La legittimità dei sistemi di "*contact tracing*", volti a prevenire la diffusione del Covid-19, secondo l'attuale normativa sulla protezione dei dati personali (GDPR)

Come noto, i sistemi di "*contact tracing*" nell'ambito della pandemia da Covid-19 vengono utilizzati per tracciare il contatto tra persone in modo che, se una di esse dovesse risultare infetta dal virus, è possibile ricostruire la catena di contatti avvenuta nel periodo precedente. Questi sistemi, dunque, possono essere utili a gestire le epidemie del virus a livello localizzato, individuando ed isolando i soggetti eventualmente venuti in contatto con l'infetto, prevenendo l'insorgere di focolai.

Il Comitato Europeo per la Protezione dei dati Personali (c.d. EDPB), nelle proprie "*Linee-guida 04/2020 sull'uso dei dati di localizzazione e degli strumenti per il tracciamento dei contatti nel contesto dell'emergenza legata al Covid-19*" adottate il 21 aprile 2020, ha chiarito che le condizioni e i principi per l'uso proporzionato dei dati di localizzazione degli strumenti di tracciamento dei contatti, avviene 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.

Il Comitato, tuttavia, aggiunge che: "*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*".

Il Comitato ritiene che le autorità sanitarie nazionali possano essere titolari di tale trattamento, ma si possono comunque prendere in considerazione altre configurazioni di titolarità.

L'EDPB, infine, ricorda che l'uso delle applicazioni di tracciamento dei contratti si basa sul trattamento di dati personali pseudonimizzati degli utenti delle applicazioni.

È dunque chiaro l'indirizzo del Garante Privacy Europeo sui sistemi di tracciamento.

Passando al quadro normativo italiano sulla protezione dei dati personali, si può affermare che non sussistono divieti espliciti sull'utilizzo di questi sistemi.

Pertanto, non potendo ricorrere ad indicazioni legislative specifiche, occorre far riferimento a

quanto affermato dal Garante per la Protezione dei Dati Personali, che ha manifestato il proprio indirizzo interpretativo in più occasioni, in maniera tuttavia piuttosto contraddittoria.

Innanzitutto si riporta quanto ha dichiarato la suddetta Autorità nella F.A.Q. – riportata nel paragrafo intitolato "*Trattamento dei dati nel contesto lavorativo pubblico e privato nell'ambito dell'emergenza sanitaria*"[1] – che, rispondendo alla seguente domanda: "*Sono utilizzabili applicativi con funzionalità di "contact tracing" in ambito aziendale?*", afferma: "*La funzionalità di "contact tracing", prevista da alcuni applicativi al dichiarato fine di poter ricostruire, in caso di contagio, i contatti significativi avuti in un periodo di tempo commisurato con quello individuato dalle autorità sanitarie in ordine alla ricostruzione della catena dei contagi ed allertare le persone che siano entrate in contatto stretto con soggetti risultati positivi, e disciplinata unicamente dall'art. 6, d.l. 30.4.2020, n. 28*"[2].

La norma di legge appena richiamata, si riferisce al sistema di allerta denominato "Immuni", la cui realizzazione è stata autorizzata dallo Stato al fine di prevedere al livello nazionale un sistema di allerta Covid-19. Detta applicazione utilizza la tecnologia per avvertire colui che si è trovato a stretto contatto con un utente risultato positivo al virus del Covid-19, inviandogli una notifica che lo informa del potenziale rischio di essere stato contagiato. Questo avviene senza raccogliere dati sull'identità o la posizione dell'utente.

Nel medesimo paragrafo, alla domanda "*Al fine di contenere il rischio di contagio sul luogo di lavoro sono disponibili applicativi che non trattano dati personali?*", il Garante Privacy risponde:

"*Sì, il datore di lavoro può ricorrere all'utilizzo di applicativi, allo stato disponibili sul mercato, che non comportano il trattamento di dati personali riferiti a soggetti identificati o identificabili. Ciò nel caso in cui il dispositivo utilizzato non sia associato o associabile, anche indirettamente (es. attraverso un codice o altra informazione), all'interessato né preveda la registrazione dei dati trattati*"[3].

Dalla lettura delle citate F.A.Q. sembrerebbe che, in ambito lavoristico, non ci sia spazio per altri sistemi di tracciamento, diversi da "Immuni". Il dilemma si inserisce nel contesto molto delicato della responsabilità dei datori di lavoro, stretti tra due fuochi: da un lato hanno l'obbligo di garantire l'integrità psico-fisica del lavoratore; dall'altro devono rispettare la normativa sulla privacy. Secondo parte della dottrina[4], pertanto, per utilizzare le App di tracciamento ci vorrebbe una legge che lo autorizzi, ovvero il fondamento normativo (che allo stato è costituito esclusivamente dall'art. 6 del D.L. n. 28/2020, che disciplina per l'appunto il sistema "Immuni").

Tuttavia, lo stesso Garante Privacy lascia intendere un diverso approccio sulla possibilità di utilizzare sistemi di tracciamento in altri indirizzi interpretativi, pubblicati sul sito internet istituzionale ww.garanteprivacy.it.

