consenso. Qualora autorità pubbliche forniscano un servizio sulla base di un mandato conferito dalla legge e conformemente ai requisiti stabiliti da tale legge, la base

[11] Vedi anche la comunicazione della Commissione "Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection" (Orientamenti sulle app per le azioni di sostegno alla lotta alla pandemia da COVID-19 in relazione alla protezione dei dati), Bruxelles, 16.4.2020, C (2020) 2523 final.

giuridica più pertinente risulta essere la necessità del trattamento per lo svolgimento di un compito di interesse pubblico, ossia l'articolo 6, paragrafo 1, lettera e), del Regolamento generale sulla protezione dei dati.

30. L'articolo 6, paragrafo 3, del Regolamento precisa che la base su cui si fonda il trattamento di cui all'articolo 6, paragrafo 1, lettera e) è stabilita dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare. La finalità del trattamento è definita in tale base giuridica o, per quanto riguarda il trattamento di cui al paragrafo 1, lettera e), è necessaria per l'esecuzione di un compito svolto nel pubblico interesse o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.[12]

31. Tuttavia, la base giuridica o la misura legislativa che costituisce il fondamento di liceità per l'uso dell'app di tracciamento dei contatti dovrebbero prevedere garanzie significative, compreso un riferimento alla natura volontaria dell'app. Dovrebbe essere inclusa una chiara specificazione delle finalità e delle limitazioni riguardanti l'ulteriore utilizzo dei dati personali, nonché una chiara identificazione del titolare o dei titolari coinvolti. Occorre inoltre individuare le categorie di dati e i soggetti ai quali i dati personali possono essere comunicati, e per quali scopi. A seconda del grado di interferenza, occorre integrare salvaguardie ulteriori tenendo conto della natura, della portata e delle finalità del trattamento. Infine, il Comitato raccomanda di prevedere, non appena possibile, i criteri per stabilire quando l'app dovrà essere disinstallata e a chi spetti assumere tale determinazione.

32. Tuttavia, se il trattamento dei dati si basa su una diversa base giuridica, quale[13] ad esempio il consenso (articolo 6 (1) (a)), il titolare dovrà garantire che siano soddisfatti i requisiti rigorosi previsti per tale base giuridica.

33. Inoltre, il ricorso a un'app per combattere la pandemia da COVID-19 potrebbe portare alla raccolta di dati relativi alla salute (ad esempio lo status di persona infetta). Il trattamento di tali dati è consentito quando è necessario per motivi di interesse pubblico nel settore della sanità pubblica, nel rispetto delle condizioni di cui all'articolo 9, paragrafo 2, lettera i), del Regolamento[14], o per le finalità dell'assistenza sanitaria di cui all'articolo 9, paragrafo 2, lettera h), del Regolamento stesso[15]. A seconda della base giuridica individuata, il trattamento in questione potrebbe anche fondarsi sul consenso esplicito dell'interessato (articolo 9, paragrafo (2), lettera a), del Regolamento).

34. Conformemente allo scopo iniziale, l'articolo 9, paragrafo 2, lettera j), del Regolamento consente inoltre che i dati relativi alla salute siano trattati ove necessario a fini di ricerca scientifica o a fini statistici.

35. L'attuale crisi sanitaria non dovrebbe trasformarsi in un'occasione per derogare rispetto al principio di limitazione della conservazione dei dati. La conservazione dovrebbe essere limitata alla luce delle reali esigenze e della rilevanza medica (anche con riguardo a considerazioni di natura epidemiologica quali il periodo di incubazione, ecc.) e i dati personali dovrebbero essere conservati solo per la durata della crisi dovuta al COVID-19. Successivamente, di norma, tutti i dati personali dovrebbero essere cancellati o resi anonimi.

36. Il Comitato ritiene che tali app non possano sostituire, ma solo supportare, il tracciamento manuale dei contatti effettuato da personale sanitario pubblico qualificato, che potrà stabilire con quale probabilità contatti ravvicinati diano luogo a una trasmissione del virus o meno (ad esempio, in caso di interazioni con una persona protetta da un adeguato equipaggiamento, come può avvenire ad esempio per un addetto alla cassa di un supermercato ecc.). Il Comitato sottolinea che tutte le procedure e i processi, compresi gli algoritmi implementati dalle app per il tracciamento dei contatti, dovrebbero svolgersi sotto la stretta sorveglianza di personale qualificato al fine di limitare il verificarsi di falsi positivi e negativi. In particolare, le indicazioni fornite in merito ai passi da

[12] Vedi Considerando (41).

