GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Audizione informale, in videoconferenza, del Presidente del Garante per la protezione dei dati personali sull'uso delle nuove tecnologie e della rete per contrastare l'emergenza epidemiologica da Coronavirus

English version

Audizione informale, in videoconferenza, del Presidente del Garante per la protezione dei dati personali sull'uso delle nuove tecnologie e della rete per contrastare l'emergenza epidemiologica da Coronavirus

Commissione IX (Trasporti, Poste e Telecomunicazioni) della Camera dei Deputati

(8 aprile 2020)

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.

Hearing through video conference of the President of the Italian Data Protection Authority regarding use of new technologies and the Internet to counter the Covid-19 epidemiological emergency

Committee IX of the Italian Chamber of Deputies (Transportation, Post, Telecommunications)

8 April 2020

1. Rights, derogations, restrictions

The severe emergency situation our country is coping with made it necessary to adopt, via provisions of different nature and scope, measures intended to restrict several fundamental rights; those measures are expected to be helpful in containing the spread of this contagion.

This was bound to impact the protection of personal data as well, which is a fundamental freedom right and is enshrined in the Charter of Nice. On the whole, the restrictions implemented so far are rather limited in scope.

Derogations from the standard rules on data processing were set out in the decrees that were issued shortly following the decision to declare a state of emergency – mainly concerning the communication of health data.

Section 14 of decree-law No 14/2020 basically reiterated those derogations, which were however taken up in a primary law instrument (no longer in a governmental decree) and clearly marked out as temporary in nature without envisaging particularly 'innovative' data collection mechanisms.

New, more intrusive data collection arrangements might be introduced on grounds of public health, which make up a specific legal basis like with the 'emergency rescue' activities – on condition the relevant provisions are compliant with the principles of necessity, proportionality, adequacy and respect the essential core of the right at issue.

2. Epidemiological mapping and surveillance

This is the framework in which to place the proposal to collect data on location or interactions with other devices of the mobile devices held by individuals who have tested positive for COVID-19 in order to evaluate epidemiological trends or trace back the spread of the contagion.

Firstly, since a wide gamut of measures can be envisaged, one should implement a stepwise approach and accordingly determine whether less intrusive measures can be enough for the purposes of epidemiological prevention.

From this perspective, the acquisition of genuinely anonymised mobility patterns raises no specific issues. Article 9 of the e-privacy directive legitimises the acquisition of location data without the data subject's consent, providing the data have been anonymised.

This approach allows mapping, for instance, the development of the epidemics, which is highly helpful for prognosis and statistics, whilst it is less so for diagnostic purposes as such.

On the other hand, using non-anonymised data on location or interactions with other devices may prove helpful in many ways.

In any case, this will require – also pursuant to Article 15 of the e-privacy directive – sufficiently detailed rules including adequate safeguards.

The data in question may be used theoretically, taking also the cue from the public debate over the past few weeks, for various purposes:

a) To determine the location of an individual placed under home confinement because tested positive for the virus, that is to say, the geo-location of the mobile phone (which is assumed to be carried permanently by that individual) can be used to establish compliance with the home confinement obligations; or

b) To acquire, going backwards, data on the interactions of the virus-positive individual with other individuals, in order to establish his or her possible contacts during the virus activity period via several technologies: phone cells, GPS, Bluetooth.

Different purposes underlie the two scenarios described here – which is unquestionably a key factor to assess whether the processing is ultimately lawful.

In the former case, the mobile phone location is used as if with a sort of electronic bracelet, by replacing ‘human’ controls through the electronic eye; however, it is taken for granted that an individual violating the confinement obligations will carry his or her phone with them, which is clearly counter-intuitive.

Another measure used to check compliance with social distancing obligations consists in the use of drones by public security authorities.

Again, such tools should be implemented in compliance with the proportionality principle – particularly on account of their highly privacy-intrusive potential.

Indeed, where this measure is implemented by the police to monitor compliance with home confinement obligations rather than to flag ‘unidentified’ gatherings, one can hardly expect the proportionality principle to be respected as a wide gamut of personal data can be potentially collected.

It would be desirable to introduce specific legislation in this respect, partly because the legal basis referred to currently mentions requirements linked to territorial surveillance for purposes of public security, fight against terrorism and organised crime – which cannot be equated in full to those at issue here (see Section 5(3-e) of decree-law No 7/2015 as enacted, with amendments, by Law No 43/2015 and subsequently amended by decree-law No 113/2018 enacted with amendments by Law No 132/2018).

3. Contact tracing

The latter scenario is more complex as it has to do with tracing backwards the contacts held by the virus-positive individuals during the incubation period. This can be done, at least theoretically, by matching several categories of data including commercial transactions, phone cells, interactions with other mobile devices as extracted from Bluetooth data.

