DIRITTO24

COVID-19

Il contact tracing, quale misura di contenimento del Covid-19, alla luce delle Linee guida dell'EDPS sul principio di proporzionalità e dell'EDPB sull'uso dei dati di localizzazione e degli strumenti per il tracciamento dei contatti nel contesto dell'emergenza legata al COVID-19

a cura dell' avv. Mario Valentini , partner di Pirola Pennuto Zei & Associati

L'emergenza sanitaria di questi mesi, scaturita dalla diffusione del virus Covid-19, ha radicalmente inciso sulle vite dei cittadini di tutto il mondo, facendo emergere la necessità di limitare il più possibile la diffusione del contagio ed evitare il sovraccarico delle strutture sanitarie, mediante l'utilizzo di misure sempre più stringenti e strumenti di controllo più efficaci per vigilare sulla loro attuazione.

Attraverso il contact tracing, in casi di contagio si potrà risalire ai contatti del singolo negli ultimi 14 giorni, e avere informazioni chiare sui luoghi e le persone che ha frequentato e a cui potrebbe aver trasmesso il virus. Finita la fase di test e apportate le modifiche che si saranno eventualmente rese necessarie, l'App così sviluppata potrà essere messa a disposizione di tutti.

Si pone, quindi, il problema del bilanciamento tra la tutela della salute pubblica e le libertà individuali, quali la tutela dei dati personali degli interessati.

Sul tema del rispetto della **tutela del trattamento dei dati personali e delle norme contenute nel Regolamento UE n. 2016/679** nel contesto dell'emergenza sanitaria legata al Covid-19, è intervenuto lo stesso **Comitato europeo per la protezione dei dati - European Data Protection Board (EDPB)**, prospettando il trattamento di dati personali mediante contact tracing, come misura volta a contenere la pandemia.

Nella **Dichiarazione sul trattamento dei dati personali nel contesto dell'epidemia di COVID-19** del 19 marzo u.s. l'EDPB ha evidenziato che le norme in materia di protezione dei dati, quale il GDPR, non ostacolano l'adozione di misure per il contrasto della pandemia di Covid-19. La lotta contro le malattie trasmissibili è obiettivo condiviso da tutte le nazioni, in quanto è nell'interesse dell'umanità arginare la diffusione delle malattie, anche mediante l'utilizzo di tecniche moderne.

In occasione della sua **23ma sessione plenaria**, il Comitato europeo per la protezione dei dati ha adottato due **Linee-guida, una sul trattamento di dati relativi alla salute per finalità di ricerca nel contesto dell'emergenza legata al COVID-19, e una sull'utilizzo della geolocalizzazione e di altri strumenti di tracciamento** nel contesto dell'emergenza stessa.

Su quest'ultimo porremo l'attenzione per vedere come lo stesso sia stato riflesso nel Decreto Legge 30 aprile 2020 n. 28.

Anche in questi momenti eccezionali, titolari e responsabili del trattamento devono garantire la protezione dei dati personali degli interessati, tenendo conto di una serie di considerazioni per

garantire la liceità del trattamento di dati personali e facendo sì che qualsiasi misura adottata in questo contesto rispetti i principi generali del diritto e non possa essere irrevocabile. L'EDPB evidenzia, infatti, sin dalla Dichiarazione sul trattamento dei dati personali nel contesto dell'epidemia di COVID-19 del 19 marzo 2020, che "***l'emergenza è una condizione giuridica che può legittimare limitazioni delle libertà, a condizione che tali limitazioni siano proporzionate e confinate al periodo di emergenza"*** .(1)

L'EDPB sottolinea, poi, che "l***l GPDR, come normativa di ampia portata, contiene disposizioni che si applicano anche al trattamento dei dati personali in un contesto come quello relativo al COVID-19. Il GDPR consente infatti alle competenti autorità sanitarie pubbliche e ai datori di lavoro di trattare dati personali nel contesto di un'epidemia, conformemente al diritto nazionale e alle condizioni ivi stabilite. Ad esempio, se il trattamento è necessario per motivi di interesse pubblico rilevante nel settore della sanità pubblica"***.

