Camera dei deputati
Ufficio Rapporti
con l'Unione europea
XVIII Legislatura

Documentazione per le Commissioni
Attività dell'**Unione europea**

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

Dossier n° 33 -
29 aprile 2020

Premessa

Il 16 aprile 2020 la Commissione europea ha presentato una serie di orientamenti per quanto riguarda le **caratteristiche** e i **requisiti** delle app volte al contrasto della crisi Covid-19 al fine di 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 (GDPR) e della direttiva *e-privacy*.

La pubblicazione del documento si inserisce nell'ambito della tabella di marcia per la revoca graduale delle **misure** di **contenimento** dell'epidemia di coronavirus, presentata il 15 aprile 2020 dalla Presidente della Commissione europea e dal Presidente del Consiglio europeo, che prevede, tra l'altro, un'adeguata capacità di **monitoraggio** e **diagnostiche** su larga scala, per individuare e isolare in tempi rapidi le persone infette, nonché di **rilevamento** e **tracciabilità** dei **contatti.** Gli orientamenti fanno altresì seguito alla raccomandazione (UE) 2020/518 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, e sono stati presentati contestualmente al pacchetto di strumenti "Applicazioni mobili per supportare la traccia dei contatti in lotta contro COVID-19" sviluppati dagli Stati membri dell'UE, con il sostegno della Commissione, mediante la rete comune eHealth Network (organismo di collegamento tra le autorità nazionali responsabili dell'assistenza sanitaria online designate dagli Stati Membri).

Gli orientamenti sono stati elaborati, inoltre, sulla base delle contributo del Comitato europeo per la protezione dei dati (EDPB), il quale ha successivamente pubblicato le 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.

La Commissione europea ha precisato che gli orientamenti **non sono giuridicamente vincolanti** e non pregiudicano il **ruolo**, esclusivo, della **Corte di giustizia dell'UE** per l'attività di interpretazione autentica del diritto dell'UE.

Ambito di applicazione

Gli orientamenti riguardano solo le 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**);
- allertare le persone che si sono trovate per un certo tempo in **prossimità** di una persona infetta (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**).

La Commissione europea **raccomanda** dunque l'uso di **app facoltative**.

Alla base di tale scelta, negli orientamenti si precisa che se, da un lato, in base alla direttiva e-privacy l'uso di un'app che incida sui **diritti alla riservatezza** delle comunicazioni di cui all'articolo 5 è possibile mediante una **legge** che sia **necessaria**, **opportuna** e **proporzionata** al fine di conseguire determinati **obiettivi specifici** (indicati tramite rinvio ai principi definiti nel regolamento generale sulla protezione dei dati

personali), dall'altro, per **l'elevata invasività** di siffatto approccio e in considerazione delle **criticità** che sorgerebbero in termini di messa in atto di idonee salvaguardie, è opportuno prima di ricorrere a questa opzione sia necessario effettuare un'attenta analisi.

Si ricorda infatti che, in ogni caso, l'articolo 5 della direttiva citata prevede che l'utente dei servizi di comunicazioni elettroniche possa prestare il **consenso** a tutta una serie di attività in esso precisate che incidono sulla sfera della riservatezza delle sue comunicazioni.

Sono escluse dall'ambito degli orientamenti le app (anche obbligatorie) finalizzate al rispetto delle prescrizioni in materia di **quarantena**.

Contenuti

La Commissione definisce gli elementi per un **uso fiduciario** e **responsabilizzato** delle app, in particolare, i limiti alla loro l'**intrusività**, i criteri per rispettare la legislazione dell'UE in materia di protezione dei **dati personali** e della **vita privata**, sfere di libertà garantite dalla **Carta europea dei diritti fondamentali**.

Le funzionalità delle app sono considerate suscettibili di incidere su altri principi contenuti nella Carta: **dignità umana**, **non discriminazione**, libertà di **circolazione**, libertà d'**impresa**, libertà di **riunione** e di **associazione**.

Titolarità del trattamento

Data la sensibilità dei dati personali in questione e la finalità del trattamento dei dati, 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).