It should be considered that the individual data categories have clearly different implications in terms of epidemiological significance – the latter being higher the more the given category can pinpoint more relevant contacts, which are in turn those showing greater physical closeness as these are more likely to have caused the infection to spread.

We will see that selecting the most effective data category also impacts on the overall assessment of proportionality, since increased selectivity reduces the intrusiveness of the given measure to what is strictly necessary and produces socially meaningful effects in terms of protecting the health of individuals and the community as a whole.

Generally speaking, the purpose underlying the approach in question is to be received most favourably because it is not focused on repression – contrary to what is the case with the surveillance of quarantined individuals based on their geolocation – but on solidarity.

The ultimate purpose would actually consist in the need to test all those individuals who may have come in contact with an individual subsequently tested positive, or anyhow to take measures intended to prevent contagion.

The objective pursued would therefore lie within the scope of the solidarity element inherent in the right to health, seen as a societal interest, which has been highlighted by the Constitutional Court in their decisions on mandatory vaccination.

There would be actually very few valid alternatives to the use of such technologies in order to trace back the spread of contagion.

Interviewing patients may leave room to loopholes and the information may be flawed ultimately because lacking several details on who one may have been in contact with in the most diverse situations (at the chemist’s, in a supermarket, etc.).

A possible drawback of the approaches based on telephone data lies in the assumption that everybody carry their phones around. Whilst this may be true for the younger population, it is certainly not the case with the elderly who actually ought to be contacted first in case of a possible infection in order to be treated as timely as possible.

‘Technological’ solutions are actually powerful tools for epidemiological prevention purposes, however they require supplementary measures to be in place in order to overcome the limitations caused, among other things, by the digital divide.

This consideration regarding the limitations inherent in technological solutions has twofold implications.

Firstly, in assessing the expected effectiveness of a measure one should not fail to consider those supplementary measures, that is to say, the measures envisaged for the reasonably subsequent stage when the individuals identified via data tracing as potentially infected will have to undergo medical tests.

Indeed, one may well collect all possible information on potential virus carriers (whether in good health or not), but if there are not enough resources (or reagents) to establish whether those carriers do test positive to the virus, then one will not go very far.

Secondly, the need to trace back the spread of contagion by means of electronic devices makes it difficult to impose a general obligation for everyone to use those devices. Indeed, a precondition for this is that everyone can – not only in monetary terms, but also in terms of cognitive skills – use a smartphone and the many functions it holds, which is factually not feasible for everyone.

Additionally, such a mandatory use would hardly lend itself to coercive measures unless one introduced a veritable sort of electronic bracelet.

If one imagines – as is being mulled currently – to use an app to directly activate Bluetooth functions, how could one oblige individuals to leave home only if they bring their own (sufficiently charged) smartphones with them?

These considerations point to the advisability of relying on approaches that are based on the voluntary acceptance of the individuals allowing their locations to be traced. Still, this consent should be in no way conditional so as to ensure that it is truly free and therefore valid with a view to data processing.

Accordingly, consent given to the processing of data acquired via the mechanisms described so far could not be regarded as valid if it were framed as a precondition, for instance, to obtain certain services or goods – as was the case in China.

In any case, the effectiveness of this solution for diagnostic purposes is related to the support received from citizens since the data could only be collected, by definition, from that part of the population that would give their consent to ‘tracing’.

It is estimated that at least 60% of the population should give their consent in order to achieve effectiveness.

In Singapore basically the whole population did consent, but this would appear to be due mainly to the specific cultural milieu and the advanced digital innovation scenario of that country.

Still, one cannot rule out that raising adequate awareness of the advisability of this approach, even merely for egoistic purposes, i.e. to be informed that one may have been infected because of having come into contact with virus-positive individuals, might not result into widespread acceptance by citizens.

From this standpoint, the voluntary activation of an app intended to collect data on device interactions could be a precondition for a regulatory framework grounded in public health requirements, including appropriate safeguards for data subjects (Article 9(2), letter i), of Regulation 2016/679).

The next step in the processing at issue, following data collection, consists basically in the storage of the data with a view to their subsequent use in order to alert possibly infected individuals.

This ‘customisation’ activity should take place with regard to virus-positive individuals and the individuals that have had significant contacts with them – but only during the period of potential infectiousness.

From the perspective of privacy implications as related to the storage of the data for their possible subsequent use, one should certainly prefer a solution whereby a ‘contact journal’ would be created on the very device owned by the individual at issue. This would avoid storage of the personal data in the telecom operators’ databases, which might raise the criticalities already flagged by the EU Court of Justice regarding data retention.