[13] I titolari del trattamento (in particolare le autorità pubbliche) devono prestare particolare attenzione al fatto che il consenso non dovrebbe essere considerato liberamente espresso se la persona non ha l'effettiva possibilità di rifiutare o di revocare il proprio consenso senza subire pregiudizio.

[14] Il trattamento deve basarsi sul diritto dell'Unione o degli Stati membri che preveda misure appropriate e specifiche per tutelare i diritti e le libertà della persona interessata, in particolare il segreto professionale.

[15] Si veda l'articolo 9, paragrafo 2, lettera h), del Regolamento generale sulla protezione dei dati.

compiere successivamente alla ricezione di un alert non dovrebbero basarsi unicamente su un trattamento automatizzato.

37. Al fine di garantire la correttezza dei trattamenti, il rispetto del principio di responsabilizzazione e, più in generale, la conformità con la legge, gli algoritmi devono essere verificabili e devono essere soggetti a un riesame periodico da parte di esperti indipendenti. Il codice sorgente dovrebbe essere reso pubblico così da assicurare la più ampia trasparenza possibile.

38. Vi sarà sempre, in una certa misura, la possibilità del verificarsi di falsi positivi. Poiché l'identificazione di un rischio di infezione può avere un forte impatto sui singoli individui, ad esempio imponendo l'autoisolamento fino a negativizzazione del test, è indispensabile poter effettuare correzioni dei dati e/o dei risultati delle analisi successive. Naturalmente ciò vale solo in presenza di situazioni o implementazioni in cui il trattamento e la conservazione dei dati sono configurati in modo da permettere tecnicamente di apportare le correzioni suddette, e ove sia probabile il verificarsi degli effetti negativi di cui sopra.

39. Infine, il Comitato ritiene che debba essere effettuata una valutazione d'impatto sulla protezione dei dati prima di implementare le app in questione, in quanto il trattamento configura una probabilità di rischio elevato (dati relativi alla salute, adozione prevista su larga scala, monitoraggio sistematico, uso di una nuova soluzione tecnologica)[16]. Il Comitato raccomanda vivamente la pubblicazione degli esiti di tali valutazioni.

3.2 Raccomandazioni e requisiti funzionali

40. Conformemente al principio di minimizzazione, tra le altre misure in ossequio al principio di protezione dei dati fin dalla progettazione e per impostazione predefinita[17], i dati trattati dovrebbero essere limitati a quelli strettamente necessari. L'app non dovrebbe raccogliere informazioni non correlate o non necessarie come, per esempio, dati anagrafici, identificativi di comunicazione, voci di directory del dispositivo, messaggi, registrazioni di chiamate, dati relativi all'ubicazione, identificativi del dispositivo, ecc. .

41. I dati trasmessi dall'app devono includere solo identificatori univoci e pseudonimi, generati dall'app e specifici di tale app. Tali identificatori devono essere rinnovati regolarmente, secondo una frequenza compatibile con lo scopo di contenere la diffusione del virus e sufficiente a limitare il rischio di identificazione e di localizzazione fisica delle persone.

42. Le applicazioni per il tracciamento dei contatti possono seguire un approccio centralizzato o decentrato[18]. Entrambe le opzioni sono praticabili, a condizione che siano in vigore adeguate misure di sicurezza, ed entrambe comportano una serie di vantaggi e svantaggi. Pertanto, la fase di progettazione delle app dovrebbe sempre prevedere un esame approfondito di entrambi gli approcci, ponderandone attentamente gli effetti in termini di protezione dei dati e privacy nonché i possibili impatti sui diritti delle persone.

43. Ogni server coinvolto nel sistema di tracciamento dei contatti deve raccogliere soltanto la cronologia dei contatti o gli identificativi pseudonimizzati di un utente diagnosticato come infetto a seguito di un'adeguata valutazione effettuata dalle autorità sanitarie e di un'azione volontaria dell'utente stesso. Alternativamente, il server deve conservare un elenco degli identificativi pseudonimizzati di utenti infetti o la rispettiva cronologia dei contatti solo per il periodo necessario a informare gli utenti potenzialmente infetti della loro avvenuta esposizione, senza tentare di individuare tali utenti potenzialmente infetti.