Ai sensi dell'articolo 4 del GDPR, è titolare del trattamento la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le **finalità** e i **mezzi** del trattamento di dati personali; il titolare del trattamento è **responsabile** del rispetto del GDPR.

Controllo dei dati personali

L'obiettivo è garantire che le persone che utilizzano le app mantengano il controllo dei propri dati trattati per mezzo di tali strumenti. A tal fine, secondo la Commissione europea:

- 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**;

Si ricorda che il Comitato europeo per la protezione dei dati (EDPB) ha precisato che i titolari del trattamento dei dati dovranno garantire che il consenso al trattamento dei dati sulla base previsto dall'app soddisfi requisiti rigorosi, e (in particolare se si tratti di autorità pubbliche) dovranno prestare particolare attenzione al fatto che il consenso non dovrebbe essere liberamente espresso se la persona non ha l'effettiva possibilità di rifiutare o di revocare il proprio consenso senza subire pregiudizio.

La Commissione non fornisce indicazioni sulle conseguenze negative cui fa riferimento; né, del resto, sono indicati possibili strumenti di incentivazione all'impiego di tali tecnologie che eviterebbero di rimettere tale scelta esclusivamente alla discrezionalità del possessore di un dispositivo ovvero ai comportamenti poco corretti del soggetto gestore della app. Come da più parti segnalato, l'utilità di una app dipende in larga parte dalla sua diffusione, stante la necessità d raggiungere una soglia critica adeguata di adesione presso la popolazione .

- le diverse funzionalità dell'app (informazioni, controllo dei sintomi, tracciamento dei contatti e allerta) **non** dovrebbero essere **raggruppate**, dando la possibilità all'utente di **attivarle separatamente**, eventualmente anche **in combinazione** tra di loro;
- i **dati di prossimità** (sostanzialmente, **durata** e **vicinanza** di un contatto con una persona contagiata, determinate secondo criteri epidemiologici) devono essere conservati sul dispositivo della persona; la Commissione precisa tuttavia, che 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;
- la persona dovrebbe essere in grado di esercitare i **diritti** previsti dal GDPR;
- la **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** (anche in assenza di disinstallazione da parte dell'utente).

Base giuridica per il trattamento

La Commissione indica una serie di **fondamenti di liceità** del **trattamento** a seconda del tipo di **dato** che ne è oggetto.
In sintesi, richiamando la direttiva e-pricacy (articolo 5):

- la conservazione di informazioni sul dispositivo dell'utente o l'accesso a informazioni già conservate sono consentiti o sulla base del **previo consenso espresso** dell'utente (opzione 1), o anche qualora sono normalmente **necessari** affinché le app funzionino e purché vi sia un **servizio** (l'installazione o l'attivazione dell'app) espressamente **richiesto** da parte dell'utente (opzione 2);
- diversamente, nell'ambito della funzionalità del tracciamento dei contatti e dell'**allerta**, essendo richiesta la conservazione sul dispositivo dell'utente di informazioni differenti da quelle citate ed eventualmente i **dati di prossimità**, la Commissione europea precisa che tale caricamento **non può considerarsi necessario** per il funzionamento dell'app in quanto tale. Di conseguenza, il consenso (opzione 1) rimane il motivo più adeguato per le attività pertinenti: esso deve **libero**, **specifico**, **esplicito** e **informato** ai sensi del GPPR, nonché espresso mediante un'**azione positiva inequivocabile** della persona.

La Commissione europea ricorda inoltre che le **autorità sanitarie nazionali** trattano generalmente dati personali quando esiste un **obbligo legale** stabilito dal diritto dell'UE o nazionale che prevede tale trattamento, o quando tale trattamento è necessario per promuovere l'**interesse pubblico** riconosciuto dal diritto dell'UE o nazionale.

Si ricorda, inoltre, ai sensi dell'articolo 9 del GDPR i dati relativi alla salute (per i quali è normalmente previsto il divieto di trattamento), possono essere trattati, tra l'altro, ove sia necessario per motivi di **interesse pubblico** nel settore della **sanità pubblica**, quali la **protezione** da **gravi minacce** per la salute a **carattere transfrontaliero** o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il **segreto professionale**.

