

## I TEMI: COVID-19 - APP IMMUNI: LE LINEE GUIDA DEL COMITATO EUROPEO PER LA PROTEZIONE DEI DATI PERSONALI

### 01. NOZIONE

La situazione di grave emergenza venutasi a creare a seguito dell'espandersi del virus identificato come **COVID-19** sta, come era prevedibile, espandendo il disagio economico per i cittadini, per le imprese e per le arti e professioni.

Tra DL, DPCM, DM, Ordinanza, Circolari, Risoluzioni, Raccomandazioni, Protocolli tutti, beninteso, utili appare sempre più difficile mantenere un filo logico soprattutto per il loro accavallarsi.

Nell'ambito di una probabile, seppur parziale riapertura, la task force di nomina governativa, ha fortemente insistito per la creazione di una APP che possa meglio garantire i cittadini eventualmente vittime di un contagio di ritorno, l'ormai famosa **IMMUNI**. Tale strumento consentirebbe di identificare i telefonini venuti a contatto con la persona contagiata consentendo una più agevole ricerca ed avviso delle persone potenzialmente a rischio.

Ovviamente tale tecnologia, se mal utilizzata, lede il diritto alla privacy delle persone.

In tale ambito le **Linee guida del Comitato europeo per la protezione dei dati** adottate il **21 aprile 2020** e pubblicate sotto il titolo "**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**"

In questa scheda ne seguiamo il dettato.

## 02. IL CONTESTO DI OSSERVAZIONE

L'elaborato prende atto che 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 che ciò suscita numerose preoccupazioni in materia di tutela della vita privata.

Il Comitato sottolinea che il quadro giuridico in materia è stato concepito **per essere flessibile** e con lo scopo di conseguire una risposta efficace per limitare la pandemia e, nel contempo, proteggere i diritti umani e le libertà fondamentali. Rimane forte convinzione del Comitato **che la protezione dei dati è elemento indispensabile** per generare un clima di fiducia che porti all'accettazione sociale della soluzione proposta per poter garantire **l'efficacia della stessa**.

Appare preferibile sviluppare un approccio comune europeo o, almeno, realizzare una cornice di interoperabilità.

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.

Senza dimenticare che tali strumenti hanno limiti intrinseci e che restano indispensabili 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.

Le presenti linee-guida in discussione 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.

L'efficienza 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). Tali applicazioni 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.**

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-22.

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.**

### **03. UTILIZZO DEI DATI RELATIVI ALL'UBICAZIONE**

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;

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.).

Il Comitato ricorda **che i dati** relativi all'ubicazione 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.

Per quanto riguarda **le informazioni**, compresi i dati relativi all'ubicazione, raccolte direttamente dall'apparecchiatura terminale, si applica **l'articolo 5** 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**

l'utente ha prestato il consenso;

la memorizzazione e/o l'accesso sono strettamente necessari al servizio della società dell'informazione esplicitamente richiesto dall'utente

Rimangono 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**.

I dati già in possesso **possono essere ulteriormente trattati 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.

Si sottolinea che occorre sempre privilegiare il trattamento di dati anonimi. La valutazione della robustezza della tecnica di anonimizzazione adottata dipende da tre fattori:

**individuabilità** (singling out) (possibilità di isolare una persona all'interno di un gruppo sulla base dei dati);

**correlabilità** (possibilità di correlare due record riguardanti la stessa persona);

**inferenza** (possibilità di dedurre, con probabilità significativa, informazioni sconosciute relative a una persona).

Fatti degli esempi il Comitato sottolinea che un ampio corpus di ricerche ha dimostrato 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. 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 a meno che non si riduca in misura sufficiente la precisione delle coordinate geografiche, o se non si eliminano dettagli del percorso di tracciamento.

Al fine di conseguire l'anonimizzazione, i dati relativi all'ubicazione devono essere trattati con attenzione per soddisfare il test di ragionevolezza.

#### **04. APP PER IL TRACCIAMENTO DEI CONTATTI**

**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**.

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. Comunque **devono essere definiti con chiarezza e fin dall'inizio i ruoli e le responsabilità rispettive e di tutto ciò devono essere informati gli utenti**.

**Le finalità devono essere sufficientemente specifiche così da escludere trattamenti ulteriori per scopi non correlati alla gestione della crisi sanitaria causata da COVID-19, definita con chiarezza la finalità, sarà necessario garantire che l'uso dei dati personali sia adeguato, necessario e proporzionato.**

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.

Per quanto riguarda **la liceità** del trattamento. 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.

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. La base giuridica più pertinente risulta essere la necessità del trattamento per lo svolgimento di un compito di interesse pubblico.

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.

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.

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.

Il Comitato ritiene che tali app non possano sostituire, ma solo supportare, il tracciamento manuale dei contatti effettuato da personale sanitario pubblico qualificato.

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.

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). **Il Comitato raccomanda vivamente la pubblicazione degli esiti di tali valutazioni.**

## 05. CONCLUSIONE

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.

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**