Si fa riferimento in particolare alla F.A.Q. riportata nel paragrafo intitolato "*App nazionale di contact tracing e App regionali per Covid-19*" che risponde alla domanda:

"*Quale è la base giuridica delle altre App, diverse da quelle di telemedicina, utilizzate per il contrasto al Covid 19?*", secondo cui: "*Premesso che le App di tracciamento devono avere una adeguata base normativa e rispettare i*

*criteri già definiti a livello nazionale, le App, volte a fornire servizi diversi dalla telemedicina o comunque non strettamente necessari alla cura (App divulgative; App per la raccolta di informazioni sullo stato di salute della popolazione di un dato territorio), che comportino il trattamento di dati personali, **possono essere utilizzate, in linea generale, solo previo consenso libero, specifico, esplicito e informato dell'interessato** (cfr. provvedimento del 7 marzo 2019 - doc. web n. 9091942)"* [5].

Inoltre, va considerata la risposta fornita alla successiva F.A.Q.: "*Come devono essere configurate le App per assicurare il rispetto dei principi di privacy by design e privacy by default?*, secondo cui: "*Le App devono trattare solamente i dati strettamente necessari a perseguire le finalità del trattamento evitando di raccogliere dati eccedenti (es. quelli relativi all'ubicazione del dispositivo mobile dell'utente) e limitandosi a richiedere permessi per l'accesso a funzionalità o informazioni presenti nel dispositivo, solo se indispensabili.*

Anche nella pagina di presentazione delle suddette F.A.Q., si legge: "*Per l'utilizzo di app diverse da quelle di telemedicina (quali, ad esempio, app divulgative o app per la raccolta di informazioni sullo stato di salute della popolazione di un dato territorio), è necessario invece il consenso dell'interessato, il quale deve essere adeguatamente informato sull'uso che verrà fatto dei suoi dati. L'Autorità ha inoltre sottolineato che le app devono trattare solamente i dati strettamente necessari a perseguire le finalità del trattamento, evitando di raccogliere dati eccedenti (ad esempio, quelli relativi all'ubicazione del dispositivo mobile dell'utente) e limitandosi a richiedere permessi per l'accesso a funzionalità o informazioni presenti nel dispositivo solo se indispensabili*"[7].

Dal dato letterale di queste risposte ufficiali del Garante Privacy, emerge con chiarezza – sebbene in forza di una interpretazione ermeneutica – che:

- **possono essere utilizzate altre App di tracciamento**, ivi comprese quelle regionali;
- l'App "Immuni" non è l'unico sistema di tracciamento contemplato dal mercato;
- le App di tracciamento devono avere una adeguata base normativa e rispettare i criteri già definiti a livello nazionale[8];
- dette App possono essere utilizzate solo previo "consenso" dell'interessato[9], che costituisce così la base giuridica del trattamento dei dati connesso all'utilizzo del dispositivo;
- non si possono utilizzare dati relativi all'ubicazione dell'utente;
- non si possono utilizzare informazioni presenti sul dispositivo, se non quelle strettamente necessarie al relativo utilizzo.

Anche il Presidente del Garante per la Protezione dei Dati Personali, Antonello Soro – con riferimento alla polemica sorta con sistemi di tracciamento proposti da alcune Regioni – ha dichiarato in una recente intervista pubblicata su *La Repubblica* che: "*Nel nostro ordinamento ora esiste un principio di* "accountability", *di responsabilità, per cui chi mette in piedi sistemi di tracciamento deve fare una valutazione di impatto che il Garante valuterà, anche nel prossimo futuro. Se la valutazione non è stata fatta su misura dei rischi, interverremo*" [10].

L'Autorità pertanto non esclude affatto la possibilità che vi siano dei sistemi di tracciamento diversi da Immuni, ma ne subordina la legittimità all'effettuazione della Valutazione di Impatto sulla Protezione dei Dati (c.d. "DPIA"[11]) ed al più generale principio di *accountability*[12]. Sono dunque da ritenersi legittime, a maggior ragione, i sistemi di tracciamento diversi dalle App, il cui funzionamento si basa su un minor utilizzo di dati personali.

Appare evidente che questi sistemi di tracciamento devono essere avulsi dall'utilizzo di particolari categorie di dati (dati sanitari nello specifico), che in ambito lavoristico hanno una disciplina specifica e diversa base giuridica.

Non a caso si fa riferimento a "tracciamento di contatti", e non tracciamento di persone (tantomeno di lavoratori), senza che vi sia trattamento di alcun dato sulla salute degli interessati. L'eventuale insorgenza di casi Covid-19, infatti, non è connessa all'utilizzo in sé del sistema di tracciamento, che semmai sarà utilizzato esclusivamente per ricostruire la catena dei contatti, nell'ambito della gestione dell'emergenza epidemiologica e della tutela della salute nei luoghi di lavoro (con le conseguenze che ne derivano in termini di applicazione della specifica e differente normativa).

In ogni caso, nel contesto di un sistema 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*). Quindi non soltanto si deve far riferimento ai principi di liceità, finalità e necessità, ma assumono rilievo i principi di proporzionalità, **m**inimizzazione e conservazione dei dati.

