# TESTO DELL'AUDIZIONE DEL PRESIDENTE DEL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

## L'uso delle nuove tecnologie a fini di contenimento dei contagi da Covid-19.
## Profili di protezione dei dati personali

### 1.Diritti, deroghe, limiti

La gravissima emergenza che il Paese sta affrontando ha imposto l'adozione- con norme di vario rango- di misure limitative di molti diritti fondamentali, necessarie per contenere auspicabilmente, il numero dei contagi.

La protezione dei dati personali – fondamentale diritto "di libertà", sancito dalla Carta di Nizza– non poteva fare, naturalmente, eccezione, benché le limitazioni sinora adottate siano nel complesso contenute.

Alcune deroghe al regime ordinario di gestione dei dati sono state previste sin dalle primissime ordinanze intervenute pochi giorni dopo la deliberazione dello stato di emergenza, con prevalente riferimento all'ambito di comunicazione dei dati sanitari.

L'art. 14 d.l. 14/2020 ha sostanzialmente replicato tale disposizione, elevandone la fonte e rimarcandone il carattere temporaneo, senza tuttavia allo stato attuale riferirsi a raccolte di dati particolarmente "innovative".

Nuove e più invasive raccolte di dati potrebbero fondarsi su esigenze di sanità pubblica che -al pari del "soccorso di necessità"- costituiscono autonomi presupposti di liceità, in presenza di una previsione normativa conforme ai principi di necessità, proporzionalità, adeguatezza, nonché del rispetto del contenuto essenziale del diritto.

## 2.Mappe epidemiologiche e sorveglianza

Va valutata entro questa cornice l'ipotesi della raccolta dei dati sull'ubicazione o sull'interazione dei dispositivi mobili dei soggetti risultati positivi, con altri dispositivi, al fine di analizzare l'andamento epidemiologico o per ricostruire la catena dei contagi.

Anzitutto, dal momento che sono ipotizzabili misure molto diverse tra loro, si dovrebbe privilegiare un criterio di gradualità e dunque valutare se le misure meno invasive possano essere sufficienti a fini di prevenzione epidemiologica.

In tale prospettiva non pone particolari problemi l'acquisizione di trend, effettivamente anonimi, di mobilità. L'art. 9 della direttiva e-privacy legittima il trattamento, anche in assenza del consenso dell'interessato, dei dati relativi all' ubicazione, purché anonimi.

Tale soluzione consente di realizzare, ad esempio, mappe descrittive dell'andamento dell'epidemia, utilissime a fini prognostici e statistici, meno a scopi diagnostici in senso proprio.

Per altro verso, l'uso di dati identificativi sull'ubicazione o sull'interazione con altri dispositivi può risultare funzionale a diversi scopi.

In ogni caso, esso richiede – anche ai sensi dell'art. 15 della direttiva e-privacy – una disposizione normativa sufficientemente dettagliata e contenente adeguate garanzie.

I vari utilizzi possibili di tali dati possono essere finalizzati, in via teorica (e ragionando nei termini assunti dal dibattito pubblico di queste settimane):

a) o alla verifica della posizione del soggetto sottoposto ad obbligo di permanenza domiciliare perché positivo, utilizzando dunque la geolocalizzazione del telefono (che si presuppone, ma non è detto, segua passo passo il soggetto**)** per accertare l'effettivo rispetto del divieto di allontanamento dal domicilio, oppure:

b) all'acquisizione, a ritroso, dei dati sull'interazione del soggetto poi risultato positivo con altri soggetti, per verificarne, nel periodo in cui aveva

capacità virale, gli eventuali contatti desumibili tramite varie tecniche: celle telefoniche, gps, bluetooth.

Le due ipotesi differiscono nella finalità: elemento, questo, indubbiamente rilevante per la valutazione della complessiva legittimità del trattamento.

La prima ipotesi infatti, nell'utilizzare la localizzazione del telefono come fosse una sorta di braccialetto elettronico atipico, presuppone la sostituzione, con l'occhio elettronico, dei controlli "umani", dando però per acquisito che chi decida di violare gli obblighi di permanenza domiciliare porti con sé il telefono, il che è evidentemente contro-intuitivo.

Tra le altre misure utilizzate a fini di verifica del rispetto degli obblighi di distanziamento sociale vi è il ricorso, da parte dell'autorità di pubblica sicurezza, ai droni.

Anche tali strumenti vanno utilizzati nel rispetto del canone di proporzionalità, soprattutto in ragione delle loro potenzialità particolarmente invasive della riservatezza.

