II

(Comunicazioni)

COMUNICAZIONI PROVENIENTI DALLE ISTITUZIONI, DAGLI ORGANI E DAGLI ORGANISMI DELL'UNIONE EUROPEA

COMMISSIONE EUROPEA

COMUNICAZIONE DELLA COMMISSIONE

Orientamenti sulle app a sostegno della lotta alla pandemia di covid-19 relativamente alla protezione dei dati

(2020/C 124 I/01)

1 CONTESTO

La pandemia di Covid-19 rappresenta una sfida senza precedenti per l'Unione e per gli Stati membri, i loro sistemi di assistenza sanitaria, il loro stile di vita, la loro stabilità economica e i loro valori. Le tecnologie e i dati digitali rivestono un ruolo importante nel contrasto alla crisi Covid-19. Le applicazioni mobili di solito installate su smartphone (app) possono aiutare le autorità sanitarie, a livello nazionale e dell'UE, a monitorare e contenere l'attuale pandemia di Covid-19 e sono particolarmente importanti in fase di revoca delle misure di contenimento. Possono infatti fornire indicazioni dirette ai cittadini e sostenere lo sforzo di tracciamento dei contatti. In una serie di paesi, nell'UE e nel resto del mondo, le autorità nazionali o regionali ovvero gli sviluppatori hanno annunciato il lancio di app con funzionalità diverse finalizzate a sostenere la lotta contro il virus.

L'8 aprile 2020 la Commissione ha adottato una raccomandazione relativa a un pacchetto di strumenti comuni dell'Unione per l'uso della tecnologia e dei dati al fine di contrastare la crisi Covid-19 e uscirne, in particolare per quanto riguarda le applicazioni mobili e l'uso di dati anonimizzati sulla mobilità (la "raccomandazione") ([1]). La raccomandazione ha lo scopo, tra l'altro, di sviluppare un approccio europeo comune ("pacchetto di strumenti") per l'uso delle applicazioni mobili, coordinato a livello dell'UE, per consentire ai cittadini di adottare efficaci misure di distanziamento sociale e per scopi di allerta, prevenzione e tracciamento dei contatti al fine di contribuire a limitare la propagazione della Covid-19. La raccomandazione stabilisce i principi generali cui dovrebbe essere improntato lo sviluppo di tale pacchetto di strumenti e annuncia che la Commissione pubblicherà ulteriori orientamenti, anche sui risvolti dell'uso delle applicazioni in questo campo in riferimento ai dati personali e alla vita privata.

Con la tabella di marcia comune europea verso la revoca delle misure di contenimento della Covid-19, la Commissione, in cooperazione con il presidente del Consiglio europeo, ha stabilito una serie di principi guida per la graduale revoca delle misure di contenimento della pandemia di Covid-19. Le applicazioni mobili, comprese le funzionalità di tracciamento dei contatti, possono svolgere un ruolo importante in questo contesto. In funzione delle caratteristiche delle app e di quanto la popolazione le usa, possono avere un impatto significativo sulla diagnosi, sul trattamento e sulla gestione della Covid-19 in ambiente ospedaliero e all'esterno. Sono particolarmente importanti in fase di revoca delle misure di contenimento e quando il rischio di infezione cresce man mano che aumentano i contatti tra le persone. Queste applicazioni possono contribuire a interrompere le catene di infezione più rapidamente e in modo più efficiente delle misure generali di contenimento e possono ridurre il rischio di diffusione significativa del virus. Dovrebbero quindi essere un elemento importante della strategia di uscita, complementare ad altre misure quali l'aumento delle capacità di eseguire test ([2]). Conditio sine qua non per lo sviluppo, l'accettazione e l'utilizzo di tali app da parte delle persone è la fiducia. I cittadini devono essere certi che è garantito il rispetto dei diritti fondamentali e che le app verranno utilizzate solo per finalità specificamente definite, che non saranno utilizzate per la sorveglianza di massa e che le persone continueranno ad avere il controllo dei propri dati. Su questo presupposto si fondano la precisione e l'efficacia di tali app nel contenere la diffusione

([1]) Raccomandazione C(2020) 2296 final dell'8 aprile 2020 https://ec.europa.eu/info/sites/info/files/recommendation_on_apps_for_contact_tracing_4.pdf.

([2]) https://ec.europa.eu/info/sites/info/files/communication_-_a_european_roadmap_to_lifting_coronavirus_containment_measures_0.pdf

del virus. È quindi essenziale individuare soluzioni che siano le meno intrusive possibile e pienamente conformi ai requisiti stabiliti dal diritto dell'UE in materia di riservatezza e protezione dei dati personali. Inoltre le applicazioni dovrebbero essere disattivate al più tardi quando la pandemia sarà dichiarata sotto controllo. Le applicazioni dovranno anche contenere le più avanzate protezioni della sicurezza delle informazioni.