44. La realizzazione di una complessiva strategia di tracciamento dei contatti comprendente sia l'impiego di app sia il tracciamento manuale può richiedere, in alcuni casi, il trattamento di ulteriori

---

[16] Si vedano le Linee-Guida del WP29 (fatte proprie dal Comitato europeo per la protezione dei dati) sulla valutazione d'impatto sulla protezione dei dati e sulla circostanza per cui il trattamento "possa comportare un rischio elevato" ai fini del regolamento (UE) n. 2016/679.

[17] Si vedano le Linee-guida del comitato europeo per la protezione dei dati 4/2019 sulla protezione dei dati fin dalla fase di progettazione e per impostazione predefinita.

[18] In via generale, la soluzione decentrata è maggiormente conforme al principio di minimizzazione.

informazioni. In questo caso, tali informazioni supplementari dovrebbero rimanere nel dispositivo dell'utente e saranno trattate solo ove strettamente necessario e con il previo e specifico consenso dell'utente stesso.

45. Si deve fare ricorso a tecniche crittografiche di ultima generazione per garantire la conservazione sicura dei dati memorizzati nei server e nelle app, nonché gli scambi tra le app e il server remoto. Occorre inoltre implementare sistemi di autenticazione reciproca tra l'app e il server.

46. La segnalazione nell'app di utenti infetti da SARS-CoV-2 deve essere soggetta a idonea procedura, ad esempio mediante l'impiego di un codice monouso correlato a una identità pseudonima della persona infetta e collegato a un laboratorio o a un operatore sanitario. Se la conferma non può essere ottenuta in modo sicuro, non dovrebbe aversi alcun trattamento di dati sulla base di una presunzione di validità dello status relativo all'utente.

47. Il titolare del trattamento, in collaborazione con le autorità pubbliche, deve fornire informazioni chiare e inequivocabili sul link ove scaricare l'app ufficiale per il tracciamento dei contatti al fine di ridurre il rischio che gli utenti utilizzino un'app di terze parti.

4 CONCLUSIONE

48. Il mondo si trova ad affrontare una grave crisi sanitaria che richiede risposte forti, il cui impatto si manifesterà anche oltre il termine di questa emergenza. Il trattamento automatizzato dei dati e le tecnologie digitali possono essere elementi chiave nella lotta al COVID-19. Tuttavia, occorre guardarsi dal rischio di effetti irreversibili. Spetta a noi tutti garantire che ogni misura adottata in queste circostanze eccezionali sia necessaria, limitata nel tempo, di portata minima e soggetta a un riesame periodico ed effettivo nonché a una valutazione scientifica.

49. Il Comitato europeo per la protezione dei dati sottolinea che a nessuno dovrebbe essere chiesto di scegliere tra una risposta efficace all'attuale crisi e la tutela dei diritti fondamentali: entrambi gli obiettivi sono alla nostra portata, e i principi di protezione dei dati possono svolgere un ruolo molto importante nella lotta contro il virus. Il diritto europeo in materia di protezione dei dati consente l'uso responsabile dei dati personali per la gestione della salute, garantendo al contempo che non siano erosi i diritti e le libertà individuali.

Per il Comitato europeo per la

protezione dei dati

La Presidente

Andrea Jelinek

ALLEGATO --- APPLICAZIONI PER IL TRACCIAMENTO DEI CONTATTI GUIDA ALL'ANALISI

0. Avvertenza

I seguenti orientamenti non sono né prescrittivi né esaustivi e intendono unicamente fornire indicazioni generali per sviluppatori e realizzatori di app di tracciamento dei contatti. Soluzioni diverse da quelle qui descritte sono ammesse e lecite purché conformi al pertinente quadro giuridico (il Regolamento generale sulla protezione dei dati e la Direttiva e-privacy).

Si osservi, inoltre, che la presente guida ha natura generale. Di conseguenza, le raccomandazioni e gli obblighi contenuti nel presente documento non devono essere considerati esaustivi. Le valutazioni devono essere effettuate caso per caso; inoltre, determinate app possono richiedere misure supplementari non comprese nelle indicazioni qui fornite.

1. Sintesi

In molti Stati membri si valuta il ricorso ad applicazioni (app) di *tracciamento dei contatti* per facilitare l'individuazione di eventuali contatti con una persona affetta da SARS-Cov-2.