Se utilizzata dalle forze di polizia, non per segnalare "impersonali" assembramenti, ma per monitorare il rispetto puntuale degli obblighi di permanenza domiciliare, infatti, tale misura difficilmente potrà garantire il rispetto del canone di proporzionalità, potendo prestarsi a una raccolta assai ampia di dati personali.

Sarebbe auspicabile, sul punto, una precisazione normativa, considerando anche che la norma di riferimento richiama genericamente le (non del tutto sovrapponibili) esigenze di controllo del territorio per finalità di pubblica sicurezza, contrasto del terrorismo e del crimine organizzato *(cfr. art. 5, c.3-sexies d.l, n. 7/2015, convertito, con modificazioni, dalla l. 43/2015, come novellato dal dl 113/2018, convertito con modificazioni dalla l. 132/2018*).

## 3.Il contact tracing

Più complessa è la seconda ipotesi, relativa alla mappatura a ritroso dei contatti tenuti, nel periodo d'incubazione, da soggetti risultati contagiati. Tale ricostruzione dei contatti può avvenire, almeno astrattamente, attraverso l'incrocio di tipologie di dati diversi: quelli sulle transazioni

commerciali, sulle celle telefoniche, quelli sull'interazione con altri dispositivi mobili desunti dal ricorso a tecnologie bluetooth.

Va premesso che ciascuna tipologia di questi dati ha, naturalmente, una diversa significatività a fini epidemiologici, tanto maggiore quanto più idonea a selezionare i contatti più rilevanti perché più ravvicinati e, dunque, maggiormente suscettibili di aver determinato, almeno potenzialmente, un contagio.

Come vedremo più avanti, la scelta della tipologia di dati più efficace incide anche sul complessivo giudizio di proporzionalità, in quanto la maggiore selettività riduce il perimetro di incidenza della misura al solo stretto necessario, con effetti socialmente apprezzabili in termini di tutela della salute, individuale e collettiva.

In termini generali, comunque, il fine perseguito da tale misura risulta particolarmente apprezzabile perché non già repressivo (come invece nel caso della sorveglianza del soggetto in quarantena obbligatoria mediante la sua geolocalizzazione), ma solidaristico.

Lo scopo perseguito coinciderebbe, infatti, con l'esigenza di sottoporre ad accertamenti quanti siano entrati potenzialmente in contatto con un soggetto risultato positivo al virus o, comunque, di adottare le misure utili a prevenire il contagio.

Si perseguirebbe, dunque, quella componente solidaristica del diritto alla salute quale interesse collettivo, valorizzata dalla giurisprudenza costituzionale sugli obblighi vaccinali.

L'utilizzo di tale tecnologia avrebbe, del resto, poche valide alternative ai fini della ricostruzione della catena epidemiologica.

La semplice intervista del paziente può essere, infatti, lacunosa o comunque scontare la mancata conoscenza di molti soggetti con i quali si possa essere entrati in contatto nei più vari contesti (in farmacia, al supermercato ecc.).

Un elemento di fragilità delle soluzioni basate sui dati acquisiti da telefono attiene, però, al suo presupporre che tutti si spostino con il telefono addosso. E se questo avviene quasi sistematicamente per le fasce più giovani della popolazione, non avviene altrettanto sicuramente per gli anziani, che

dovrebbero invece essere i primi a dover essere contattati in caso di temuto contagio, per essere curati con la massima tempestività.

Le soluzioni “tecnologiche” sono, infatti, validissime alleate dell’azione di prevenzione epidemiologica ma necessitano, evidentemente, di misure complementari di diversa natura, idonee a superare i limiti imposti, tra le altre cose, dal divario digitale.

Tale considerazione, sui limiti intrinseci alle opzioni tecnologiche, ha un duplice ordine di implicazioni.

In primo luogo, la valutazione dell’efficacia attesa dalla misura non può prescindere da un’analisi inerente le azioni complementari e, dunque, la fase- che dovrebbe ragionevolmente conseguirne- dell’accertamento sanitario dei soggetti individuati, tramite data tracing, quali potenziali contagiati.

Si possono raccogliere, infatti, tutti i dati possibili sui potenziali portatori (sani o meno che siano), ma se poi non si hanno le risorse (e persino i reagenti!) per accertarne l’effettiva positività, non si va molto lontano.

In secondo luogo, la necessità di ricostruire la catena dei contagi mediante i dati di dispositivi elettronici rende problematica l’imposizione di un obbligo generalizzato di uso di tali sistemi. Ciò, infatti, presupporrebbe la possibilità (non solo economica ma anche cognitiva) di utilizzo di smartphone e di loro funzionalità che non sono, oggettivamente, a tutti accessibili.

Inoltre, un simile obbligo di utilizzo sarebbe difficilmente coercibile salvo ricorrere a un vero e proprio braccialetto elettronico.