I presenti orientamenti tengono conto del contributo del comitato europeo per la protezione dei dati (EDPB) ([3]) e del dibattito nell'ambito della rete di assistenza sanitaria online (e-Health). L'EDPB prevede di pubblicare nei prossimi giorni linee guida in materia di geolocalizzazione e altri strumenti di localizzazione nel contesto della pandemia di Covid-19.

Ambito degli orientamenti

Per garantire un approccio coerente in tutta l'UE e fornire indicazioni agli Stati membri e agli sviluppatori di app, il presente documento stabilisce le caratteristiche e i requisiti cui le app devono rispondere per garantire il rispetto della legislazione dell'UE in materia di protezione dei dati personali e della vita privata, in particolare del regolamento generale sulla protezione dei dati ([4]) (GDPR) e della direttiva e-privacy ([5]). I presenti orientamenti non trattano ulteriori condizioni, restrizioni comprese, che gli Stati membri potrebbero aver inserito nelle rispettive legislazioni nazionali in relazione al trattamento dei dati relativi alla salute.

Gli orientamenti non sono giuridicamente vincolanti e non pregiudicano il ruolo della Corte di giustizia dell'UE, l'unica istituzione che può dare l'interpretazione autentica del diritto dell'UE.

I presenti orientamenti trattano solo le app facoltative a sostegno della lotta alla pandemia di Covid-19 (app scaricate, installate e utilizzate su base volontaria dalle persone) con una o più delle seguenti funzionalità:

— dare informazioni precise alle persone sulla pandemia di Covid-19;

— offrire alle persone questionari di autovalutazione e di orientamento (funzionalità di controllo dei sintomi) ([6]);

— allertare le persone che si sono trovate per un certo tempo in prossimità di una persona infetta, per dare informazioni ad esempio sull'opportunità di mettersi in auto-quarantena e su dove sottoporsi ai test (funzionalità di tracciamento dei contatti e allerta);

— offrire un canale di comunicazione tra pazienti e medici nelle situazioni di auto-isolamento o per effettuare ulteriori diagnosi e dare consulenza sui trattamenti (maggiore ricorso alla telemedicina).

A norma della direttiva e-privacy l'uso di un'app che va a toccare i diritti alla riservatezza delle comunicazioni di cui all'articolo 5 è possibile solo mediante una legge che sia necessaria, opportuna e proporzionata al fine di conseguire determinati obiettivi specifici. Date l'elevata invasività di siffatto approccio e le sfide che comporta, anche in termini di messa in atto di idonee salvaguardie, la Commissione ritiene che prima di ricorrere a questa opzione sia necessario effettuare un'attenta analisi. Per i motivi suesposti, la Commissione raccomanda l'utilizzo di app facoltative.

I presenti orientamenti non riguardano le app finalizzate a far rispettare le prescrizioni in materia di quarantena (compresi quelle obbligatorie).

2 CONTRIBUTO DELLE APP ALLA LOTTA CONTRO LA COVID-19

La funzionalità di controllo dei sintomi è uno strumento che consente alle autorità sanitarie pubbliche di dare indicazioni ai cittadini sui test diagnostici della Covid-19 e informazioni sull'auto-isolamento, su come evitare di trasmettere la malattia e su quando è necessario rivolgersi a un medico. Può inoltre integrare la sorveglianza sanitaria di base e dare migliori informazioni sui tassi di trasmissione della Covid-19 nella popolazione.

([3]) https://edpb.europa.eu/sites/edpb/files/files/file1/edpbletterecadvisecodiv-appguidance_final.pdf

([4]) 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), GU L 119 del 4.5.2016, pag. 1.

([5]) 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), GU L 201 del 31.7.2002, pag. 37.

([6]) Se le app forniscono informazioni relative a diagnosi, prevenzione, monitoraggio, previsione o prognosi, è opportuno valutarne la potenziale qualifica come dispositivi medici conformemente al quadro normativo sui dispositivi medici. Per quanto concerne detto quadro, si veda la direttiva 93/42/CEE del Consiglio, del 14 giugno 1993, concernente i dispositivi medici (GU L 169 del 12.7.1993, pag. 1) e il regolamento (UE) 2017/745 del Parlamento europeo e del Consiglio, del 5 aprile 2017, relativo ai dispositivi medici (GU L 117 del 5.5.2017, pag. 1).

Le funzionalità di tracciamento dei contatti e di allerta sono strumenti che consentono alle autorità sanitarie pubbliche di individuare le persone entrate in contatto con una persona infettata dalla Covid-19 e di informarle sugli opportuni passi successivi, ad esempio l'auto-quarantena o i test, oppure di consigliare loro come comportarsi se insorgono sintomi. Si tratta quindi di una funzionalità utile sia ai singoli cittadini che alle autorità sanitarie pubbliche. Può inoltre svolgere un ruolo importante nella gestione delle misure di contenimento durante gli scenari di mitigazione. Il suo impatto può essere rafforzato da una strategia a sostegno di un maggior numero di test per le persone che presentano sintomi lievi.