Non sono ancora definite le condizioni alle quali tali app contribuirebbero efficacemente alla gestione della pandemia, e tale definizione dovrebbe costituire un presupposto necessario per l'implementazione di un'app del tipo descritto. Tuttavia, è opportuno fornire linee-guida che, in via preliminare, diano indicazioni pertinenti ai team di sviluppatori in modo da assicurare la protezione dei dati personali fin dalla fase iniziale di progettazione.

Si osservi, inoltre, che la presente guida ha natura generale. Di conseguenza, le raccomandazioni e gli obblighi contenuti nel presente documento non devono essere considerati esaustivi. Le valutazioni devono essere effettuate caso per caso; inoltre, determinate app possono richiedere misure supplementari non comprese nelle indicazioni qui elaborate. Scopo della presente guida è fornire orientamenti generali per sviluppatori e realizzatori di app di tracciamento dei contatti.

Alcuni criteri potrebbero andare al di là dei requisiti strettamente derivanti dal quadro normativo in materia di protezione dei dati. Tali criteri mirano a garantire il massimo livello di trasparenza al fine di favorire l'accettazione sociale delle app di tracciamento dei contatti.

A tal fine, i soggetti che rilasciano sul mercato app di tracciamento dei contatti dovrebbero tener conto dei seguenti criteri:

- L'uso dell'app deve essere rigorosamente volontario e non può costituire condizione per l'esercizio dei diritti previsti dalla legge. Le persone devono avere il pieno controllo dei propri dati in ogni momento e devono poter scegliere liberamente se utilizzare l'app o meno.
- Le app di tracciamento dei contatti possono comportare un rischio elevato per i diritti e le libertà delle persone fisiche e, quindi, è necessaria una valutazione d'impatto sulla protezione dei dati prima della loro introduzione.
- È possibile ottenere informazioni sulla prossimità tra utenti dell'app senza geolocalizzarli. Questo tipo di app non necessita di dati relativi all'ubicazione e, pertanto, non deve comportarne l'utilizzo.

- A seguito della diagnosi di infezione da SARS-Cov-2 concernente un utente, dovrebbero essere informate solo le persone con le quali l'utente è stato in stretto contatto durante il periodo epidemiologicamente rilevante ai fini del tracciamento dei contatti.
- Il funzionamento di questo tipo di applicazioni potrebbe richiedere, a seconda dell'architettura prescelta, l'utilizzo di un server centralizzato. In tal caso, conformemente ai principi della minimizzazione dei dati e della protezione dei dati fin dalla progettazione, i dati trattati dal server centralizzato dovrebbero limitarsi al minimo necessario:
    - Quando a un utente viene diagnosticata l'infezione, d'accordo con l'utente possono essere raccolte le informazioni relative ai precedenti contatti ravvicinati o gli identificativi trasmessi dall'app. Occorre stabilire un metodo di verifica che consenta di certificare che la persona è realmente infetta senza identificare l'utente. Tecnicamente ciò sarebbe possibile allertando i contatti solo dopo l'intervento di un operatore sanitario, ad esempio utilizzando un codice speciale monouso.
    - Le informazioni memorizzate nel server centrale non dovrebbero consentire al titolare del trattamento di identificare gli utenti con diagnosi di infezione né i soggetti che sono venuti in contatto con tali utenti, e neppure dovrebbero consentire di effettuare inferenze sulla rete di contatti se non per ciò che è necessario ai fini della determinazione dei contatti pertinenti.
- Il funzionamento di un'app di questo tipo richiede la trasmissione di dati che sono letti e ascoltati dai dispositivi di altri utenti:
    - È sufficiente lo scambio di identificativi pseudonimizzati tra i dispositivi mobili degli utenti (computer, tablet, orologi connessi, ecc.), ad esempio mediante loro trasmissione attraverso il Bluetooth a bassa energia.
    - Gli identificativi devono essere generati utilizzando i processi più avanzati di crittografia.
    - Gli identificativi devono essere rinnovati regolarmente per ridurre il rischio di tracciamento fisico e di attacchi diretti.
- Questo tipo di applicazione deve essere protetto in modo da garantire la sicurezza dei processi tecnici di elaborazione. In particolare:
    - L'app non dovrebbe fornire agli utenti informazioni che consentano loro di desumere l'identità o la diagnosi di soggetti terzi. Il server centrale non deve né identificare gli utenti né effettuare inferenze nei loro riguardi.

