ANALISI

Covid-19 e geolocalizzazione: 3 soluzioni tecnologiche a prova di privacy

Prof. Avv. Emilio Tosi, Professore Associato Abilitato di Diritto Privato - Università degli Studi di Milano Bicocca Direttore Centro Studi Diritto delle Nuove Tecnologie® - 20 Marzo 2020

Geolocalizzazione anonima, big data e tracciamento movimenti personali per contrastare l'emergenza sanitaria Covid-19: ammissibilità e limiti inderogabili.
In questi giorni di distanziamento sociale e restrizione alla libertà di circolazione dei cittadini italiani, a causa dell'emergenza sanitaria Covid-19, è esploso il caso della sorveglianza sanitaria tramite geolocalizzazione mediante utilizzo di specifiche App su smartphone.

Sorveglianza finalizzata al controllo dell'ottemperanza in particolare, ma non esclusivamente, dell'isolamento domiciliare da parte dei positivi al virus.

Occorre, tuttavia, fare chiarezza tra i vari strumenti utilizzabili in astratto distinguendo tra quelli immediatamente applicabili a normativa vigente e a quelli ulteriormente ammissibili in caso di approvazione di nuove norme ad hoc nel quadro costituzionale dei principi invalicabili, anche in emergenza, del rispetto della dignità della persona e non semplicemente della riservatezza personale.
Il diritto alla riservatezza e alla protezione dei dati è un diritto fondamentale della persona, un diritto di libertà, elastico: può, quindi, essere compresso in situazione di emergenza, nel rispetto dei fondamentali principi di bilanciamento degli interessi, proporzionalità, necessità, ragionevolezza, trasparenza e accountability.

Come il diritto alla privacy può essere compresso

Può, quindi, essere compresso – temporaneamente – per ragioni di salute pubblica, come previsto dall'articolo 16 del GDPR e dall'art.15 della direttiva ePrivacy.

La soluzione della Regione Lombardia è a prova di privacy

Sgombriamo subito il campo da un dubbio che ha turbato i cittadini lombardi nei giorni scorsi: siamo sorvegliati a distanza dalle autorità regionali?

La risposta è negativa: tale attività di controllo virtuale degli spostamenti individuali delle persone – allo stato della normativa vigente – non sarebbe certo possibile e nemmeno è stata effettuata come ampiamente precisato dal Governatore Fontana, che in quanto avvocato è uomo di diritto ben attento al rispetto delle regole giuridiche.

La Regione Lombardia – modello operativo di gestione eccellente dell'emergenza – si è solo, opportunamente attivata, considerata la situazione sanitaria drammatica, per monitorare in forma anonima e aggregata i movimenti dei dispositivi mobili di comunicazione – i ben noti smartphone – nel pieno rispetto, quindi, della normativa vigente a tutela della sicurezza e della privacy individuale, come disposto dal General Data Protection Regulation e dal Codice della Privacy.

Stiamo parlando, quindi, di analisi di flussi di dati aggregati, rectius anonimi, si ribadisce.

Nessuna App di geolocalizzazione, dunque: almeno per ora si potrebbe dire vista l'evoluzione continua della normativa emergenziale che potrebbe, il condizionale è d'obbligo, mutare rapidamente per contrastare efficacemente l'epidemia in corso.

D'altra parte anche l'Organizzazione mondiale della sanità (Oms) ha sollecitato i governi sul punto: la chiusura di attività, scuole e aziende, il lockdown, non basta. Occorre incrementare l'analisi dei flussi informativi correlati alla diffusione del virus, anche attraverso lo strumento analitico del contact tracing: così ha dichiarato, nei giorni scorsi, il direttore generale dell'autorità, Tedros Adhamon Ghebreyesus.

Paesi come Cina, Corea del Sud, Taiwan, Hong Kong e Singapore hanno proprio fatto affidamento, seppure con modalità e invasività differenti, sui dati per contenere il contagio da coronavirus. Non sono mancati, tuttavia, effetti collaterali di ostracismo sociale in danno dei contagiati e dei soggetti positivi al virus, ulteriori rispetto a quelli legittimamente attesi dell'osservanza del doveroso isolamento domiciliare. Luci e ombre della geolocalizzazione sanitaria, si potrebbe dire.

La prima scelta tecnologica compatibile con il GDPR è l'analisi dei big data

La prima scelta tecnologica compatibile con il GDPR – a regole invariate – da attuare

subito è, dunque, quella dell'analisi di big data relativi alla circolazione, compresi dati di geolocalizzazione anonima tramite celle telefoniche, smartphone e GPS.

Sappiamo quante persone si trovano in un dato luogo in quel momento ma non sappiamo chi: big data analytics applicata efficacemente ai dati di mobilità delle persone non al controllo degli spostamenti individuali di Tizio e Caio.