Entrambe le funzionalità possono altresì essere una fonte di dati rilevante per le autorità sanitarie pubbliche e facilitare la trasmissione di tali dati alle autorità epidemiologiche nazionali e al Centro europeo per la prevenzione e il controllo delle malattie (ECDC). Questo aiuterebbe a comprendere i modelli di trasmissione e, in combinazione con i risultati dei test, a stimare il valore predittivo positivo dei sintomi respiratori in una determinata comunità nonché a dare informazioni sul livello di circolazione del virus.

Il grado di affidabilità delle stime dipende direttamente dalla quantità e dall'attendibilità dei dati trasmessi.

Pertanto, in combinazione con adeguate strategie di test, le funzionalità di controllo dei sintomi e di tracciamento dei contatti possono entrambe fornire informazioni sul livello di circolazione del virus e aiutare a valutare l'impatto delle misure di distanziamento fisico e di confinamento. Come indicato nella raccomandazione, per consentire la collaborazione transfrontaliera e assicurare il rilevamento dei contatti tra gli utenti di app diverse (aspetto particolarmente importante negli spostamenti transfrontalieri dei cittadini) deve essere garantita l'interoperabilità tra le soluzioni informatiche dei vari Stati membri. Laddove una persona infetta entra in contatto con un utente di un'app di un altro Stato membro, la trasmissione transfrontaliera dei dati personali di tale utente alle autorità sanitarie del suo Stato membro deve essere possibile per quanto strettamente necessario. La questione verrà affrontata nell'ambito del pacchetto di strumenti annunciato dalla raccomandazione. L'interoperabilità dovrà essere garantita sia mediante requisiti tecnici sia migliorando la comunicazione e la cooperazione tra autorità sanitarie nazionali. Un modello di cooperazione particolare ([7]) potrebbe essere utilizzato anche come modello di governance per le app di tracciamento dei contatti durante la pandemia di Covid-19.

3 ELEMENTI PER UN USO FIDUCIARIO E RESPONSABILIZZATO DELLE APP

Le funzionalità contenute nelle app possono incidere in misura diversa su un'ampia gamma di diritti sanciti dalla Carta dei diritti fondamentali dell'UE: dignità umana, rispetto della vita privata e familiare, protezione dei dati di carattere personale, libertà di circolazione, non discriminazione, libertà d'impresa, libertà di riunione e di associazione. L'interferenza con la vita privata e il diritto alla protezione dei dati di carattere personale può essere particolarmente significativa dato che alcune delle funzionalità si basano su un modello ad elevata intensità di dati.

Gli elementi presentati di seguito mirano a fornire orientamenti su come limitare l'intrusività delle funzionalità delle app per garantire il rispetto della legislazione dell'UE in materia di protezione dei dati personali e della vita privata.

3.1 Le autorità sanitarie nazionali (o i soggetti che svolgono compiti nel pubblico interesse nel campo della salute) come titolari del trattamento

L'identificazione di chi determina i mezzi e le finalità del trattamento dei dati (il titolare del trattamento) è fondamentale per stabilire chi è responsabile del rispetto delle norme dell'UE in materia di protezione dei dati personali, e in particolare: chi deve dare informazioni alle persone che scaricano l'app su come verranno usati i loro dati personali (preesistenti o che verranno generati tramite il dispositivo, ad esempio uno smartphone, sul quale è installata l'app), su quali saranno i loro diritti, su chi sarà chiamato a rispondere in caso di violazione dei dati, ecc.

Data la sensibilità dei dati personali in questione e la finalità del trattamento dei dati descritta di seguito, la Commissione ritiene che le app debbano essere progettate in modo tale che i titolari del trattamento siano le autorità sanitarie nazionali (o i soggetti che svolgono un compito nel pubblico interesse nel campo della salute) ([8]). I titolari del trattamento sono responsabili del rispetto del GDPR (principio di responsabilizzazione). Tale accesso dovrebbe essere delimitato sulla base dei principi descritti nella sezione 3.5 in appresso.

([7]) Siffatta cooperazione avviene già nell'ambito del progetto MyHealth@EU per lo scambio dei profili sanitari sintetici dei pazienti e delle prescrizioni elettroniche. Cfr. anche l'articolo 5, paragrafo 5, e il considerando 17 della decisione di esecuzione 2019/1765 della Commissione.

([8]) Cfr. considerando 45 del GDPR.

Questo contribuirà anche ad aumentare la fiducia dell'opinione pubblica e quindi l'accettazione delle app (e dei sistemi di informazione sulle catene di trasmissione delle infezioni che ne sono alla base) e garantirà che queste soddisfino la finalità perseguita della tutela della salute pubblica. Le politiche, le prescrizioni e i controlli soggiacenti dovrebbero essere allineati e attuati in modo coordinato dalle competenti autorità sanitarie nazionali.