Avvertenza: I principi di cui sopra si riferiscono all'obiettivo dichiarato delle *app di tracciamento dei contatti*, e unicamente a tale obiettivo, ossia fornire in modo automatico informazioni ai soggetti potenzialmente esposti al virus (senza necessità di identificarli). I gestori delle app e delle relative infrastrutture sono soggetti alle verifiche delle competenti autorità di controllo. L'osservanza della totalità o di parte di questi orientamenti non è sufficiente di per sé a garantire la piena conformità al quadro normativo in materia di protezione dei dati.

2. Definizioni

Contatto	Con riguardo a una app di tracciamento dei contatti, un contatto è un utente che ha partecipato a un'interazione con un altro utente di cui è confermato lo stato di positività al virus, per un periodo e a una distanza tali da comportare un rischio di esposizione significativa all'infezione. I parametri relativi alla durata dell'esposizione e alla distanza interpersonale devono essere definiti dalle autorità sanitarie e possono essere configurati nella app.
Dati relativi all'ubicazione	Qualsiasi dato trattato in una rete di comunicazione elettronica o da un servizio di comunicazione elettronica che indichi la posizione geografica dell'apparecchiatura terminale di un utente di un servizio di comunicazione elettronica accessibile al pubblico (quale definito nella direttiva e-privacy), nonché i dati provenienti da altre fonti potenziali relativi a: • latitudine, longitudine o altitudine dell'apparecchiatura terminale; • la direzione di marcia dell'utente; o • l'ora in cui sono state registrate le informazioni relative all'ubicazione.
Interazione	Nel contesto di un'app di tracciamento dei contatti, per interazione si intende lo scambio di informazioni tra due dispositivi situati in prossimità reciproca (nello spazio e nel tempo), all'interno del range proprio della tecnologia di comunicazione utilizzata (ad esempio Bluetooth). Questa definizione esclude l'ubicazione dei due utenti partecipanti all'interazione.
Vettore del virus	In questo documento sono considerati vettori del virus gli utenti che sono risultati positivi al virus e che hanno ricevuto una diagnosi ufficiale da medici o centri sanitari.
Tracciamento dei contatti	Chi si è trovato a stretto contatto (secondo i criteri epidemiologici) con persone infette dal virus corre un rischio significativo di essere infetto e di infettare a sua volta altre persone. Il tracciamento dei contatti è una metodologia di controllo delle patologie che prevede la creazione di un elenco di tutte le persone che si sono trovate nelle immediate vicinanze di un vettore del virus, in modo da verificare se siano a rischio di infezione e adottare nei loro confronti misure sanitarie adeguate.

3. Indicazioni generali

GEN-1	L'app deve essere uno strumento complementare alle tecniche convenzionali di tracciamento dei contatti (in particolare la raccolta dell'anamnesi di persone infette), ossia deve far parte di un programma di sanità pubblica più ampio. Deve essere utilizzata solo fino a quando le tecniche di tracciamento manuale dei contatti non consentiranno in modo autonomo di gestire il numero delle nuove infezioni.

GEN-2	Occorre prevedere una procedura per interrompere la raccolta degli identificativi (disattivazione generale dell'app, istruzioni per la disinstallazione dell'app, disinstallazione automatica, ecc.) e per la cancellazione di tutti i dati raccolti da tutte le banche dati (applicazioni mobili e server), da attivare al più tardi quando le autorità pubbliche competenti avranno stabilito che la situazione si è «normalizzata ».
GEN-3	Il codice sorgente dell'app e del suo *back-end* deve essere pubblicamente disponibile e le specifiche tecniche devono essere rese pubbliche, in modo che le parti interessate possano verificare il codice e, se del caso, contribuire a migliorarlo correggendo eventuali *bug* e garantendo la trasparenza nel trattamento dei dati personali.
GEN-4	Il processo di implementazione dell'app deve consentire di validarne progressivamente l'efficacia in termini di salute pubblica. A tal fine occorre definire previamente un protocollo di valutazione che specifichi gli indicatori utili a misurare l'efficacia dell'app.

