CORONAVIRUS
OVERCOMING THE DIFFICULTIES

BIG DATA E GEOLOCALIZZAZIONE NEL CONTRASTO ALLA DIFFUSIONE DI COVID-19: NUOVE SFIDE NELLA PROTEZIONE DEI DATI PERSONALI

DE BERTI JACCHIA FRANCHINI FORLANI
STUDIO LEGALE

Con il prolungarsi del periodo di quarantena e il continuo evolversi delle misure di sicurezza e prevenzione adottate dal Governo nel fronteggiare l'emergenza sanitaria causata dalla diffusione di Covid-19, non è di certo passato inosservato il caso della Regione Lombardia, che ha dichiarato di aver monitorato e analizzato gli spostamenti dei cittadini mediante i loro dispositivi cellulari.

La notizia, naturalmente, ha destato non poche perplessità e preoccupazioni, specialmente per quanto riguarda il rispetto e la tutela della privacy dei cittadini italiani che, inevitabilmente, deve fare i conti con la più sentita esigenza di tutelare il loro diritto alla salute. Alcuni hanno interpretato l'adozione di questa misura come un primo passo verso l'adozione di misure simili a quelle implementate da Cina e Corea del Sud.

In realtà, l'attività di controllo sugli spostamenti messa in piedi dalla Regione Lombardia è una misura molto meno invasiva e lesiva dei diritti di libertà dei cittadini di quanto si possa pensare, ben lontana dai sopra citati modelli.

La tecnologia che sta dietro al monitoraggio degli spostamenti dei cittadini fa leva sull'utilizzo delle celle telefoniche. Più in dettaglio ricordiamo come una rete di telecomunicazioni sia composta da molte celle, ognuna delle quali "alimenta" il segnale che i nostri telefoni cellulari agganciano, tramite le antenne o i ripetitori collocati sul territorio, per assicurarci la migliore copertura di rete disponibile.

Il principio con cui avviene il tracciamento degli spostamenti è molto semplice: quando un utente si trova in una determinata zona, il suo cellulare è collegato a una cella, che gli restituisce il segnale con una certa intensità. Quando lo stesso utente si muove, allontanandosi da quella cella, il segnale diviene sempre più debole finché non viene superato per intensità da quello di un'altra cella confinante, a cui il telefono cellulare si aggancia. Gli operatori delle compagnie telefoniche conservano tali dati in forma aggregata e anonima: ciò significa che, teoricamente, non è possibile risalire al fatto che un utente individualmente identificato, a cui è collegato un determinato telefono cellulare, si è spostato da una zona a un'altra. Risulterà, invece, che in una determinata area gli spostamenti sono stati effettuati da un certo numero di persone.

Questo tipo di tracciamento, come detto in forma anonima e aggregata non costituisce trattamento di dati personali in quanto, com'è evidente, si tratta di un'attività che non è riferibile a persone singolarmente identificabili bensì a una collettività di persone.

Alcune compagnie telefoniche hanno messo a disposizione della Regione Lombardia i dati relativi all'ubicazione dei dispositivi telefonici. Questo *modus operandi* ha reso quindi possibile, mediante l'analisi delle variazioni di cella dei telefonini, ricostruire con una certa approssimazione il tasso e il raggio degli spostamenti effettuati sul territorio lombardo, da cui è risultato che, nonostante i movimenti dei cittadini fossero consentiti solo in casi limitati, gli stessi fossero diminuiti solo del 60%. Tale trasmissione sarebbe avvenuta in forma aggregata e anonima e, quindi, non in violazione delle disposizioni di legge in tema di tutela dei dati personali.

Il Garante per la Protezione dei Dati Personali, in una recente intervista al suo presidente Antonello Soro, si è espresso favorevolmente all'impiego delle tecnologie per contrastare il diffondersi del contagio, ma non senza adeguate garanzie per i cittadini. Il Garante ha ricordato come le attività di trattamento dei dati personali devono essere sempre ispirate ai principi di necessità, proporzionalità e minimizzazione. Il Garante in tale occasione ha altresì rilevato che alcune proposte di tracciamento massivo dei cittadini, ispirate alle esperienze di Cina e Corea del Sud, come il monitoraggio costante degli spostamenti 24 h su 24, secondo il Garante, non risponderebbero ai canoni di proporzionalità e necessità sopra indicati, vista la mole di dati che verrebbe raccolta e l'impossibilità di realizzare in sincrono con tale raccolta dei mirati controlli diagnostici. I dati risulterebbero poi inutili, poiché allo stato attuale, sebbene esista un sostanziale obbligo alla permanenza domiciliare, non esiste un divieto assoluto di spostamento e, in definitiva, le informazioni raccolte non risponderebbero a una efficace logica di monitoraggio. Il Garante ha chiarito poi come non si possa guardare ai modelli di Cina e Corea del Sud come riferimenti a cui ispirarsi: in questi due paesi sono state adottate misure di monitoraggio sistematico e su larga scala difficilmente accettabili in un contesto come quello del nostro stato.