3.2 **Garantire che la persona mantenga il controllo**

Un fattore determinante per la fiducia delle persone nelle app è la dimostrazione che esse mantengono il controllo dei propri dati personali. Per garantire questo, la Commissione ritiene che debbano essere soddisfatte in particolare le seguenti condizioni:

— l'installazione dell'app sul dispositivo dovrebbe avvenire su base volontaria e senza conseguenze negative per la persona che decide di non scaricare/utilizzare l'app;

— le diverse funzionalità dell'app (ad esempio, informazioni, controllo dei sintomi, tracciamento dei contatti e allerta) non dovrebbero essere raggruppate, in modo da consentire alla persona di dare separatamente il proprio consenso a ciascuna funzionalità. Ciò non dovrebbe impedire all'utente di combinare diverse funzionalità dell'app, se il fornitore offre questa opzione;

— se si usano dati di prossimità (dati generati dallo scambio di segnali Bluetooth a bassa energia (BLE) tra dispositivi a una distanza epidemiologicamente significativa e durante il periodo epidemiologicamente rilevante), questi devono essere conservati sul dispositivo della persona. Se tali dati devono essere condivisi con le autorità sanitarie, essi dovrebbero essere condivisi solo dopo la conferma che la persona interessata è infettata dalla Covid-19 e a condizione che essa scelga di farlo;

— le autorità sanitarie dovrebbero fornire alle persone tutte le informazioni necessarie relative al trattamento dei propri dati personali (conformemente agli articoli 12 e 13 del GDPR e all'articolo 5 della direttiva e-privacy);

— la persona dovrebbe essere in grado di esercitare i diritti previsti dal GDPR (in particolare, accesso, rettifica e cancellazione). Qualsiasi limitazione dei diritti previsti dal GDPR e dalla direttiva e-privacy dovrebbe essere conforme a tali atti e necessaria, proporzionata e prevista dalla normativa;

— le app dovrebbero essere disattivate al più tardi quando la pandemia sarà dichiarata sotto controllo. La disattivazione non dovrebbe dipendere dalla disinstallazione da parte dell'utente.

3.3 **Base giuridica per il trattamento**

Installazione delle app e conservazione delle informazioni sul dispositivo dell'utente

Come osservato in precedenza, ai sensi della direttiva e-privacy (articolo 5), la conservazione di informazioni sul dispositivo dell'utente o l'accesso a informazioni già conservate sono consentiti solo solo se i) l'utente ha espresso preliminarmente il proprio consenso o ii) la conservazione e/o l'accesso sono strettamente necessari per il servizio della società dell'informazione (ad esempio l'app) esplicitamente richiesto (ad esempio, installato e attivato) da parte dell'utente.

La conservazione di informazioni sul dispositivo della persona e l'accesso alle informazioni già conservate su tale dispositivo sono normalmente necessari affinché le app funzionino. La funzionalità "tracciamento dei contatti" e "allerta" richiede inoltre la conservazione sul dispositivo dell'utente di altre informazioni (pseudonimi temporanei che cambiano periodicamente per gli utenti di questa funzionalità in prossimità). Tale funzionalità potrebbe richiedere inoltre che l'utente (infetto o potenzialmente infetto) carichi dati di prossimità. Il caricamento non è necessario per il funzionamento dell'app in quanto tale. Pertanto i criteri dell'opzione ii) di cui sopra non sono soddisfatti. Il consenso (opzione i) sopra) rimane pertanto il motivo più adeguato per le attività pertinenti. Tale consenso dovrebbe essere libero, specifico, esplicito e informato ai sensi del GDPR. Dovrebbe essere espresso mediante un'azione positiva inequivocabile della persona, il che esclude forme di consenso tacito (ad esempio, il silenzio o l'inattività) ([9]).

([9]) Cfr. le linee guida del comitato europeo per la protezione dei dati in merito al consenso: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051

Base giuridica per il trattamento da parte delle autorità sanitarie nazionali — diritto dell'Unione o nazionale

Le autorità sanitarie nazionali trattano generalmente dati personali quando esiste un obbligo legale stabilito dal diritto dell'UE o nazionale che prevede tale trattamento e nel rispetto delle condizioni di cui all'articolo 6, paragrafo 1, lettera c), e all'articolo 9, paragrafo 2, lettera i), del GDPR o quando tale trattamento è necessario per promuovere l'interesse pubblico riconosciuto dal diritto dell'UE o nazionale ([10]).

Qualsiasi normativa nazionale deve prevedere misure specifiche e adeguate per tutelare i diritti e le libertà degli interessati. In linea generale, quanto maggiore è l'impatto sulle libertà delle persone, tanto maggiori dovrebbero essere le garanzie corrispondenti previste dalla pertinente normativa.

Le norme dell'UE e degli Stati membri che esistevano prima della pandemia di Covid-19 e quelle che gli Stati membri stanno adottando per combattere specificamente la diffusione della pandemia possono, in linea di principio, essere utilizzate come base giuridica per il trattamento dei dati personali se prevedono misure che consentono il monitoraggio della pandemia e se tali norme rispettano le disposizioni dell'articolo 6, paragrafo 3, del GDPR.

