

NETWORK **DIGITAL 360**

I NOSTRI SERVIZI

MENU

Agenda  Digitale 

Cittadinanza digitale ▾ Sicurezza Informatica ▾ Sanità digitale

ACCEDI

CORONAVIRUS

Pizzetti: "A rischio le libertà dei cittadini, urgente un intervento giuridico"

Home > Sicurezza Digitale > Privacy



La normativa permette deroghe alla privacy in caso di emergenza, ma l'Italia ha scelto modalità giuridiche pericolose, lasciando ampi poteri alle autorità locali di comprimere le libertà. Serve una normativa temporanea che ci rimetta nell'alveo dei diritti costituzionali e in seguito una legge che chiarisca i termini esatti

3 ore fa

Franco Pizzetti

professore emerito in diritto costituzionale, Università di Torino, ex Garante Privacy



IN QUESTO PERIODO
DI GRANDE INCERTEZZA,
NON FERMARTI:
I WEBINAR SONO
UNA GRANDE OPPORTUNITÀ!

**Argomenti**

D dati personali **T** Tutto su GDPR

Canali

P Privacy **S** Sicurezza digitale

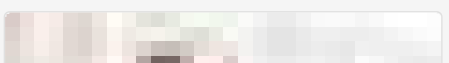
Articoli correlati**GDPR**

Raccolta dati personali presso terzi, le sfide normative e come affrontarle

07 Ott 2019

di **Fabio Di Resta**

Condividi



Da quando il 31 gennaio 2020 con delibera del Consiglio dei ministri è stato dichiarato lo stato di emergenza per l'epidemia coronavirus si è aperta nell'ordinamento italiano una **fase molto caotica di procedimenti normativi, legati alla lotta a tale emergenza, che pone numerosi problemi di rapporto fra le fonti dell'ordinamento e, quel che più conta, di tutela o compressione dei diritti fondamentali dei cittadini.**

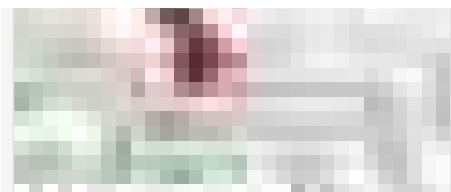
Questi problemi, già molto rilevanti rispetto alla compressione di diritti fondamentali previsti e disciplinanti dalla Costituzione, primi fra tutti la libertà di circolazione e di riunione, meritano anche, e forse soprattutto, in questa fase emergenziale il **dovuto inquadramento giuridico**, perché si garantisca realmente l'interesse pubblico secondo quanto previsto dalla legge e non contro la legge o, peggio, in modo improvvisato, ingenerando nei cittadini la sensazione che le loro **libertà fondamentali potessero essere compresse senza un obiettivo** "di sistema" condiviso e corrente nella complessa catena decisionale all'interno dell'organizzazione dello Stato, che sta oggi fronteggiando l'emergenza del coronavirus.

Indice degli argomenti

Quando è cominciata la compressione delle libertà fondamentali

Il punto di partenza del ragionamento è senz'altro costituito dal decreto legge del **23 febbraio 2020 n.6, con cui il Presidente del Consiglio ha adottato "Misure urgenti per evitare la diffusione del COVID-19"**. Si è trattato di un intervento appropriato, che ha sanato precedenti ordinanze adottate nell'imminenza del contagio dal Capo della protezione civile, nella forma di un decreto legge, atto previsto dalla Costituzione proprio per far fronte agli stati di necessità e urgenza e sottoposto comunque al controllo del parlamento attraverso legge di conversione.

Ovvio che così operando il Presidente del Consiglio dei Ministri si è sostituito al corpo nazionale dei vigili del fuoco e delle forze armate, anche se in larga parte il contenuto del decreto riprende alcune delle disposizioni contenute nell'ordinanza adottata dal Capo della protezione civile in attuazione della delibera che aveva dichiarato lo



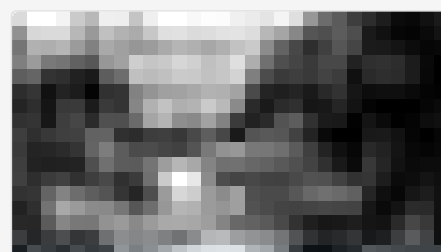
GDPR

Data protection by design e by default: ecco le linee guida EDPB

29 Nov 2019

di **Mario Valentini e Federica Lamoratta**

Condividi 



PRIVACY E SALUTE

Consenso al trattamento dei dati sanitari: ecco perché col GDPR è cambiato tutto

21 Gen 2020

di **Chiara Rauccio**

Condividi 

stato di emergenza.

È bene inoltre rilevare come l'art. 4 del decreto legge 23 febbraio 2020 specifichi che l'Autorità competente ad assicurare l'esecuzione delle nuove misure sia il Prefetto, che può avvalersi delle Forze di polizia e, ove occorra, dei Vigili del fuoco e delle Forze armate sentiti i comandi territoriali.

Successivamente, il Presidente del Consiglio dei ministri adotta, il l'11 marzo 2020, un nuovo decreto-legge contenente "Ulteriori disposizioni attuative del decreto-legge 23 febbraio 2020, n.6, recenti misure urgenti in materia di contenimento e gestione dell'emergenza epidemiologica del COVID-19 applicabili sull'intero territorio nazionale". Con questo decreto tuttavia non ci si limita a estendere a tutto il territorio nazionale le misure emergenziali già adottate con i precedenti decreti legge e con numerose ordinanze emanate da diversi Ministri, si procede anche a una ulteriore revisione e modifica dei provvedimenti già presi, soprattutto con rilievo agli obblighi imposti ai cittadini e alle loro associazioni.