In relazione al trattamento dei dati personali, comprese le categorie particolari di dati, da parte di autorità pubbliche competenti, quali appunto le autorità sanitarie pubbliche, l'EDPB ritiene che "***gli articoli 6 e 9 del GDPR consentano tale trattamento, in particolare quando esso ricada nell'ambito delle competenze che il diritto nazionale attribuisce a tale autorità pubblica e nel rispetto delle condizioni sancite dal GDPR"*** (2)

Con riferimento all'uso dei dati di localizzazione da dispositivi mobili, e nello specifico con riguardo all'utilizzo da parte dei governi degli Stati membri dei dati personali relativi ai telefoni cellulari dei singoli nell'intento di monitorare, contenere o attenuare la diffusione del Covid-19, l'EDPB evidenzia che *"In alcuni Stati membri i governi prevedono di utilizzare i dati di localizzazione da dispositivi mobili per monitorare, contenere o attenuare la diffusione del COVID-19. Ciò implicherebbe, ad esempio, la possibilità di geolocalizzare le persone o di inviare messaggi di sanità pubblica ai soggetti che si trovano in una determinata area, via telefono o SMS.* ***Le autorità pubbliche dovrebbero innanzitutto cercare di trattare i dati relativi all'ubicazione in modo anonimo (ossia, trattare dati in forma aggregata e tale da non consentire la successiva re-identificazione delle persone), il che potrebbe permettere di generare analisi sulla concentrazione di dispositivi mobili in un determinato luogo ("cartografia").*** Al riguardo, ***si applica anche il principio di proporzionalità. Si dovrebbero quindi sempre privilegiare le soluzioni meno intrusive, tenuto conto dell'obiettivo specifico da raggiungere***."

Su questo aspetto, il sopra menzionato Decreto Legge 30 aprile 2020, n. 28, che comprende, tra l'altro, le previsioni normative relative alla APP Immuni, prevede al 2 comma dell'art. 6 che Il Ministero della Salute, all'esito di una valutazione di impatto, costantemente aggiornata, effettuata ai sensi dell'articolo 35 del Regolamento (UE) 2016/679, adotti misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato ai rischi elevati per i diritti e le libertà degli interessati.

Con riferimento a quest'aspetto, **le Linee guida sul principio di proporzionalità, adottate in data 19 dicembre 2019 dal Garante europeo della protezione dei dati (EDPS),** si configurano quale strumento utile ai fini della valutazione della proporzionalità delle misure legislative, che si intendono adottare..

Infatti, tali Linee guida, definendo ulteriormente il contenuto e lo scopo delle garanzie espresse dalla Carta dei diritti fondamentali dell'Unione europea e dal GDPR, si configurano per i responsabili politici nazionali quale strumento pratico per valutare la conformità delle misure proposte, che potrebbero avere un impatto sulla protezione dei dati personali, come delineata dalla stessa Carta dei diritti fondamentali dell'Unione europea.

Le Linee guida evidenziano che l'articolo 8 della Carta dei diritti fondamentali dell'Unione europea sancisce il diritto alla protezione dei dati personali. Tale diritto non è assoluto e può essere limitato, a condizione che le limitazioni siano conformi ai requisiti di cui all'articolo 52, paragrafo 1, della Carta, che afferma che "*eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla presente Carta devono essere previste dalla legge e rispettare il contenuto essenziale di detti diritti e libertà. Nel rispetto del principio di proporzionalità, possono essere apportate limitazioni solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui*".

Per essere lecita, qualsiasi limitazione all'esercizio dei diritti fondamentali tutelati dalla Carta deve quindi rispettare i seguenti criteri:

•deve essere prevista dalla legge;

•deve rispettare l'essenza dei diritti;

•deve conseguire obiettivi di interesse generale riconosciuti dall'Unione o la necessità di proteggere i diritti e le libertà altrui;

•deve essere necessaria;

•deve essere proporzionata.