Tenuto conto della natura dei dati personali in questione (in particolare dei dati relativi alla salute che costituiscono una categoria particolare di dati personali) e delle circostanze dell'attuale pandemia di Covid-19, l'utilizzo della normativa come base giuridica contribuirebbe alla certezza del diritto, in quanto i) stabilirebbe con precisione il trattamento di determinati dati relativi alla salute e specificherebbe chiaramente le finalità del trattamento; ii) indicherebbe chiaramente il titolare del trattamento, ossia l'entità incaricata del trattamento dei dati, e chi, oltre al titolare del trattamento, può avere accesso a tali dati; iii) escluderebbe la possibilità di trattare tali dati per finalità diverse da quelle elencate nella normativa e iv) prevederebbe garanzie specifiche. Al fine di non compromettere l'utilità pubblica e l'accettazione delle app, il legislatore nazionale dovrebbe prestare particolare attenzione al fatto che la soluzione scelta sia quanto più inclusiva possibile nei confronti dei cittadini.

Il trattamento da parte delle autorità sanitarie sulla base della normativa non cambia il fatto che le persone restano libere di decidere se installare o no l'app e di condividere i propri dati con le autorità sanitarie. Non dovrebbero pertanto verificarsi conseguenze negative per gli utenti quando l'app è disinstallata.

Le app di tracciamento dei contatti e di allerta consentono di avvertire le persone. Quando le persone sono avvertite direttamente dall'app, la Commissione richiama l'attenzione sul divieto di sottoporre le persone a una decisione basata unicamente sul trattamento automatizzato che produca effetti giuridici che le riguardano o che incida in modo analogo significativamente sulla loro persona (articolo 22 del GDPR).

3.4 **Minimizzazione dei dati**

I dati prodotti per mezzo di dispositivi e già precedentemente conservati su tali dispositivi sono protetti come segue:

— in quanto "dati personali", ossia qualsiasi informazione riguardante una persona fisica identificata o identificabile (articolo 4, paragrafo 1, del GDPR), sono protetti a norma del GDPR. I dati relativi alla salute beneficiano di una protezione aggiuntiva (articolo 9 del GDPR);

— in quanto "dati relativi all'ubicazione", ossia dati trattati in una rete di comunicazione elettronica o da un servizio di comunicazione elettronica che indichi la posizione geografica dell'apparecchiatura terminale dell'utente, sono protetti a norma della direttiva e-privacy (articolo 5, paragrafo 1, e articoli 6 e 9) ([11]);

— Tutte le informazioni conservate nell'apparecchiatura terminale dell'utente e da essa accessibili sono protette ai sensi dell'articolo 5, paragrafo 3, della direttiva e-privacy.

I dati non personali (quali i dati anonimizzati in modo irreversibile) non sono protetti ai sensi del GDPR.

La Commissione ricorda che il principio della minimizzazione dei dati prevede che solo i dati personali che sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità ([12]) possono essere trattati. Una valutazione della necessità di trattare i dati personali e della pertinenza di tali dati personali dovrebbe essere effettuata alla luce della/e finalità perseguite.

La Commissione osserva che, ad esempio, se la finalità della funzionalità è il controllo dei sintomi o la telemedicina, tali finalità non richiedono l'accesso all'elenco dei contatti della persona proprietaria del dispositivo.

([10]) Articolo 6, paragrafo 1, lettera e), del GDPR.

([11]) Il codice delle comunicazioni elettroniche prevede che siano contemplati anche i servizi che sono equivalenti, dal punto di vista funzionale, ai servizi di comunicazione elettronica.

([12]) Principio della minimizzazione dei dati

La produzione e il trattamento di una quantità minore di dati limitano i rischi per la sicurezza. Di conseguenza il rispetto di misure di minimizzazione dei dati offre anche garanzie di sicurezza.

— Funzionalità "informazioni"

Un'app che ha solo questa funzionalità non ha bisogno di trattare dati relativi alla salute delle persone ma si limita a fornire soltanto informazioni. Al fine di conseguire tale finalità, le informazioni contenute nell'apparecchiatura terminale e da essa accessibili non possono essere trattate oltre quanto necessario a fornire le informazioni.

— Funzionalità "controllo dei sintomi" e "telemedicina"

Se l'app comprende una o entrambi queste funzionalità, essa tratterà dati personali relativi alla salute. Pertanto un elenco dei dati che possono essere trattati dovrebbe essere specificato nella normativa di riferimento applicabile alle autorità sanitarie.

Le autorità sanitarie potrebbero inoltre aver bisogno dei numeri di telefono delle persone che hanno utilizzato la funzionalità "controllo dei sintomi" e che hanno caricato i risultati. Le informazioni contenute nell'apparecchiatura terminale e da essa accessibili possono essere trattate solo nella misura necessaria per consentire all'app di conseguire la propria finalità e consentirne il funzionamento.