4. Finalità

PUR-1	L'app deve mirare unicamente al tracciamento dei contatti, in modo da avvertire e prendere in carico i soggetti potenzialmente esposti al SARS-CoV-2. Non deve essere utilizzata per altre finalità.
PUR-2	L'utilizzo dell'app non deve derogare dalla sua finalità primaria allo scopo di controllare la conformità alle misure di quarantena o di confinamento e/o di distanziamento sociale.
PUR-3	L'app non deve essere utilizzata per trarre conclusioni sull'ubicazione degli utenti in base alla loro interazione e/o ad altri elementi.

5. Considerazioni funzionali

FUNC-1	L'app deve fornire una funzionalità che consenta agli utenti di essere informati di una loro potenziale esposizione al virus; tale informazione deve basarsi sulla prossimità a un utente infetto verificatasi entro un periodo di X giorni prima del test di screening positivo (dove il valore X è definito dalle autorità sanitarie).
FUNC-2	L'app dovrebbe fornire indicazioni agli utenti identificati come potenzialmente esposti al virus. Dovrebbe trasmettere istruzioni sulle misure da adottare e consentire all'utente di chiedere un consulto. In tal caso sarebbe obbligatorio un intervento umano.
FUNC-3	L'algoritmo che misura il rischio di infezione alla luce dei fattori distanza e tempo, e che quindi stabilisce quando inserire un contatto nell'elenco di tracciamento dei contatti, deve essere regolabile in modo sicuro per tener conto delle conoscenze più recenti sulla diffusione del virus.
FUNC-4	**Gli utenti devono essere informati di essere stati esposti al virus,** o devono ricevere periodicamente informazioni indicanti se siano stati esposti o meno al virus, durante il periodo di incubazione del virus stesso.

FUNC-5	L’app dovrebbe essere interoperabile con altre applicazioni sviluppate negli Stati membri per fornire un’informazione efficace agli utenti che si spostano in più Stati membri.

6. Dati

DATA-1	L’app deve essere in grado di trasmettere e ricevere dati attraverso tecnologie di comunicazione di prossimità quali il Bluetooth a bassa energia in modo da poter effettuare il tracciamento dei contatti.
DATA-2	I dati trasmessi devono comprendere identificativi pseudo-casuali, con chiave di cifratura forte, generati dall’app e specifici per quest’ultima.
DATA-3	Il rischio di collisione tra gli identificativi pseudo-casuali dovrebbe essere sufficientemente basso.
DATA-4	Gli identificativi pseudo-casuali devono essere rinnovati regolarmente, con una frequenza sufficiente a limitare il rischio di reidentificazione, tracciamento fisico o collegamento tra individui da parte di qualsiasi soggetto, compresi il gestore del server centrale, altri utilizzatori dell’app o terzi malintenzionati. Questi identificativi devono essere generati dall’app, eventualmente sulla base di un seme (*seed*) fornito dal server centrale.
DATA-5	In conformità al principio della minimizzazione dei dati, l’app non deve raccogliere dati diversi da quelli strettamente necessari ai fini del tracciamento dei contatti
DATA-6	L’app non deve raccogliere dati relativi all'ubicazione ai fini del tracciamento dei contatti. I dati relativi all'ubicazione possono essere trattati al solo scopo di consentire l'interazione con applicazioni simili in altri paesi e dovrebbero limitarsi a quelli strettamente necessari, in termini di precisione, per tale unico scopo.
DATA-7	L’app non dovrebbe raccogliere dati relativi alla salute ulteriori rispetto a quelli strettamente necessari ai fini dell'app stessa, tranne che su base facoltativa e al solo scopo di supportare il processo decisionale mirato all’informazione dell'utente.
DATA-8	Gli utenti devono essere informati di tutti i dati personali che saranno raccolti. Tali dati dovrebbero essere raccolti solo previa autorizzazione dell'utente.

7. Caratteristiche tecniche

TECH-1	L’app dovrebbe utilizzare le tecnologie disponibili per individuare utenti in prossimità del dispositivo che abbiano installato l’applicazione, ad esempio tecnologie di comunicazione di prossimità (come il Bluetooth a bassa energia).
TECH-2	L’app dovrebbe conservare lo storico dei contatti di un utente all’interno del dispositivo, per un periodo limitato e predefinito.
TECH-3	L’app può utilizzare un server centralizzato per implementare alcune funzionalità.

TECH-4	L’architettura dell’app deve sfruttare per quanto possibile i dispositivi degli utenti.
TECH-5	La trasmissione al server centrale dello storico dei contatti o degli identificativi degli utenti dovrebbe avvenire su iniziativa degli utenti stessi che risultino infetti e previa conferma di tale status da parte di un professionista sanitario abilitato.