In questo senso si suggerisce di affidare i dati ad un responsabile per il trattamento dei dati (esterno o interno all'azienda), preferibilmente **i**ndipendente, affinché non sussista una associazione diretta tra dispositivi e utilizzatori, e la soluzione del sistema di tracciamento risulti essere – almeno in prima battuta – completamente anonima (in termini di pseudonimizzazione). Solo qualora un utilizzatore risultasse positivo al Covid-19 si potrebbe risalire alla catena dei contatti di quest'ultimo al sol fine di informare gli interessati di un rischio più elevato di contagio (essendo stati in contatto con un caso di infezione accertato) affinché essi possano procedere a verifiche più approfondite sul proprio stato di salute e/o utilizzare maggiore prudenza nella socialità.

I dati trasmessi dal sistema di tracciamento dovrebbero includere solo identificatori univoci e pseudonimi, generati dal sistema e specifici a tale funzione. Tali identificatori devono essere rinnovati regolarmente, secondo una frequenza compatibile con lo scopo di contenere la diffusione del virus e limitare il rischio di identificazione e di localizzazione fisica delle persone[13].

Le generalità dell'infetto devono comunque rimanere nell'anonimato. Ugualmente, sarebbe opportuno che restino secretati e non rivelati neanche i soggetti che hanno avuto contatto con l'infetto: questi dati dovrebbero infatti essere messi a disposizione esclusivamente delle Autorità sanitarie.

L'utilizzo dei sistemi di tracciamento in ambito lavorativo, quindi, deve necessariamente coordinarsi con la disciplina prevista dalla normativa specifica[14].

In considerazione di quanto è emerso dall'esame del materiale giuridico sopra citato e degli attuali indirizzi interpretativi del Garante per la Protezione dei Dati Personali, si può desumere che i sistemi di tracciamento volti alla ricostruzione della catena dei contatti siano legittimi, nel rispetto delle condizioni sopra richiamate e nella consapevolezza che è compito dell'operatore garantire che ogni misura adottata in queste circostanze eccezionali sia necessaria, limitata nel tempo, di portata minima e soggetta ad un riesame periodico ed effettivo.

Note

[1] Pubblicata sul sito internet istituzionale del Garante Privacy e consultabile al seguente link: https://www.garanteprivacy.it/temi/coronavirus/faq#app; la pagina non ha una data precisa di pubblicazione e risulta in costante aggiornamento.

[2] Convertito in legge, con modificazioni, dall' art. 1, comma 1, Legge n. 70/2020.

[3] Si veda la nota 1.

[4] In tal senso Antonio Ciccia Messina, in un articolo intitolato *Stop alle app di tracciamento*, pubblicato su *ItaliaOggi* del 9 luglio 2020. *Nell'ambito delle relative valutazioni di impatto sarà, inoltre, necessario valutare attentamente, tra l'altro, la liceità e i rischi derivanti dall'eventuale trasferimento di dati a terze parti (es. social login, notifiche push, ecc.), soprattutto se stabilite al di fuori dell'Unione Europea*"[6].

[5] Pubblicata sul sito internet istituzionale del Garante Privacy e consultabili al seguente link: https://www.garanteprivacy.it/temi/coronavirus/faq#contact-tracing; la pagina non ha una data precisa di pubblicazione e risulta in costante aggiornamento.

[6] Pubblicata sul sito internet istituzionale del Garante Privacy e consultabili al seguente link: https://www.garanteprivacy.it/temi/coronavirus/faq#contact-tracing; la pagina non ha una data precisa di pubblicazione e risulta in costante aggiornamento.

[7] Pagina del 13 luglio 2020, consultabile sul sito internet istituzionale del Garante Privacy al seguente link: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9435552

[8] Si veda al riguardo l'art. 6 del D.L. n. 28/2020, che detta specifici accorgimenti per i sistemi di allerta Covid-19.

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

[10] Intervista a cura di Arturo Di Corinto, *La Repubblica*, 5 giugno 2020, pubblicata sul sito internet istituzionale del Garante Privacy e consultabile al link https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9359888.

[11] Art. 35 del GDPR.

[12] Il principio di *accountability*, infatti, impone al titolare del trattamento dei dati una gestione del dato responsabile che tenga conto dei rischi connessi alla specifica attività svolta e che sia idonea a garantire la piena conformità del trattamento dei dati personali ai principi sanciti dal GDPR e dalla legislazione nazionale. Il Titolare di un trattamento dati, dunque, non è più mero esecutore di un elenco di misure imposte ad una norma, ma diviene responsabile delle misure operative e tecniche che riterrà opportune, efficaci - e dunque adeguate al rischio della propria struttura - per salvaguardare i dati che tratta.

[13] In tal senso il Comitato Europeo per la Protezione dei dati Personali (c.d. EDPB), in "*Linee-guida 04/2020 sull'uso dei dati di localizzazione e degli strumenti per il tracciamento dei contatti nel contesto dell'emergenza legata al Covid-19*" adottate il 21 aprile 2020.

[14] Anche con riferimento al divieto di utilizzo dei sistemi di controllo a distanza dei lavoratori.