La Commissione europea precisa che le **norme dell'UE** e degli **Stati membri** preesistenti alla pandemia di Covid-19 e quelle che gli Stati membri sarebbero in procinto di adottare 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 del GDPR.

L'utilizzo della normativa come base giuridica – secondo la Commissione europea - contribuirebbe alla **certezza del diritto**, sotto i seguenti profili: definizione del trattamento e sua finalità; indicazione del titolare del trattamento e dei soggetti abilitati all'accesso ai dati; esclusione di finalità diverse da quelle stabilite dalle norme, **previsione di garanzie specifiche.**

In ogni caso la Commissione europea ribadisce che 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.
Infine, la Commissione europea ricorda che la funzione di allerta nei confronti di una persona che sia entrata in contatto con un'altra positiva dovrebbe essere oggetto di valutazione anche alla luce del **divieto** di **sottoporre le persone** a una **decisione** basata **unicamente** sul **trattamento automatizzato** che produca **effetti sulla loro sfera giuridica** o che incida in modo

analogo significativamente sulla loro persona (articolo 22 del GDPR).

Tale principio è generalmente contemperato mediante una serie di **deroghe**, basate tra l'altro sul consenso o sul diritto nazionale o dell'UE, purché vengano previste **misure adeguate** a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato.

In proposito, il Comitato europeo per la protezione dei dati (EDPB) ha in ogni caso precisato che le indicazioni fornite dalle autorità sanitarie in merito ai passi da compiere successivamente alla ricezione di un alert non dovrebbero basarsi unicamente su un trattamento automatizzato.

Il tema richiede un ulteriore approfondimento circa la questione dei limiti alla divulgazione e all'accesso, presupponendo che, per poter indirizzare a utenti tracciati una determinata misura restrittiva, le autorità dovrebbero avere la facoltà di risalire ai nominativi degli effettivi utenti dell'app tracciati mediante codici pseudonimizzati e trasmessi dai dispositivi, eventualmente mediante l'organizzazione e l'impiego una banca dati centralizzata (vedi infra).

Minimizzazione dei dati

La protezione garantita dalla normativa europea (GPDR e direttiva *e-pricacy*) riguarda: i **dati personali**; i dati relativi all'**ubicazione**; tutte le informazioni conservate nell'**apparecchiatura terminale** dell'utente e da essa accessibili.

In tale contesto, la Commissione europea richiama il rispetto del principio della **minimizzazione dei dati** (previsto dal GPDR), in base al quale solo i dati personali che sono **adeguati**, **pertinenti** e **limitati a quanto necessario rispetto alle finalità** possono essere trattati. Secondo la Commissione, pertanto, una valutazione della necessità di trattare i dati personali e della loro pertinenza dovrebbe essere effettuata alla luce delle **finalità** perseguite; infine viene sottolineato che la produzione e il trattamento di una quantità minore di dati si traducono anche in **minor rischio per la loro sicurezza**.

Dall'applicazione del principio discende, tra l'altro che ove l'app ricomprenda la funzionalità "**controllo dei sintomi**" e "**telemedicina"**, l'implicazione di dati personali relativi alla **salute**, comporta - secondo la Commissione europea - la necessità che la normativa di riferimento applicabile alle autorità sanitarie **specifichi l'elenco dei dati** che possono essere trattati.

La minimizzazione dei dati è declinata dalla Commissione europea con particolare riferimento alla funzionalità di **tracciamento** e **allerta**, in particolare per quanto concerne il trattamento dei **dati di prossimità**, considerati necessari per interrompere l'eventuale catena di infezione.

La Commissione raccomanda l'uso di dati di comunicazione basati sul **Bluetooth a bassa energia** (o di dati basati su una tecnologia analoga) per determinare la prossimità, anche in considerazione del fatto che tale tecnologia **evita la possibilità di** registrare spostamenti (a differenza dei dati di geolocalizzazione).

In questo contesto, infatti, la Commissione consiglia di **non utilizzare i dati relativi all'ubicazione**, in quanto **non 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. In definitiva 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.