Ma anche senza smartphone, ci sono molti altri strumenti per monitorare, in forma anonima e aggregata, al fine di mitigare il contagio, movimenti delle persone e contatti sociali, ricorrendo al GPS dei veicoli come pure al data mining dei social network.

Non a caso Facebook ha lanciato subito il progetto Data for good mettendo a disposizione data set utili per studiare la diffusione del coronavirus, comprensivi di dati – anonimi e non identificabili – sulla mobilità e mappe sulla densità della popolazione per analizzare la diffusione del virus.

Limitatamente alla big data analysis della mobilità, in particolare tramite geolocalizzazione anonima, si ritiene, quindi, che possa bastare un'ordinanza della Protezione Civile esecutiva dell'art.14 del D.L. 9/3/2020 citato, per partire immediatamente.

La seconda scelta compatibile a norme invariate

La seconda scelta compatibile a norme invariate e semplice ordinanza esecutiva della Protezione Civile: raccolta dati geolocalizzazione smartphone con il consenso degli interessati e altri dispositivi digitali nei 14 giorni anteriori al rilievo della positività al virus. Sostituire, quindi, il tracciamento cartaceo degli spostamenti autodichiarati, obsoleto nella società dell'informazione e necessariamente lacunoso, in alcuni casi, persino omissivo, con quello dei dati delle celle telefoniche e dei GPS del soggetto interessato.

Terza scelta con nuove regole

Terza scelta che richiede, invece, nuove regole, in deroga alle norme ordinarie del GDPR, ulteriori rispetto a quelle già introdotte dall'art. 14 del D.L. 9/3/2020 dovrà riguardare la disciplina delle App di sorveglianza personalizzata dei contagiati e positivi al virus, rectius geolocalizzazione della singola persona, non più, quindi, in forma aggregata e anonima, attivando anche alert di geofencing che avvisino le autorità competenti in caso di violazione dell'isolamento prescritto ai positivi al Covid-19.

La fattibilità tecnologica è già stata sperimentata, con diversi gradi di invasività nella sfera personale, in Cina e in Corea. Tuttavia, come noto, non tutto ciò che la tecnologia consente di fare è ammissibile dal punto di vista giuridico. Ricordiamoci che occorre operare nel quadro delle regole comunitarie delineate dal GDPR e dal

nostro Codice della Privacy oltre che più in generale della nostra Costituzione e dei Trattati comunitari.

Si ricorda, in proposito, che la Direttiva 58/2002, disciplinante il trattamento dei dati personali nel settore delle comunicazioni elettroniche, si applica al trattamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazione (art. 3.1 Direttiva 58/2002), quindi anche ai dati di geolocalizzazione di smartphone e GPS.

Tale Direttiva richiede necessariamente il consenso dell'interessato per il trattamento dei dati relativi alla geolocalizzazione, diversamente gli stessi possono essere trattati solo in forma anonima.

L'utilizzo dei dati riconducibili a ciascun cittadino, al di fuori di questi casi, è consentito unicamente per esigenze straordinarie, come quelle che stiamo vivendo, ma occorre espressa norma di legge ai sensi dell'art. 15 della citata direttiva e-privacy.

A mio prudente avviso, a normativa vigente, non è, quindi, possibile tracciare e geolocalizzare – in forma individuale e non aggregata – i cittadini legittimamente senza il consenso degli interessati, così attivando un tracciamento individuale, una sorta di pedinamento virtuale.

Si potrebbe d'ufficio, solamente se intervenissero modifiche in sede di conversione dell'art. 14 del D.L. 9/3/2020 con l'introduzione di specifiche regole e garanzie per l'ammissibilità di tale procedura invasiva di controllo.

Detta norma emergenziale contiene già un'ampia deroga al GDPR, a partire dalla raccolta del consenso dell'interessato, per una più efficace gestione dei flussi di trattamento dei dati sanitari e dell'interscambio di dati personali, possono effettuare trattamenti, ivi inclusa la comunicazione tra loro, dei dati personali, anche relativi agli articoli 9 e 10 del regolamento (UE) 2016/679, che risultino necessari all'espletamento delle funzioni attribuitegli nell'ambito dell'emergenza determinata dal diffondersi del COVID-19.

Ma tale norma non basta in quanto non disciplina espressamente la specifica misura di controllo delle persone di cui trattasi, ma il trattamento dei dati personali in deroga al GDPR.

È certamente doveroso facilitare il trattamento e lo scambio di dati epidemiologici in contesto di emergenza. Le regole non devono essere di ostacolo ma i principi vanno salvati. Un conto è facilitare al massimo trattamento e circolazione dei dati sanitari; altro introdurre meccanismi di sorveglianza sanitaria con geolocalizzazione delle persone, non

in forma anonima.