8. Sicurezza

SEC-1	Occorre verificare lo status degli utenti segnalati nell’app come positivi al SARS-CoV-2, ad esempio fornendo un codice monouso legato a un laboratorio o a un operatore sanitario. Se non è possibile ottenere conferma in modo sicuro, i dati non devono essere trattati.
SEC-2	I dati inviati al server centrale devono essere trasmessi attraverso un canale sicuro. Dovrebbe essere attentamente valutato il ricorso ai servizi di notifica messi a disposizione dai fornitori di piattaforme OS, che non dovrebbero comportare la divulgazione di dati a terzi.
SEC-3	Le richieste non devono essere vulnerabili rispetto a manipolazioni da parte di utenti malintenzionati.
SEC-4	Devono essere implementate le tecniche più avanzate di crittografia per garantire la sicurezza degli scambi tra l'applicazione e il server e tra le singole applicazioni, nonché, in via generale, per proteggere le informazioni memorizzate nell’app e sul server. Tra gli esempi di tecniche utilizzabili figurano la cifratura simmetrica e asimmetrica, funzioni di *hash*, protocolli PMT (*private membership test*), protocolli PSI (*private set intersection*), filtri di Bloom, *private information retrieval*, cifratura omomorfica, ecc.
SEC-5	Il server centrale non deve conservare gli identificativi di connessione alla rete (ad es. indirizzi IP) degli utenti, compresi quelli che hanno ricevuto una diagnosi positiva e che hanno trasmesso la cronologia dei contatti o i propri identificativi.
SEC-6	Al fine di evitare sostituzioni di persona o la creazione di utenze inesistenti (*fake*), il server deve autenticare l’app.
SEC-7	L’app deve autenticare il server centrale.
SEC-8	Le funzionalità dei server dovrebbero essere protette da attacchi di replay.
SEC-9	Per autenticarne origine e integrità, le informazioni trasmesse dal server centrale devono essere firmate.
SEC-10	L'accesso ai dati conservati nel server centrale e non accessibili al pubblico deve essere limitato esclusivamente alle persone autorizzate.
SEC-11	Il *permission manager* del dispositivo a livello di sistema operativo deve chiedere esclusivamente le autorizzazioni necessarie per accedere a e utilizzare i moduli di comunicazione, ove necessario, per conservare i dati nel terminale e per scambiare informazioni con il server centrale.

9. Protezione dei dati personali e della privacy delle persone fisiche

Nota: le indicazioni fornite di seguito riguardano un’app il cui unico scopo è il tracciamento dei contatti.

PRIV-1	Gli scambi di dati devono rispettare la privacy degli utenti (in particolare garantire il rispetto del principio di minimizzazione).
PRIV-2	L'app non deve consentire l'identificazione diretta degli utenti.
PRIV-3	L'app non deve consentire il tracciamento degli spostamenti degli utenti.
PRIV-4	L'utilizzo dell'app non dovrebbe consentire agli utenti di acquisire informazioni su altri utenti (in particolare se siano vettori del virus o meno).
PRIV-5	Il margine di fiducia riservato al server centrale deve essere limitato. La gestione del server centrale deve seguire regole di governance chiaramente definite e comprendere tutte le misure necessarie per garantirne la sicurezza. La localizzazione del server centrale dovrebbe consentire una vigilanza efficace da parte dell'autorità di controllo competente.
PRIV-6	Deve essere effettuata una valutazione d'impatto sulla protezione dei dati le cui risultanze dovrebbero essere rese pubbliche.
PRIV-7	L'app dovrebbe informare l'utente solo dell'esposizione al virus e, se possibile, senza rivelare informazioni su altri utenti, del numero e delle date dei relativi eventi.
PRIV-8	Le informazioni trasmesse dall'app non devono consentire agli utenti di identificare gli utenti vettori del virus né i loro spostamenti.
PRIV-9	Le informazioni trasmesse dall'app non devono consentire alle autorità sanitarie di individuare utenti potenzialmente esposti senza il loro previo accordo.
PRIV-10	Le richieste inviate dall'app al server centrale non devono rivelare alcuna informazione sul vettore del virus.
PRIV-11	Le richieste inviate dall'app al server centrale non devono rivelare informazioni superflue sull'utente, con la sola eccezione, ove necessario, degli identificativi pseudonimizzati e dell'elenco dei contatti.
PRIV-12	Non devono essere possibili attacchi di *linkage*.
PRIV-13	Gli utenti devono essere in grado di esercitare i propri diritti attraverso l'app.
PRIV-14	La cancellazione dell'app deve comportare la cancellazione di tutti i dati raccolti localmente.
PRIV-15	L'app dovrebbe raccogliere esclusivamente dati trasmessi da altre istanze dell'app stessa, ovvero da altre app interoperabili di analoga natura. Non devono essere raccolti dati relativi ad altre applicazioni e/o dispositivi di comunicazione di prossimità.
PRIV-16	Al fine di evitare la re-identificazione da parte del server centrale, dovrebbero essere utilizzati server proxy. Attraverso questi *server indipendenti* è possibile combinare gli identificativi di più utenti (sia appartenenti a vettori del virus sia inviati da altri richiedenti) prima di condividerli con il server centrale, in modo da impedire a quest'ultimo di conoscere gli identificativi (ad esempio gli indirizzi IP) specifici dei singoli utenti.
PRIV-17	Sviluppo e configurazione di app e server devono essere condotti con la massima cura al fine di evitare la raccolta di dati non necessari (ad esempio, nei log del server non dovrebbero essere inclusi identificativi, ecc.) nonché per impedire il ricorso a pacchetti di sviluppo software di terzi che raccolgano dati per altri fini.