La proporzionalità in senso lato comprende sia la **necessità** *che l'***adeguatezza** *(proporzionalità in senso stretto) di una misura.*

La **necessità i***mplica una valutazione combinata e basata sui fatti dell'efficacia della misura per l'obiettivo perseguito e se sia meno invasiva rispetto ad altre opzioni per raggiungere lo stesso obiettivo.*

Il test di necessità dovrebbe essere considerato come il primo passo a cui deve conformarsi una misura proposta che comporta il trattamento di dati personali, sicché una misura che non si è dimostrata necessaria non dovrebbe essere proposta a meno che e finché non sia stata modificata per soddisfare il requisito della necessità: in altre parole, la necessità è una condizione preliminare per la proporzionalità.

Ai fini della valutazione della proporzionalità (adeguatezza) le Linee Guida offrono una vera e propria check list, articolata in quattro passaggi, che implicano:

1. la valutazione dell'importanza dell'obiettivo e in che modo la misura possa raggiungerlo;

2. la valutazione dello scopo, dell'estensione e dell'intensità dell'inferenza ingenerata dalla misura;

3. procedere ad un equo bilanciamento della misura;

4. se la misura non è proporzionata, identificare ed introdurre le adeguate clausole di salvaguardia, ovvero individuare misure di contenimento e rimedi.

Il Comitato europeo per la protezione dei dati ha quindi emanato le L**inee-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 a proposito dei sistemi di contact tracing.

Tali Linee guida possono sintetizzarsi nei termini seguenti:

a) **volontarietà:** in ragione del rilevante impatto individuale del tracciamento, l'adesione al sistema deve essere frutto di una scelta realmente libera da parte dell'interessato. La mancata adesione al sistema non deve quindi comportare svantaggi né rappresentare la condizione per l'esercizio di diritti.

Il Decreto legge del 30 aprile appare chiaro in questo senso nel recepire tale principio. Infatti, il comma 4 dell'articolo 6 del Decreto chiarisce al riguardo che il mancato utilizzo dell'applicazione non comporta conseguenze pregiudizievoli;

b) **previsione normativa:** il presupposto per lo svolgimento delle attività di trattamento può individuarsi nell'esigenza di svolgimento di un compito di interesse pubblico, in particolare per esigenze di sanità pubblica, in base a "previsione normativa o disposizione legislativa" dell'Unione europea o degli Stati membri.

Sotto questo profilo, in particolare, l'Italia ha scelto l'adozione di una norma di rango primario, scelta che soddisfa i requisiti di cui all'articolo 9, par. 2, lett. i) del GDPR, quando afferma che il trattamento dei dati particolari, inclusi quelli sullo stato di salute, è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero.