The necessity, proportionality and minimization criteria highlighted by the EU Court point anyhow to the need for limiting these privacy restrictions to what is strictly necessary in order to achieve relevant, important purposes by undermining data subjects’ rights to the minimum possible extent.

If one goes in this direction, one should firstly prefer the most selective measure, that is to say, the measure enabling the least

possible use of identifying information for both collection and storage of the data.

Thus, Bluetooth technology would appear to be preferable in order to select possibly infected individuals out of a more reliable sample, limited to significant contacts, as it yields data on spatially closer interactions compared to those that are identifiable within the much larger area covered by a phone cell. This is what Singapore and Germany would be planning to do.

In particular, one would prioritize those technologies that keep the contact journal exclusively with the user, on the latter's device, reasonably for the maximum duration of the potential incubation period.

An individual testing positive would then provide the IMEI identifier of their device to the geographically competent health care agency, which would then transmit it to the central server in order to trace back, through an algorithm, the contacts with other individuals who also have activated their Bluetooth apps.

Those other individuals would then receive an alert of potential infection and be invited to undergo medical testing – of course, one assumes such invitation to be followed responsibly.

In this manner, tracing would be based on pseudonymised data and reidentification would only be implemented in case virus positivity were established.

The communication between central server and apps of potentially infected individuals would also take place without enabling their re-identification and thus minimize the impact on their privacy.

As an alternative to the intra-app alerts, one might envisage that the local health care agency directly alerts and tests the individuals who, based on Bluetooth data, are found to have had significant contacts with a virus-positive individual.

The contact data should be retained by the server for no longer than is indispensable with a view to identifying possibly infected individuals.

The medical history to be subsequently collected by a physician would introduce a human intervention in the algorithmic process, which is required by the GDPR to prevent exclusively automated decisions and make good any distortions or inaccuracies brought about by those decisions.

In any case, it is desirable for the complex set of operations involved in contact tracing to be carried out entirely by public bodies.

If this were not feasible and even only a minor part of the processing were to be committed to private entities, the latter should meet suitable requirements in terms of reliability, transparency and controllability and compliance with such requirements should be verified carefully.

Finally, it might be helpful to introduce specific statutory offences to punish any entity that, being authorised to access the data on whatever ground, including for operational activities, uses such data for whatever different purpose.

The solution envisaged here would reduce the impact on privacy to what is foreseeably absolutely necessary. Still, the processing of personal data, albeit not massive in scope, would have to be regulated via a piece of primary legislation – including a decree-law, which allows taking timely measures without dodging parliamentary review or the assessment of compliance with constitutional principles, unlike what is the case with governmental ordinances.

If no ad-hoc legislation is passed, it would be appropriate at least to introduce additional provisions in Section 14 of decree-law No 14/2020, including safeguards to be detailed further in secondary law instruments.

Introducing specific legislation would also be efficient in order to provide a general framework of rules and safeguards to be abided by also at local level. This would avoid a patchwork of initiatives, differing from one area to the next one, which are often poorly consistent and difficult to gauge in terms of their effectiveness and may ultimately undermine the overall impact of the fight against this contagion. This call for uniformity applies both domestically and at supranational level. Accordingly, we fully share the position taken by the European Data Protection Supervisory favouring the adoption of a unified data tracing scheme at European level.

Obviously, and in line with the requirements made by the Constitutional Court in respect of any emergency measure, it is

fundamental for these provisions to be limited in time and be revoked immediately the state of emergency ceases – or if those provisions are found to be poorly effective in practice. From the latter standpoint, regular checks would be advisable.

It is also fundamental to lay down the mandatory erasure of the data once the period set for their potential use expires – subject to storage of such data in aggregate or anonymised format exclusively for statistical or research purposes. Adequate punishments should be introduced for non-compliance. By the same token, any reuse of the data for purposes other than contact tracing should be prohibited.

Within the boundaries outlined here, contact tracing might ultimately become part of the so-called ‘digital health passport’.

I am referring here to the initiatives that will be possibly implemented after the lockdown in order to assess the epidemiological risk at individual level.

Therefore, the mechanisms and scope of the measures to be adopted should be assessed in view of their effectiveness, incremental application and adequacy, without theoretical or ideological biases but also without improvising or committing necessary as well as complex activities exclusively to technology.

Proportionality, far-sightedness and reasonableness are key components of any such measures – of course, along with their temporary nature.

The risk to be averted is that of drifting away from the Korean to the Chinese model – of mistaking the waiver of all freedoms for effectiveness and the blind confidence in algorithms for the all-powerful solution.