La maggior parte delle app di tracciamento dei contatti allo studio prevede sostanzialmente due approcci qualora un utente risulti infetto: possono inviare al server la cronologia dei contatti di prossimità ottenuti mediante scansione, oppure inviare l'elenco dei propri identificativi già trasmessi. I principi ricordati di seguito sono declinati in base a questi due approcci. Tuttavia, ciò non significa che non siano possibili o addirittura preferibili altri approcci, basati per esempio sull'implementazione di forme di cifratura *end-to-end* (E2E) o sull'utilizzo di altre tecnologie di sicurezza o di potenziamento della privacy.

9.1. Principi che si applicano solo **se l'app invia al server un elenco di contatti:**

CON-1	Il server centrale deve raccogliere la cronologia dei contatti degli utenti che siano stati certificati positivi al SARS-CoV-2 soltanto quale effetto di una scelta volontaria della persona dichiarata infetta.
CON-2	Il server centrale non deve conservare né distribuire un elenco degli identificativi pseudonimizzati degli utenti che siano vettori del virus.
CON-3	La cronologia dei contatti memorizzati sul server centrale deve essere cancellata una volta che gli utenti abbiano ricevuto notifica della loro prossimità a una persona risultata positiva.
CON-4	Nessun dato deve lasciare il dispositivo dell'utente se non qualora un utente risultato positivo condivida la cronologia dei contatti con il server centrale ovvero qualora un utente presenti al server una richiesta di informazioni sulla sua esposizione potenziale al virus.
CON-5	Qualsiasi identificativo presente nella cronologia conservata in locale deve essere cancellato dopo X giorni dalla raccolta (il valore X è definito dalle autorità sanitarie).
CON-6	Le cronologie dei contatti inviate da utenti distinti non dovrebbero essere oggetto di trattamenti ulteriori, ad esempio mediante correlazioni incrociate miranti a realizzare mappe globali di prossimità.
CON-7	I dati nei log di server devono essere ridotti al minimo e soddisfare i requisiti in materia di protezione dei dati

9.2. Principi che si applicano solo se l'app invia al server un elenco dei propri identificativi:

ID-1	Il server centrale deve raccogliere gli identificativi trasmessi dall'app di utenti di cui sia stata accertata la positività al SARS-CoV-2, a seguito di un intervento volontario da parte di tali utenti.
ID-2	Il server centrale non deve conservare né diffondere la cronologia dei contatti di utenti che siano vettori del virus.
ID-3	Gli identificativi memorizzati nel server centrale devono essere cancellati una volta distribuiti alle altre applicazioni.
ID-4	Eccettuati i casi in cui l'utente risultato positivo condivida i propri identificativi con il server centrale, ovvero qualora un utente chieda al server informazioni sulla sua potenziale esposizione al virus, nessun dato deve lasciare il device dell'utente.

ID-5	I dati nei log di server devono essere ridotti al minimo e soddisfare i requisiti in materia di protezione dei dati.