Basti pensare che sono state implementate *app* in grado di rilevare e pubblicare in tempo reale gli spostamenti di soggetti contagiati dal Covid-19: in Cina, le medesime *app* precludevano ai cittadini considerati "a rischio" l'accesso ad aree pubbliche, allertando gli altri del potenziale contatto con soggetti contagiati. È evidente che tali attività, da un lato, hanno avuto il pregio di ridurre e contrastare il contagio e il diffondersi del virus, grazie anche all'intervento dei colossi cinesi e coreani della tecnologia e alla loro analisi dei *big data,* rilevati e raccolti da ogni fonte disponibile (*app* sulla salute, geolocalizzazione, ecc…). Dall'altro lato è tuttavia palese la portata discriminatoria e preclusiva, nei confronti dei soggetti interessati e delle loro libertà, che simili misure possono avere.

Come si spiegherà meglio *infra*, tale impostazione è stata in parte superata dall'aggravarsi della situazione relativa alla diffusione del Covid-19, che ha reso non così remota la possibilità che anche in Italia siano introdotte, seppur con le necessarie garanzie, tecnologie analoghe a quelle adottate nei paesi asiatici.

L'*European Data Protection Board* ha recentemente chiarito, nello "*Statement on the processing of personal data in the context of the COVID-19 outbreak"* del 19 Marzo scorso, che, qualora non fosse possibile trattare i dati di geolocalizzazione degli interessati in forma anonima e aggregata, spetterebbe alla legislazione dei singoli stati membri stabilire le misure appropriate (e le adeguate garanzie per i soggetti interessati dal trattamento) per salvaguardare la sicurezza pubblica e, al tempo stesso, la privacy dei cittadini. In altri termini, nel delicato bilanciamento tra privacy e sicurezza, la situazione emergenziale giustifica un allentarsi dei divieti inerenti a trattamenti dei dati considerati, di per sé, invasivi e potenzialmente rischiosi per gli interessati. L'allentarsi dei divieti di trattamento di categorie di dati particolari e l'adozione di misure di controllo più stringenti deve avvenire senza perdere di vista tuttavia il valore e la delicatezza delle informazioni che vengono in tale sede trattate.

In questo senso, il Garante italiano si è espresso riferendo che "*non esistono preclusioni assolute nei confronti di determinate misure in quanto tali. Vanno studiate però molto attentamente le modalità più opportune e proporzionate alle esigenze di prevenzione, senza cedere alla tentazione della scorciatoia tecnologica solo perché apparentemente più comoda, ma valutando attentamente benefici attesi e "costi", anche in termini di sacrifici imposti alle nostre libertà"*. Il Garante non ha nemmeno osteggiato un possibile coinvolgimento dei big dell'*hi-tech* (Google e Facebook, per citarne alcuni), chiarendo che il coinvolgimento di tali colossi nelle attività di contrasto alla diffusione del virus non dovrà tradursi in un'ulteriore opportunità di acquisizione indiscriminata di dati da parte di tali società, ma dovrà essere limitato nel tempo e nella misura necessaria in relazione all'evolversi della situazione.

L'art. 76 del Decreto Cura Italia del 17 marzo scorso prevede che il Governo si avvalga, per far fronte alla situazione di emergenza, di un contingente di esperti per studiare soluzioni innovative, tecnologiche e di digitalizzazione che possano aiutare nella lotta contro il Covid-19.

Sotto questo profilo, i tre Ministeri proponenti dell'iniziativa "*Innova per l'Italia*" (il Ministero dello Sviluppo Economico, il Ministero dell'Istruzione, dell'Università e della Ricerca e il Ministero per l'Innovazione Tecnologica e la Digitalizzazione) hanno lanciato, congiuntamente al Ministero della Salute, Istituto Superiore di Sanità, Organizzazione Mondiale della Sanità e un comitato scientifico interdisciplinare una prima "*call for contributions"* di tre giorni (dal 24 al 26 marzo) al mondo dell'impresa e della ricerca. L' obiettivo è di individuare le migliori soluzioni digitali disponibili, non solo con riferimento ad app di telemedicina e assistenza domiciliare dei pazienti, ma anche con riferimento a "*tecnologie e soluzioni per* ***il tracciamento continuo, l'alerting e il controllo tempestivo*** *del livello di esposizione al rischio delle persone e conseguentemente dell'evoluzione dell'epidemia sul territorio*". Tra i requisiti per la partecipazione delle imprese è indicato che deve trattarsi di "*proposte già realizzate e disponibili per l'implementazione in tempi estremamente brevi e compatibili con l'emergenza*".