Se anche si ritenesse, come pure si sta ipotizzando, di far attivare il bluetooth direttamente da una app, come imporre, infatti, di uscire di casa solo se ‘accompagnati’ dal proprio smartphone, tra l’altro abbastanza carico?

Queste considerazioni inducono a preferire il ricorso a sistemi fondati sulla volontaria adesione dei singoli che consentano il tracciamento della propria posizione. Tuttavia, per garantire la reale libertà (e quindi la validità) del consenso al trattamento dei dati, esso non dovrebbe risultare in alcun modo condizionato.

Pertanto, non potrebbe ritenersi effettivamente valido, perché indebitamente e inevitabilmente condizionato, il consenso prestato al trattamento dei dati acquisiti con tali sistemi, se prefigurato come presupposto necessario, ad esempio, per usufruire di determinati servizi o beni (si pensi al sistema cinese).

L'efficacia diagnostica di tale soluzione dipende, in ogni caso, dal grado di adesione che essa incontri tra i cittadini, in quanto la rilevazione potrebbe per definizione avvenire solo limitatamente alla parte della popolazione che consenta di "farsi tracciare".

La percentuale minima per l'efficacia è stimata nell'ordine del 60%.

E se a Singapore tale soluzione ha visto l'adesione di pressoché tutta la popolazione, ciò sembra imputabile prevalentemente alla specifica cultura e al grado molto avanzato di innovazione digitale di quel Paese.

Ciò non esclude però che un'adeguata sensibilizzazione sull'opportunità di ricorrere a tale tecnica, anche solo a fini egoistici- ovvero per essere informati di essere stati potenzialmente e inconsapevolmente contagiati tramite un contatto con soggetti positivi- possa invece consentire un'ampia adesione dei cittadini.

In tal senso, quindi, la volontaria attivazione di una app funzionale alla raccolta dei dati sull'interazione dei dispositivi, ben potrebbe rappresentare il presupposto di uno schema normativo fondato su esigenze di sanità pubblica, con adeguate garanzie per gli interessati (art. 9, p.2, lett.i) Reg. (Ue) 2016/679).

La seconda fase del trattamento (quella, cioè, successiva alla rilevazione dei dati) consiste essenzialmente nella conservazione degli stessi, in vista del loro eventuale, successivo utilizzo per allertare i potenziali contagiati.

Tale opera di "personalizzazione" dovrebbe avvenire limitatamente ai soggetti risultati poi positivi e a coloro ai quali, con essi, siano entrati in contatto significativo, per il solo periodo di potenziale contagiosità.

Sotto il profilo dell'impatto sulla riservatezza, determinato dalla conservazione in sé dei dati, in vista del loro successivo utilizzo, è certamente preferibile la soluzione della registrazione del "diario dei

contatti" sullo stesso dispositivo individuale nella disponibilità del soggetto. Si eviterebbe così la conservazione di dati personali in banche dati dei gestori, che riproporrebbe le criticità rilevate dalla giurisprudenza della Cgue sulla data retention.

I criteri di necessità, proporzionalità e minimizzazione rimarcati dalla giurisprudenza europea indicano, comunque, l'esigenza di contenere tali limitazioni della privacy nella misura strettamente necessaria a perseguire fini rilevanti, con il minor sacrificio possibile per gli interessati.

Seguendo questo criterio, dovremmo allora ritenere anzitutto preferibile la misura più selettiva, che garantisca cioè il minor ricorso possibile a dati identificativi, sia in fase di raccolta sia in fase di conservazione.

In tal senso, ai fini della raccolta, il bluetooth, restituendo dati su interazioni più strette di quelle individuabili in celle telefoniche assai più ampie, parrebbe migliore nel selezionare i possibili contagiati all'interno di un campione più attendibile perché, appunto, limitato ai contatti significativi (così parrebbero orientati Singapore e Germania).

In particolare, sarebbero apprezzabili quelle tecnologie che mantengono il diario dei contatti esclusivamente nella disponibilità dell'utente, sul suo dispositivo, ragionevolmente per il solo periodo massimo di potenziale incubazione.

Il soggetto che risultasse positivo dovrebbe fornire l'identificativo Imei del proprio dispositivo all'asl, che sarebbe poi tenuta a trasmetterlo al server centrale per consentirgli così di ricostruire, tramite un calcolo algoritmico, i contatti tenuti con altre persone le quali si siano, parimenti, avvalse dell'app blue tooth.

Queste ultime riceverebbero poi una segnalazione (nella forma di un alert sul sistema) di potenziale contagio, con l'invito a sottoporsi ad accertamenti che, naturalmente, sarà efficace nella misura in cui sia responsabilmente seguito.