Si potrebbe, forse, il condizionale è d'obbligo, considerare proporzionale un tale trattamento rispetto ai soggetti contagiati o risultati positivi virus al fine di assicurare il rispetto della quarantena domiciliare e del distanziamento sociale.

Dubito, tuttavia, che lo stesso giudizio positivo di proporzionalità, anche in caso di emergenza, possa essere esteso alla geolocalizzazione indiscriminata di tutti i cittadini italiani.

Il parere dell'EDPB

Nello stesso senso il parere di Andrea Jelinek, presidente EDPB : "For the processing of electronic communication data, such as mobile location data, additional rules apply. The national laws implementing the ePrivacy Directive provide for the principle that the location data can only be used by the operator when they are made anonymous, or with the consent of the individuals. The public authorities should first aim for the processing of location data in an anonymous way (i.e. processing data aggregated in a way that it cannot be reversed to personal data). This could enable to generate reports on the concentration of mobile devices at a certain location ("cartography"). When it is not possible to only process anonymous data, Art. 15 of the ePrivacy Directive enables the member states to introduce legislative measures pursuing national security and public security. This emergency legislation is possible under the condition that it constitutes a necessary, appropriate and proportionate measure within a democratic society".

Così anche si esprime anche il Garante italiano Antonello Soro che pone un limite al tracciamento di massa delle persone. "Mi sfugge l'utilità di una sorveglianza generalizzata alla quale non dovesse conseguire sia una gestione efficiente e trasparente di una mole così estesa di dati, sia un conseguente test diagnostico altrettanto generalizzato e sincronizzato". E ancora Soro invita giustamente a non "cedere alla tentazione della scorciatoia tecnologia solo perché apparentemente più comoda, ma valutando attentamente benefici attesi e 'costi', anche in termini di sacrifici imposti alle nostre libertà".

Il Parlamento in sede di conversione del D.L. 9/3/2020, potrà, quindi, introdurre, in relazione a persone contagiate e positive al virus, norme per la geolocalizzazione individuale nel rispetto dei generali principi di proporzionalità, necessità, trasparenza, accountability e sicurezza per un limitato periodo di tempo da stabilire espressamente e prevedendo una clausola di salvaguardia che preveda obbligo di cessazione del controllo stesso con cancellazione obbligata ai termini dell'emergenza,

affidando la gestione e la sicurezza dei dati alla competenza esclusiva della Protezione Civile e la vigilanza di conformità al Garante per la Protezione dei Dati personali.

Dubito che misure non circostanziate ma estese al tracciamento personale, non semplicemente anonimo e aggregato, di tutti gli italiani possa, senza difficoltà, anche in situazione di emergenza, superare indenne i rilievi specifici del Garante Privacy e quelli più generali di costituzionalità.

Nelle situazioni di emergenza si possono e si devono derogare le regole ordinarie per il bene superiore di tutti. Ma non è mai opportuno rinunciare a preservare i principi fondamentali e le libertà dell'ordinamento costituzionale che devono sempre essere difese anche nelle condizioni più avverse.

Tra l'altro la durata del trattamento per finalità di sorveglianza sanitaria in deroga alle regole ordinarie potrebbe avere – il condizionale è d'obbligo – un'estensione più lunga del previsto non inferiore a 12 mesi, forse 24 mesi, stando alle recenti previsioni epidemiologiche: necessità di controllo emergenziale che verosimilmente cesserà solamente con la vaccinazione di massa, quando questa sarà disponibile sul mercato.

Occorre, in conclusione, in questi giorni drammatici, evitare il "fai da te" e affidare ogni inziativa tecnologica alla regia esclusiva della Protezione Civile – in forza dell'ampia delega alla gestione dell'emergenza contenuta nel DL citato – dalla messa a punto, all'approvazione dell'utilizzo di App già esistenti sino alla gestione della banca dati di sorveglianza sanitaria che tali dati raccoglierà e analizzerà.

Da subito si potrà procedere al controllo dei movimenti, in forma aggregata e anonima, dei residenti nelle aree di contagio e – in caso di nuove regole introdotte dal Parlamento in sede di conversione in legge – anche dei movimenti personali dei soggetti individuati e positivi al Covid-19: pur sempre con modalità rispettose della dignità della persona e delle norme fondamentali della nostra Costituzione.

Occorre massima prudenza al fine di escludere passi irreversibili affrettati ed effetti collaterali indesiderati nei confronti dei contagiati e dei soggetti positivi al virus: si eviti attentamente, con ogni mezzo, il possibile rischio sociale, indesiderato e deprecabile, di colonna infame digitale.