In particolare, la Commissione europea **non ritiene necessario conservare l'ora** del contatto o il **luogo esatti**, sottolineando invece che potrebbe 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) e per inviare il messaggio di follow-up raccomandando, ad esempio, la durata del periodo di quarantena. I dati di prossimità inoltre dovrebbero essere generati e trattati solo se sussiste un rischio reale di infezione (in funzione della **vicinanza** e della durata del **contatto**).

Le citate linee guida dell'EDPB ribadiscono l'importanza del rispetto del principio di minimizzazione e dei principi della protezione dei dati fin dalla progettazione e per impostazione predefinita (data protection by design and by default), precisando, tra l'altro, che le app per il tracciamento dei contatti non necessitano della registrazione della posizione dei singoli utenti e che occorre invece utilizzare i dati di prossimità. L'EDPB, ha chiarito, in una sezione distinta del medesimo documento le condizioni e i principi per l'uso proporzionato 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.

Circa le **modalità di allerta** delle persone che sono state in contatto ravvicinato con una persona infetta la Commissione europea propone due alternative:

a) l'**invio automatico** di un'allerta (tramite messaggio definito dalle autorità sanitarie **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**);

Sono codici TAN quelli che vengono generati per essere usati una volta sola, come nelle procedure di accesso e di operazioni sui siti di *homebanking*. I QR sono codici a barre bidimensionali, largamente diffusi per memorizzare informazioni facilmente lette tramite gli *smarphone*.

b) gli **identificativi temporanei** generati in modo arbitrario sono **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**.

Limiti alla divulgazione di dati e l'accesso ai dati

La Commissione europea stabilisce una serie di principi in materia per contenere la divulgazione e l'accesso ai dati.

In particolare in relazione alla funzionalità controllo dei sintomi e telemedicina, e all'obiettivo di garantire l'assistenza sanitaria adeguata, l'orientamento è che si possa decidere che le autorità sanitarie ed epidemiologiche debbano **accedere** alle informazioni fornite dal paziente; è altresì contemplata la possibilità per il Centro europeo per la prevenzione e il controllo delle malattie (ECDC) di ricevere i **dati aggregati** dalle autorità nazionali ai fini della sorveglianza epidemiologica.

Divulgazione e accesso dei dati relativamente alla funzionalità "tracciamento dei contatti" e "allerta"

La Commissione europea distingue i dati delle persone infette da quelli delle persone che sono state in contatto (epidemiologico) con la persona infetta.

Con riferimento ai primi, il punto di partenza è che le app debbano generare **identificativi pseudonimi** generati arbitrariamente per i **telefoni** che sono in **contatto** con l'utente. Sono contemplati (e in astratto **ammessi**) due tipi di approccio:

- secondo il **trattamento decentralizzato**, gli identificativi (in codice) sono conservati sul dispositivo dell'utente;
- secondo la soluzione del **server back end** gli identificativi arbitrari sono conservati nel server al quale le autorità sanitarie hanno accesso;

L'orientamento della Commissione europea è che la **soluzione decentralizzata** sia **più conforme al principio della minimizzazione**.

Di parere analogo anche l'EDPBE che, pur ritenendo entrambe le opzioni praticabili a condizione che siano in vigore adeguate misure di sicurezza, (e premesso che entrambe comportano una serie di vantaggi e svantaggi), ribadisce la maggiore conformità al principio della soluzione decentralizzata.

Inoltre, la Commissione europea ritiene che:

- le autorità sanitarie dovrebbero avere accesso **soltanto ai dati di prossimità** del dispositivo della persona infetta (i dati delle persone a rischio contagio, in modo da contattarli);
- siano a disposizione delle autorità sanitaria solo i **dati proattivamente condivisi** dalla persona infetta;
- la persona infetta **non dovrebbe conoscere l'identità** delle persone tracciate epidemiologicamente (che riceveranno l'allerta).

Per quanto concerne i dati delle persone che sono state in contatto (epidemiologico) i principali orientamenti della Commissione sono:

- l'**identità** della **persona infetta** non dovrebbe essere comunicata alle persone con le quali è stata **in contatto** epidemiologico, mentre è sufficiente mettere queste ultime a conoscenza del contatto epidemiologico con persona infetta nel corso degli **ultimi 16 giorni**;
- non devono essere conservati né comunicati dati relativi a **ora** e **luogo** del contatto;
- 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.