— Funzionalità "tracciamento dei contatti" e "allerta"

La maggior parte delle infezioni da Covid-19 avviene tramite goccioline che percorrono solo su una distanza limitata. Individuare al più presto le persone che sono state in prossimità di una persona infetta è un fattore chiave per interrompere la catena di infezione. La determinazione della prossimità è una funzione della distanza e della durata del contatto e dovrebbe avvenire da un punto di vista epidemiologico. L'interruzione della catena di infezione è particolarmente importante per evitare la ricomparsa di infezioni nella fase di uscita dalla crisi.

I dati di prossimità potrebbero essere necessari a tal fine Per la misurazione della prossimità e dei contatti ravvicinati le comunicazioni basate sul Bluetooth a bassa energia (BLE) tra i dispositivi appaiono più precise e, pertanto, più appropriate dell'uso dei dati di geolocalizzazione (GNSS/GPS o dati di localizzazione cellulare). Il BLE evita la possibilità di tracciamento (a differenza dei dati di geolocalizzazione). La Commissione raccomanda pertanto l'uso di dati di comunicazione basati sul BLE (o di dati basati su una tecnologia analoga) per determinare la prossimità.

I dati relativi all'ubicazione non sono necessari ai fini delle funzionalità di tracciamento dei contatti, in quanto il loro obiettivo non è quello di seguire i movimenti delle persone o di far rispettare le prescrizioni. Inoltre il trattamento dei dati relativi all'ubicazione nel contesto del tracciamento dei contatti sarebbe difficile da giustificare alla luce del principio della minimizzazione dei dati e potrebbe creare problemi di sicurezza e di tutela della vita privata. Per questo motivo la Commissione consiglia di non utilizzare i dati relativi all'ubicazione in questo contesto.

Indipendentemente dai mezzi tecnici utilizzati per determinare la prossimità, non sembra necessario conservare l'ora del contatto o il luogo esatti (se disponibili). Potrebbe tuttavia essere utile conservare il giorno del contatto per sapere se il contatto si è verificato quando la persona ha sviluppato sintomi (o 48 ore prima ([13])) e per inviare il messaggio di follow-up raccomandando, ad esempio, la durata del periodo di quarantena.

I dati di prossimità dovrebbero essere generati e trattati solo se sussiste un rischio reale di infezione (in funzione della vicinanza e della durata del contatto).

Si noti che la necessità e la proporzionalità della raccolta di dati dipenderanno quindi da fattori quali la disponibilità di strutture di prova, in particolare quando sono già state imposte misure come il confinamento. Le persone che sono state in contatto ravvicinato con una persona infetta possono essere avvertite in due modi.

Il primo approccio prevede l'invio automatico di un'allerta attraverso l'app ai contatti ravvicinati quando un utente informa l'app – con l'approvazione o la conferma dell'autorità sanitaria, ad esempio mediante un codice QR o TAN – di essere risultato positivo al test (trattamento decentralizzato). È preferibile che il contenuto del messaggio di allerta sia definito dall'autorità sanitaria. Il secondo approccio prevede che gli identificativi temporanei generati in modo arbitrario siano conservati su un server back-end tenuto dall'autorità sanitaria (soluzione del server back-end). Gli utenti non possono essere identificati direttamente tramite questi dati. Attraverso gli identificativi gli utenti che sono stati in contatto ravvicinato con un utente risultato positivo al test ricevono una segnalazione sul loro dispositivo. Se le autorità sanitarie desiderano contattare gli utenti che sono stati in contatto ravvicinato con una persona infetta anche tramite telefono o SMS, hanno bisogno del consenso di tali utenti per fornire i numeri di telefono.

([13]) La persona infetta è contagiosa a partire da 48 ore prima del manifestarsi dei sintomi.

3.5 **Limitare la divulgazione di dati/l'accesso ai dati**

— Funzionalità "informazioni"

Nessuna informazione contenuta nell'apparecchiatura terminale e da essa accessibile può essere condivisa con le autorità sanitarie se non necessaria per ottenere la funzionalità "informazioni". Poiché questa funzionalità si limita ai mezzi di comunicazione, le autorità sanitarie non potranno accedere ad altri dati.

— Funzionalità "controllo dei sintomi" e "telemedicina"

La funzionalità "controllo dei sintomi" può essere utile per gli Stati membri per indirizzare i cittadini verso eventuali test, fornire informazioni sull'isolamento e sulle tempistiche e le modalità di accesso all'assistenza sanitaria, in particolare per i gruppi a rischio. Questa funzionalità può inoltre integrare l'assistenza sanitaria di base e aiutare a comprendere quali sono i tassi di infezione da Covid-19 nella popolazione. Si potrebbe pertanto decidere che le autorità sanitarie e le autorità epidemiologiche nazionali competenti debbano avere accesso alle informazioni fornite dal paziente. Il Centro europeo per la prevenzione e il controllo delle malattie (ECDC) potrebbe ricevere i dati aggregati dalle autorità nazionali ai fini della sorveglianza epidemiologica.

Se si decide di consentire un contatto con gli operatori sanitari piuttosto che soltanto attraverso l'app, è necessario comunicare alle autorità sanitarie nazionali il numero telefonico degli utenti dell'app.