Il GDPR sembra dunque aver tenuto in chiara considerazione il trattamento di dati in contesti come questo che stiamo vivendo.
Garanzie ulteriori potranno essere stabilite con il previsto provvedimento del Garante da adottare ai sensi dell'articolo 2-quinquiesdecies del medesimo Codice.
Le Linee Guida prevedono altresì un ulteriore criterio, quello della trasparenza: è necessario assicurare il pieno rispetto degli obblighi di trasparenza previsti dal Regolamento nei confronti degli interessati. In linea con tale esigenza appare la previsione di cui all'articolo 1, comma 2, lett. a), del Decreto Legge, che assicura agli interessati un'idonea informazione sul trattamento e in particolare sulla pseudonimizzazione dei dati. Infatti, l'art. 1, comma 2 lettera a) del Decreto prevede che "*gli utenti ricevano, prima dell'attivazione dell'applicazione, ai sensi degli articoli 13 e 14 del Regolamento (UE) 2016/679, informazioni chiare e trasparenti al fine di raggiungere una piena consapevolezza, in particolare, sulle finalita' e sulle operazioni di trattamento, sulle tecniche di pseudonimizzazione utilizzate e sui tempi di conservazione dei dati*".
Al riguardo, il Parere del Garante in materia raccomanda all'Amministrazione interessata di sottoporre la valutazione di impatto, cui è tenuta, come ricordavamo, ai sensi del comma 2 dell'Art. 6 del Decreto, al più ampio regime di conoscibilità possibile.
E' opportuno altresì prevedere, anche nella norma, eventualmente in sede di conversione, il carattere libero e aperto del software da rilasciare con licenza open source.
Le Linee guida del Comitato Europeo per la protezione dei dati contengono poi i seguenti principi, tutti riflessi nel decreto del 30 aprile e salvo alcune precisazioni di cui si dirà. I principi sono:
d) **determinatezza ed esclusività** dello scopo: il tracing dev'essere finalizzato esclusivamente al contenimento dei contagi, escludendo fini ulteriori, ferme restando le possibilità di utilizzo a fini di ricerca scientifica e statistica, purché nei soli termini generali previsti dal Regolamento;
e) **selettività e minimizzazione dei dati**: i dati raccolti devono poter tracciare i contatti stretti e non i movimenti o l'ubicazione del soggetto. Devono essere raccolti solo i dati strettamente necessari ai fini della individuazione dei possibili contagi, con tecniche di anonimizzazione e pseudonimizzazione affidabili. Anche la conservazione deve limitarsi al periodo strettamente necessario, da valutarsi sulla base delle decisioni dell'autorità sanitaria su parametri oggettivi come il periodo di incubazione.
A tal riguardo le disposizioni del Decreto su tali aspetti è opportuno che siano ulteriormente articolate in sede di attuazione dal Ministero della salute ai sensi del comma 2 del Decreto stesso.
In particolare si fa riferimento alla sorte dei dati raccolti sul dispositivo di chi, in un momento successivo all'installazione dell'applicazione, abbia poi **deciso di disinstallarla;**
f) non esclusività del processo algoritmico e possibilità di esercitare in ogni momento i diritti di cui agli articoli da 15 a 22 del Regolamento;
g) interoperabilità con altri sistemi di contact tracing utilizzati in Europa. Tali caratteristiche di interoperabilità potranno essere assicurate in sede applicativa e, ancor prima, nell'ambito dei provvedimenti di competenza del Ministero;
h) reciprocità di anonimato tra gli utenti dell'app, i quali devono peraltro non essere identificabili dal titolare del trattamento, dovendo la identificazione ammettersi al limitato fine dell'individuazione dei contagiati
La norma, al comma 2 lettera e) del Decreto, non specifica infatti chiaramente se si intenda optare per la conservazione dei dati in forma centralizzata ovvero decentrata.
Infatti la norma afferma che "dati relativi ai contatti stretti siano conservati, anche nei dispositivi mobili degli utenti, per il periodo strettamente necessario al trattamento, la cui durata è stabilita dal Ministero della salute e specificata nell'ambito delle misure di cui al presente comma".
In ogni caso, la centralizzazione richiederebbe in sede attuativa la previsione di misure di sicurezza rafforzate, adeguate alla fattispecie.

Alla luce delle considerazioni sopra esposte, deve ritenersi ammissibile l'utilizzo del **contact tracing** per fornire alle autorità sanitarie dati utili per il contenimento del contagio.
Tuttavia, devono sempre essere utilizzate tecniche in grado di garantire l'anonimato e, solo qualora ciò non fosse possibile, predisporre un sistema di garanzie adeguate.
In ogni caso, gli Stati membri devono **agire nel rispetto** d**el principio di proporzionalità**, mediante l'impiego di tecniche meno intrusive possibili.
Soltanto in tal modo potrà essere garantita nel delicato contesto attuale la tutela dei dati personali degli interessati.
NOTE
EDPB, Dichiarazione sul trattamento dei dati personali nel contesto dell'epidemia di COVID-19 del 19 marzo 2020, www.garanteprivacy.it
EDPB, Dichiarazione sul trattamento dei dati personali nel contesto dell'epidemia di COVID-19 del 19 marzo 2020, www.garanteprivacy.it