Stabilire le finalità precise del trattamento

La Commissione indica in che modo il diritto nazionale o dell'UE dovrebbe individuare gli obiettivi degli specifici trattamenti dei dati. Al riguardo, per quanto concerne il controllo dei sintomi" e "telemedicina" 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.
Con riferimento alle funzioni di tracciamento e allerta la Commissione raccomanda di specificare ulteriormente 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
La Commissione consiglia di **non utilizzare** i dati raccolti nelle suddette condizioni **per scopi diversi dalla lotta alla Covid-19**; anche le finalità relative alla **ricerca scientifica** e la **statistica** andrebbero esplicitate agli utenti dell'app **fin dall'inizio**.

Limiti alla conservazione dei dati

In tale sezione la Commissione europea applica alle diverse funzionalità delle app il **principio** che impedisce di conservare i dati personali **più a lungo del necessario**, premettendo che il limite temporale dovrebbe basarsi sulla **pertinenza medica** e sui **tempi** realisticamente **necessari** per l'adozione di eventuali **misure amministrative**.
In particolare, i dati raccolti durante l'installazione di questa funzionalità dovrebbero essere immediatamente cancellati.
I dati necessari per il controllo dei sintomi e la telemedicina dovrebbero essere **cancellati** dalle autorità sanitarie dopo un **periodo massimo** di **un mese** o dopo che la persona è stata sottoposta al **tampone con esito negativo**, salva la possibilità di periodi più lunghi per ragioni di sorveglianza e ricerca (ma in tal caso in forma anonima).
Circa la funzionalità di **tracciamento** e **allerta**, la Commissione europea ritiene che i dati di prossimità dovrebbero essere cancellati **non appena cessano di esser necessari** per **allertare** le persone; per la cancellazione viene raccomandato lo stesso lasso di tempo, compreso il regime dell'estensione per fini di sorveglianza e attività di ricerca. Inoltre, la Commissione europea precisa che i dati nell'ambito di tale funzionalità 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). La Commissione chiarisce che andrebbero in definitiva caricati su tale server solo i dati dei contatti ravvicinati di una persona risultata positiva all'infezione da Covid-19.

Sicurezza dei dati

In tale sezione la Commissione raccomanda, tra l'altro, che:

la conservazione dei dati sul dispositivo terminale della persona avvenga **in forma criptata** impiegando le tecniche di ultima generazione;

- in caso di conservazione su **server centrale**, l'accesso, anche quello amministrativo, sia **registrato**;
- durante la raccolta dei **dati di prossimità** tramite il Bluetooth a bassa energia (BLE) siano creati e conservati gli identificativi utente **temporanei** che vengono **periodicamente modificati** invece di conservare il vero identificativo del dispositivo;
- il **codice sorgente** dell'app sia reso **pubblico** e **accessibile** a fini di riesame (cosiddetto *open source*);

Infine, la Commissione europea sottolinea la necessità di garantire l'**esattezza** dei dati sia quale principio generale della normativa europea sulla protezione dei dati, sia come precondizione per **l'efficienza** dell'app, raccomandando a tal fine l'uso di tecnologie capaci di valutazioni più precise del contatto, come il BT.

È infine raccomandato il coinvolgimento delle **autorità per la protezione dei dati** nelle fasi dello **sviluppo** e del **monitoraggio** delle app.

Infine, in linea di massima, sia la Commissione europea sia il citato Comitato ritengono che debba essere effettuata una **valutazione d'impatto** sulla protezione dei dati (generalmente prevista dall'articolo 35 del GDPR) **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). Il Comitato raccomanda vivamente la **pubblicazione** degli esiti di tali **valutazioni**.