— Funzionalità "tracciamento dei contatti" e "allerta"

— Dati delle persone infette

Le app generano identificativi pseudonimi generati arbitrariamente per i telefoni che sono in contatto con l'utente. Un'opzione consiste nel conservare gli identificativi sul dispositivo dell'utente (il cosiddetto trattamento decentralizzato). Un'altra opzione prevede che questi identificativi arbitrari siano conservati nel server al quale le autorità sanitarie hanno accesso (la cosiddetta soluzione del server back-end). La soluzione decentralizzata è più conforme al principio della minimizzazione. Le autorità sanitarie dovrebbero avere accesso soltanto ai dati di prossimità del dispositivo della persona infetta, in modo che possano contattare le persone a rischio di infezione.

Tali dati saranno a disposizione delle autorità sanitarie soltanto dopo che la persona infetta (una volta sottoposta a test) li condivide in maniera proattiva con loro.

La persona infetta non dovrebbe essere informata dell'identità delle persone con le quali ha avuto un contatto potenzialmente rilevante dal punto di vista epidemiologico e che saranno allertate.

— Dati delle persone che sono state in contatto (epidemiologico) con la persona infetta

L'identità della persona infetta non dovrebbe essere comunicata alle persone con le quali è stata in contatto epidemiologico. È sufficiente far loro sapere che sono state in contatto epidemiologico con una persona infetta nel corso degli ultimi 16 giorni. Come sopra indicato, i dati relativi all'ora e al luogo ove sono avvenuti tali contatti non dovrebbero essere conservati. Non è pertanto necessario né tantomeno possibile comunicarli.

Per poter tracciare i contatti epidemiologici di un utente app che risulta infetto, dovrebbe essere comunicato alle autorità sanitarie nazionali solo l'identificativo della persona con la quale la persona infetta è stata in contatto epidemiologico dalle 48 ore che hanno preceduto l'insorgere dei primi sintomi fino a 14 giorni dopo la comparsa dei sintomi, a seconda della vicinanza e della durata del contatto.

Le autorità nazionali potrebbero trasmettere all'ECDC dati aggregati per il tracciamento dei contatti ai fini della sorveglianza epidemiologica sulla base di indicatori definiti in collaborazione con gli Stati membri.

3.6 **Stabilire le finalità precise del trattamento**

La base giuridica (normativa dell'Unione o dello Stato membro) dovrebbe stabilire la finalità del trattamento. La finalità dovrebbe essere specifica, così che non vi siano dubbi sul tipo di dati personali che occorre trattare per conseguire l'obiettivo perseguito, ed esplicita.

La/le finalità precise dipenderanno dalle funzionalità dell'app. Per ogni funzionalità potranno esserci più finalità. Al fine di garantire alle persone il pieno controllo dei loro dati, la Commissione raccomanda di non raggruppare le diverse funzionalità. In ogni caso, la persona dovrebbe avere la possibilità di scegliere tra diverse funzionalità che perseguono ciascuna una finalità distinta.

La Commissione consiglia di non utilizzare i dati raccolti nelle suddette condizioni per scopi diversi dalla lotta alla Covid-19. Qualora fosse necessario prevedere finalità quali la ricerca scientifica e la statistica, queste andrebbero incluse fin dall'inizio nell'elenco delle finalità e comunicate in modo chiaro agli utenti.

— Funzionalità "informazioni"

Scopo di questa funzionalità è fornire le informazioni che sono pertinenti dal punto di vista delle autorità sanitarie nel contesto della crisi emergenziale.

— Funzionalità "controllo dei sintomi" e "telemedicina"

La funzionalità "controllo dei sintomi" può fornire un'indicazione della percentuale effettivamente infetta degli individui che presentano sintomi compatibili con la Covid-19 (ad esempio, eseguendo tamponi e testando tutti o un numero casuale di individui che presentano tali sintomi, se si dispone di capacità adeguate). Nell'identificare la finalità si dovrebbe chiarire che i dati personali relativi alla salute saranno trattati allo scopo i) di fornire alla persona la possibilità di autovalutare, sulla base di una serie di domande, se ha sviluppato sintomi della Covid-19, oppure ii) di ottenere una consulenza medica nel caso in cui abbia effettivamente sviluppato tali sintomi.

— Funzionalità "tracciamento dei contatti" e "allerta"

La semplice indicazione di una finalità "prevenzione di ulteriori infezioni da Covid-19" non è abbastanza specifica. In questo caso, la Commissione raccomanda di specificare ulteriormente la/le finalità sulla falsariga seguente: "conservare i contatti delle persone che utilizzano l'app e che possono essere state esposte all'infezione da Covid-19 per avvertirle che potrebbero essere state potenzialmente contagiate".