Si apre, dunque, la strada all'introduzione nel breve periodo anche nel nostro Paese di tecnologie di "*digital contact tracing".* Si tratta di tecnologie che consentono, similmente a quanto previsto in Corea del Sud e Cina, attraverso l'installazione di app sui telefoni cellulari, di mappare e tracciare gli spostamenti dei soggetti infetti e di coloro che sono entrati in contatto con questi ultimi. In altre parole, tali tecnologie dovrebbero ricostruire la rete di contatti dei contagiati, consentendo di intervenire tempestivamente a disporre la quarantena. Naturalmente, l'implementazione e l'utilizzo di tale tecnologia pone rilevanti questioni in materia di privacy, non trattandosi più del mero utilizzo di dati in forma aggregata.

In una recentissima intervista, il Garante per la Protezione dei Dati Personali ha cominciato a delineare quali potrebbero essere i "paletti" nell'uso delle tecnologie di *digital contact tracing*. In via preliminare, il Garante ha rilevato che, al fine di garantire la liceità del trattamento è necessario un intervento legislativo *ad hoc*, anche sotto forma di decreto-legge ove sia indispensabile salvaguardare le ragioni di urgenza. Il Garante, evidentemente, non ritiene sufficiente per giustificare trattamenti mediante tecnologia di *digital contact tracing*, l'art. 14 del D.L. 9 marzo 2020 rubricato "*Disposizioni sul trattamento dei dati personali nel contesto emergenziale*", che consente, fino al termine dello stato di emergenza, alcuni trattamenti di dati personali per motivi di interesse pubblico nel settore della sanità pubblica e, in particolare, per garantire la protezione dall'emergenza sanitaria determinata dalla diffusione del Covid-19, da parte di determinati soggetti pubblici e privati.

La necessità di un intervento legislativo si pone naturalmente in linea con il Regolamento (UE) 2016/679 ("GDPR"). Sotto questo profilo, già l'*European Data Protection Board* nello "*Statement on the processing of personal data in the context of the COVID-19 outbreak"* aveva individuato quali basi giuridiche per analoghe tipologie di trattamento, quelle indicate all'art. 9 par. 2 lett. i) – il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, inclusa

la protezione da gravi minacce per la salute – e lett. c) – necessità di tutelare un interesse vitale dell'interessato o di un'altra persona giuridica (anche se tale previsione, considerata di carattere residuale, si applicherebbe solo qualora l'interessato si trovi nell'incapacità di esprimere un consenso). La base giuridica di cui all'art. 9 par. 2 lett. i) richiede espressamente che il trattamento avvenga sulla base del diritto dell'Unione o di quello di uno degli Stati membri, rendendo, dunque, necessario l'intervento legislativo richiamato dal Garante.

Vengono poi in rilievo i Considerando (46) e (54) del GDPR. Il Considerando (46) prevede espressamente che alcuni tipi di trattamento possono rispondere sia a rilevanti motivi di interesse pubblico sia agli interessi vitali dell'interessato, ad esempio "*se il trattamento è necessario … per tenere sotto controllo l'evoluzione di epidemie e la loro diffusione*". Il Considerando (54) del GDPR specifica poi che "*Il trattamento di categorie particolari di dati può essere necessario per motivi di interesse pubblico nei settori della sanità pubblica, senza il consenso dell'interessato*" e purché "*soggetto a misure appropriate e specifiche a tutela dei diritti e delle libertà delle persone fisiche*".

Sempre con riferimento ai trattamenti con tecnologia *digital contact tracing*, il Garante ha sottolineato la necessità di rispettare i principi della protezione dei dati fin dalla progettazione e per impostazione predefinita (*privacy by design* e *by default*) di cui all'art. 25 del GDPR, al fine di garantire che qualsiasi soluzione tecnologica adottata tenga conto sin dal principio della necessità di implementare idonee misure di sicurezza. Sotto questo profilo, viene senz'altro in rilievo l'utilizzo della pseudonimizzazione che consiste nel trattamento di dati personali che non possano più essere attribuiti ad un interessato specifico senza l'utilizzo di informazioni aggiuntive, le quali devono essere conservate separatamente e soggette a particolari misure di sicurezza. La pseudonimizzazione consentirebbe in questo caso di procedere alla re-identificazione del soggetto e alla ricostruzione della sua rete di contatti solo una volta che lo stesso sia stato trovato positivo al virus Covid-19.