In tal modo, il tracciamento sarebbe affidato a un flusso di dati pseudonimizzati, suscettibili di reidentificazione solo in caso di rilevata positività.

Anche in tali circostanze, comunque, la stessa comunicazione tra server centrale ed app dei potenziali contagiati avverrebbe senza consentirne la reidentificazione, così minimizzando l'impatto della misura sulla privacy individuale.

In alternativa all'alert intra-app, si potrebbe ipotizzare che sia direttamente l'asl ad avvisare e, quindi, sottoporre ad accertamento le persone le quali, dalle rilevazioni bluetooth, risultino essere entrate in contatto significativo con il soggetto positivo.

La conservazione dei dati di contatto, da parte del server, dovrebbe comunque limitarsi al tempo strettamente indispensabile alla rilevazione dei potenziali contagiati.

L'anamnesi rimessa al medico consentirebbe, poi, di realizzare quell'intervento umano sul processo algoritmico richiesto dal Regolamento 2016/679 per evitare l'esclusiva soggezione umana a decisioni automatizzate, correggendone anche, così, possibili distorsioni e inesattezze.

In ogni caso, è auspicabile che la complessa filiera del contact tracing possa realizzarsi interamente in ambito pubblico.

Ove, tuttavia, ciò non fosse possibile e anche solo un segmento del trattamento dovesse essere affidato a soggetti privati, essi dovrebbero possedere idonei requisiti di affidabilità, trasparenza e controllabilità, rigorosamente asseverati.

Potrebbe infine essere utile prevedere specifici reati propri, suscettibili di realizzazione da parte di coloro che, potendo avere accesso ai dati per qualunque ragione anche operativa, li utilizzino per altre finalità.

La soluzione ipotizzata ridurrebbe, verosimilmente allo stretto necessario, la sua incidenza sulla riservatezza. Tuttavia, benché non massivo, il trattamento di dati personali comunque realizzato richiederebbe, auspicabilmente, una norma di rango primario, (anche un decreto-legge, che assicura la tempestività dell'intervento, pur non omettendo il sindacato parlamentare né quello successivo di costituzionalità, diversamente dalle ordinanze).

Ove non si procedesse a un intervento legislativo ad hoc, sarebbe opportuno quantomeno integrare l'art. 14 dl 14/20, anche con misure di garanzia da prevedersi eventualmente con fonte subordinata.

La norma avrebbe anche una rilevante funzione performativa, fornendo una cornice generale di regole e garanzie cui uniformarsi anche a livello locale. Si eviterebbero così le autonome iniziative, differenziate da zona a zona che- in quanto spesso scoordinate e poco verificabili - rischiano di indebolire l'efficacia complessiva della strategia di contrasto. Quest'esigenza di uniformità vale sia a livello interno che sovranazionale. E', in questo senso, assolutamente condivisibile l'auspicio del Garante europeo per la protezione dei dati, in favore dell'adozione di un unico progetto di data tracing in ambito europeo.

Naturalmente, come prescritto dalla Consulta per le disposizioni emergenziali, è fondamentale l'efficacia temporalmente limitata della norma, da revocare non appena terminato lo stato di necessità o, comunque, ove la prassi ne dimostri la scarsa utilità (in tal senso, sarebbero opportuni controlli periodici).

Ed è essenziale sancire (con il presidio di sanzioni adeguate) l'obbligo di cancellazione dei dati decorso il periodo di potenziale utilizzo (salva la conservazione in forma aggregata o comunque anonima per soli fini statistici o di ricerca) e l'illiceità di qualsiasi riutilizzo dei dati per fini diversi da quelli di tracciamento dei contatti, nei termini suindicati.

Così circoscritto, il ricorso al contact tracing potrebbe anche concorrere all'eventuale formazione del "passaporto sanitario digitale".

Ci riferiamo, in particolare, alle varie iniziative suscettibili di adozione nella fase di ripresa delle attività, per la valutazione del grado individuale di rischio epidemico.

Vanno studiate, dunque, modalità e ampiezza delle misure da adottare in vista della loro efficacia, gradualità e adeguatezza, senza preclusioni astratte o tantomeno ideologiche, ma anche senza improvvisazioni o velleitarie deleghe, alla sola tecnologia, di attività tanto necessarie quanto complesse.

La chiave è nella proporzionalità, lungimiranza e ragionevolezza dell’intervento, oltre che naturalmente nella sua temporaneità.

Il rischio che dobbiamo esorcizzare è quello dello scivolamento inconsapevole dal modello coreano a quello cinese, scambiando la rinuncia a ogni libertà per l’efficienza e la delega cieca all’algoritmo per la soluzione salvifica.