3.7 **Definire limiti rigorosi per la conservazione dei dati**

Il principio di limitazione della conservazione dei dati impone l'obbligo di non conservare i dati personali più a lungo del necessario. Il limite temporale dovrebbe basarsi sulla pertinenza medica (a seconda delle finalità dell'app: periodo di incubazione, ecc.) e sui tempi realisticamente necessari per l'adozione di eventuali misure amministrative.

— Funzionalità "informazioni"

I dati raccolti durante l'installazione di questa funzionalità dovrebbero essere immediatamente cancellati. Non vi è alcun motivo per conservarli.

— Funzionalità "controllo dei sintomi" e "telemedicina"

Questo tipo di dati dovrebbe essere cancellato dalle autorità sanitarie dopo un periodo massimo di un mese (periodo di incubazione più margine) o dopo che la persona è stata sottoposta al tampone con esito negativo. Le autorità sanitarie possono conservare i dati per periodi più lunghi a fini di sorveglianza e per attività di ricerca, a condizione che ciò avvenga in forma anonima.

— Funzionalità "tracciamento dei contatti" e "allerta"

I dati di prossimità dovrebbero essere cancellati non appena cessano di esser necessari per allertare le persone. La cancellazione dovrebbe avvenire dopo un periodo massimo di un mese (periodo di incubazione più margine) o dopo che la persona è stata sottoposta al tampone con esito negativo. Le autorità sanitarie possono conservare i dati di prossimità per periodi più lunghi a fini di sorveglianza e per attività di ricerca, a condizione che ciò avvenga in forma anonima.

I dati dovrebbero essere conservati nel dispositivo dell'utente e solo quelli che sono stati comunicati dall'utente stesso e che sono necessari per perseguire la finalità prevista dovrebbero essere caricati sul server a disposizione delle autorità sanitarie nel caso in cui si scelga tale opzione (in altre parole, vanno caricati sul server solo i dati dei "contatti ravvicinati" di una persona risultata positiva all'infezione da Covid-19).

3.8 **Garantire la sicurezza dei dati**

La Commissione raccomanda di conservare i dati sul dispositivo terminale della persona in forma criptata, utilizzando tecniche crittografiche all'avanguardia. Nel caso in cui i dati siano conservati in un server centrale, l'accesso, anche quello amministrativo, dovrebbe essere registrato.

I dati di prossimità dovrebbero essere generati e conservati sul dispositivo terminale della persona soltanto in forma criptata e pseudonimizzata. Al fine di impedire il tracciamento da parte di terzi, dovrebbe essere possibile attivare il Bluetooth senza dover ricorrere ad altri servizi di localizzazione.

Durante la raccolta dei dati di prossimità tramite il Bluetooth a bassa energia (BLE) è preferibile creare e conservare gli identificativi utente temporanei che vengono periodicamente modificati invece di conservare il vero identificativo del dispositivo. Questa misura offre un'ulteriore protezione contro le intercettazioni e il tracciamento da parte di hacker e rende pertanto più difficile identificare le persone.

La Commissione raccomanda che il codice sorgente dell'app sia reso pubblico e accessibile a fini di riesame.

È possibile prevedere misure supplementari per proteggere i dati trattati, in particolare tramite la cancellazione automatica o la loro anonimizzazione dopo un certo periodo di tempo. In generale, il grado di sicurezza dovrebbe corrispondere alla quantità e alla sensibilità dei dati personali trattati.

Tutte le trasmissioni dal dispositivo personale alle autorità sanitarie nazionali devono essere criptate.

Qualora la legislazione nazionale preveda che i dati personali raccolti possono essere trattati anche per scopi di ricerca scientifica, si dovrebbe far ricorso, di norma, alla pseudonimizzazione.

3.9 **Garantire l'esattezza dei dati**

Garantire l'esattezza dei dati personali trattati non è soltanto un presupposto indispensabile per l'efficienza dell'app, ma è anche un principio previsto dalla legislazione in materia di protezione dei dati personali.

In questo contesto è essenziale garantire l'esattezza delle informazioni su un avvenuto contatto con una persona infetta (distanza epidemiologica e durata del contatto) per minimizzare il rischio di avere falsi positivi. In tal modo dovrebbero essere coperti i casi in cui il contatto tra due utenti dell'app avviene per strada, nei trasporti pubblici o all'interno di un edificio. È improbabile che l'uso dei dati relativi all'ubicazione ricavabili dalle reti di telefonia mobile sia a tal fine sufficientemente accurato.

È perciò consigliabile affidarsi a tecnologie che permettano una valutazione più precisa del contatto (ad esempio, Bluetooth).

3.10 **Coinvolgere le autorità preposte alla protezione dei dati**

Le autorità per la protezione dei dati dovrebbero essere pienamente coinvolte e consultate nel processo di sviluppo dell'app e dovrebbero continuare a monitorarne l'utilizzo. Poiché il trattamento dei dati nel contesto dell'app sarà considerato come trattamento su larga scala di categorie particolari di dati (dati relativi alla salute), la Commissione richiama l'attenzione sull'articolo 35 del GDPR riguardante la valutazione d'impatto sulla protezione dei dati.