Soluzioni adottate (o in via di adozione) in altri Stati membri o extra UE

Il Parlamento europeo ha pubblicato uno studio relativamente al tracciamento dei dispositivi mobili per il contrasto al COVID 19, che riferisce, tra l'altro, in merito alle iniziative avviate da una serie di Stati, anche extraeuropei, sul piano delle scelte delle tecnologie più opportune.
Si ricorda che in linea di massima il dibattito sull'organizzazione delle app si concentra attualmente sull'alternativa tra livelli diversi di centralizzazione dei dati. In particolare, secondo fonti informali, le più importanti società informatiche, Apple e Google, propenderebbero per soluzioni di tracciamento meno invasive della privacy, che limiterebbero l'invio dei dati a un server centrale relativi alla sola positività di un soggetto, mentre la registrazione e il riscontro di un contatto tra un utente contagiato e altri utenti dovrebbe avvenire solo localmente sui dispositivi interessati. Secondo tali informazioni, in Europa non vi sarebbe uniformità di scelta tra gli Stati: alcuni Stati membri (in particolare Germania, Austria e Spagna) sembrerebbero condividere l'approccio decentralizzato; diversamente la Francia ha finora mostrato di preferire un sistema di trattamento centralizzato, in sintonia con quanto starebbe accadendo anche in Regno Unito (Stato non più membro dell'UE).
Di seguito una sintesi delle indicazioni fornite (al 20 aprile 2020) da alcuni Stati riportate nello studio citato.

Unione europea

Francia
Il Governo starebbe riflettendo su una strategia per l'**identificazione digitale** delle persone che sono state in contatto con persone infette. L'operatore di telefonia mobile Orange ha confermato di aver iniziato a condividere dati di **geolocalizzazione** aggregati e anonimizzati con Inserm, un istituto di ricerca pubblico interamente dedicato alla salute umana, per consentire loro di anticipare e gestire meglio la diffusione dell'epidemia.

Germania
Il Ministero dell'Interno, in Germania, ha comunicato di non prevedere di "valutare e tracciare i dati dei telefoni cellulari a livello nazionale". Il Ministro della giustizia tedesco Christine Lambrecht ha affermato che le app di tracciamento per aiutare a combattere Covid-19 possono

essere utilizzate **solo volontariamente**. Deutsche Telekom ha annunciato che sta condividendo i dati anonimi sulla posizione dei suoi utenti con il Robert-Koch Institute, un istituto di ricerca e agenzia governativa responsabile del controllo e della prevenzione delle malattie.

Spagna
La Spagna prevede di utilizzare **i dati sulla posizione del telefono** cellulare per tenere traccia dei movimenti delle persone al fine di valutare **l'adesione alle misure di blocco**. Uno studio noto come "DataCovid" dovrebbe essere condotto dall'istituto nazionale di statistica in collaborazione con i principali operatori di telecomunicazioni del paese. Il Ministero della Salute avrebbe comunicato che intende anche utilizzare i dati sulla posizione per avviare un'app che avviserà gli utenti di **effettuare un'autovalutazione**. Tali app di tracciamento sono già state rilasciate in Catalogna e a Madrid.

Stati extra UE

Cina
La Cina obbliga i cittadini ad utilizzare un'app che tiene **traccia dei loro movimenti**. L'Alipay Health Code system combina i dati sulla posizione e altre informazioni (ad esempio un sondaggio sanitario) per valutare le persone in base al loro rischio di contagio e limitarne la mobilità.

Singapore
Il Governo ha lanciato l'app di **tracciamento dei contatti**, *TraceTogether*, che utilizza la tecnologia Bluetooth per tenere un registro dei dispositivi che sono entrati in prossimità. I dati vengono crittografati e archiviati sul dispositivo e le persone che diventano sintomatiche possono caricarli **volontariamente** (in formato pseudo-anonimo) in un database, che il Ministero della Salute utilizza per **notificare** ai proprietari dei dispositivi che sono stati sottoposti a tracciamento dal telefono della persona infetta.

UK
Il Governo sta discutendo con BT, uno dei maggiori operatori di telefonia mobile nel paese, sull'**uso della posizione del telefono** e dei dati per monitorare l'efficacia delle misure di distanza sociale.
Secondo fonti informali, il Regno Unito sarebbe intenzionato ad una gestione centralizzata dei dati.

Israele
Israele ha adottato norme emergenziali per consentire ai servizi di sicurezza di **tracciare i movimenti** delle persone sospette o testate positive al virus.

USA
Le agenzie governative hanno iniziato a utilizzare i dati dei dispositivi mobili per tracciare la diffusione del virus.