In questo frangente, in cui potrebbe aumentare il numero di interessati che esercitino i loro diritti, un altro aspetto di potenziale interesse sembra essere quello relativo al termine entro il quale il Titolare del trattamento debba dare riscontro alle richieste degli interessati medesimi, di norma fissato in un mese dal ricevimento dalla richiesta. A tal proposito, qualora il titolare non sia in grado di dare riscontro alle richieste degli interessati in considerazione dello stato emergenziale in atto (ad es. qualora l'impresa fosse chiusa), si potrebbe ragionevolmente sostenere che il termine mensile suindicato sia prorogabile fino a tre mesi ai sensi dell'art. 12 del GDPR o, comunque, sospeso, o, infine, che l'eventuale impossibilità a dare riscontro sia ritenuta scusabile a causa dell'impossibilità determinata dall'epidemia in essere.

Ciò, tuttavia a condizione che lo stato di impossibilità che giustificherebbe il ritardo nella risposta sia oggettivo e possa essere documentato al di là di ogni ragionevole dubbio. È per questo che, qualora, durante lo stato emergenziale, il titolare continuasse normalmente nella sua attività, ivi inclusa quella di marketing, difficilmente potrebbe avvalersi di questa esimente.

Si ricorda, infine, relativamente ai procedimenti di fronte al Garante, l'applicabilità del disposto dell'art. 103 del c.d. Decreto Cura Italia che espressamente prevede che ai fini del computo dei termini ordinatori o perentori, propedeutici, endoprocedimentali, finali ed esecutivi, relativi allo svolgimento di procedimenti amministrativi su istanza di parte o d'ufficio, pendenti alla data del 23 febbraio 2020 o iniziati successivamente a tale data, non si tiene conto del periodo compreso tra la medesima data e quella del 15 aprile 2020.

Concludiamo dicendo che il diritto alla riservatezza e le libertà che ne conseguono in questo periodo cedono necessariamente il passo al diritto alla salute, ma – auspicabilmente – senza essere prevaricati del tutto e, soprattutto, definitivamente: alla cessazione dello stato di emergenza, la compressione dei diritti di libertà e riservatezza deve cessare di trovare

giustificazione nel superiore interesse pubblico alla salute e, da quel momento, deve venir meno, con pieno ristoro delle libertà previste dal nostro ordinamento.

Nel ricordare che la suesposta disamina è soggetta alla non improbabile adozione di misure normative e regolamentari future e che necessita di una validazione e verifica caso per caso, il nostro Studio è a disposizione dei propri clienti e di quanti vorranno a noi rivolgersi per avere chiarimenti con riferimento al rapporto tra il diritto alla protezione dei dati personali e l'impatto delle norme finalizzate a contenere la diffusione dell'epidemia da Covid-19.

27 marzo 2020

I nostri contributi di informazione e aggiornamento sulla crisi del Covid-19 e sulle sue implicazioni sono uno sforzo collettivo dello Studio ed una iniziativa di servizio. Per sottolinearlo, gli autori hanno rinunciato ad indicare il proprio nome in calce ai singoli lavori. Il presente articolo ha esclusivamente finalità informative e non costituisce parere legale.

Our contributions of information and update on the Covid-19 crisis and its implications constitute a collective effort of the Firm and an initiative of service. For such reason, the authors decided notto sign individually their works and articles.
This article is exclusively for information purposes, and should not be considered as legal advice.

MILANO
Via San Paolo, 7 · 20121 Milano, Italia
T. +39 02 72554.1 · F. +39 02 72554.400
milan@dejalex.com

ROMA
Via Vincenzo Bellini, 24 · 00198 Roma, Italia
T. +39 06 809154.1 · F. +39 06 809154.44
rome@dejalex.com

BRUXELLES
Chaussée de La Hulpe 187 · 1170 Bruxelles, Belgique
T. +32 (0)26455670 · F. +32 (0)27420138
brussels@dejalex.com

MOSCOW
Ulitsa Bolshaya Ordynka 37/4 · 119017, Moscow, Russia
T. +7 495 792 54 92 · F. +7 495 792 54 93
moscow@dejalex.com