Il termine di durata delle nuove misure, come già quelle precedenti, resta fissato nel 3 aprile, con un contenuto degli obblighi in qualche caso ulteriormente compressivo di diritti fondamentali previsti dalla Costituzione.

Nell'ambito di questa complessa normativa composta da un numero elevato di atti amministrativi e ordinanze adottate da numerosi Ministri in attuazione del decreto-legge n. del 23 febbraio, **merita attenzione il decreto legge n. 14, del 9 marzo 2020**, recante "Disposizioni urgenti per il potenziamento del servizio sanitario nazionale in relazione all'emergenza COVID-19" in cui spicca l'art.14 (Disposizioni sul trattamento dei dati personali nel contesto emergenziale) che prevede che "fino al termine dello stato di emergenza [...] le strutture deputate pubbliche e private che operano nell'ambito del Servizio sanitario nazionale e i soggetti deputati monitorare e a garantire l'esecuzione delle misure disposte ai sensi del decreto legge 23 febbraio 2020 n.6 anche allo scopo di assicurare la più efficace gestione dei flussi e dell'interscambio di dati personali, possono effettuare trattamenti, ivi inclusa la comunicazione tra loro, dei dati personali, anche relativi agli art. 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".

L'articolo 14 del d.l. continua poi con altri 6 commi che disciplinano ulteriormente anche il trattamento degli altri dati personali e le modalità di applicazione dello stesso regolamento UE 2016/679.

La cascata di fonti normative

Queste poche citazioni normative dovrebbero essere sufficienti a far capire come la normativa emergenziale adottata nell'ambito della pandemia Codi-19 sia particolarmente **complessa**, da un lato e dall'altro determini una vera e propria **"cascata" di fonti normative**. Il passaggio è estremamente delicato e ogni intervento deve essere opportunamente calibrato, per non correre il rischio che l'intero impianto, che muove da alcuni decreti legge e passa attraverso i dpcm, **non finisca per legittimare un potere di ordinanza sull'aula e che in base alla necessità di far fronte all'emergenza si affermi di poter operare in deroga alla legislazione di settore**, compresa, per quanto riguarda la tutela dei dati personali al regolamento UE. **Il regolamento UE ha al suo interno sufficienti elementi di flessibilità per consentire anche la gestione, senza deroghe, di questa fase emergenziale.**

È solo una sottovalutazione delle potenzialità del regolamento UE che ha consentito lo svilupparsi di una pluralità sempre più ampia e differenziata di ordinanze, prevalentemente fondate sul potere di adottare ordinanze contingibili e d'urgenza, con il risultato, sotto gli occhi di tutti, dell'attuazione di una normativa emergenziale jeopardizzata, e con **l'adozione di provvedimenti in materia di diritti e libertà fondamentali anche diversi da area ad area del Paese. È ciò è una evidente contraddizione, che non giova alla necessaria resistenza alla diffusione del virus.**

Questo non riguarda soltanto il caso della protezione dei dati personali, di cui qui ci si occupa, ma ha determinato modalità di compressione (o di tutela) di altri diritti fondamentali spesso diverse da area ad area di Paese, che si traducono nel quadro diversificato di livelli di contagio a cui purtroppo assistiamo.

La cosa ovviamene non si è verificata quando il Governo ha agito

adottando dpcm con efficacia su tutto il territorio nazionale, ma è accaduta con l'intervento delle numerose autorità amministrative, regioni e comuni compresi, che hanno talora dato una differente interpretazione del dpcm, adottando ordinanze di urgenza diversificate per dare attuazione a quanto previsto dai decreti leggi richiamati o, in generale, alla legislazione emergenziale.

Il caso Lombardia: i dati dei cellulari

Anche rispetto alla tutela dei dati personali questo fenomeno si è verificato. Il vice presidente della regione **Lombardia**, Icardi, ha dichiarato che la regione aveva chiesto e ottenuto da gestori telefonici un numero imprecisato ma rilevante di dati di traffico telefonico di cittadini lombardi o persone viventi nel territorio della Regione e li aveva incrociati con dati di altri interessati, prevalentemente risultati positivi a test sul coronavirus, al fine dichiarato di verificare se e in che misura le ordinanze del Governo e della Regione impattavano sui comportamenti dei cittadini.

Non risultano iniziative analoghe da parte di altre Regioni, né a tuttora è noto il numero degli utenti telefonici trattati o (cosa che preoccupa maggiormente) la metodologia adottata e la sua efficacia. Non si vuole qui censurare il fine di queste iniziative, che è senz'altro commendevole, almeno in principio, in quella martoriata Regione. Ci si permette soltanto di sottolineare che c'è una situazione persino peggiore dei tempi difficili che stiamo vivendo, a cui si può arrivare e molto rapidamente, anche in buona fede, proprio attraverso il trattamento di dati personali, ossia il proliferare di "esperimenti" incontrollati e improvvidi, condotti su dati di scarsa qualità che non solo non limitano i contagi ma determinano un maggiore stato di angoscia nella popolazione e una caccia all'untore di manzoniana memoria. Il giurista di buon senso deve essere in favore di trattamenti di dati personali che, condotti da soggetti qualificati, concorrano a limitare realmente l'aggressività del virus e possibilmente aiutino il Paese a uscire prima dall'emergenza. Il giurista di buon senso deve opporsi con ogni forza a trattamenti di dati personali estemporanei, senza nessuna valenza scientifica, inadatti a generare una migliore conoscenza del fenomeno e capaci soltanto di generare sospetto tra persona e persona e maggiore incertezza. Bisogna fare molta attenzione a parlare di modello Corea

del Sud.

A questo punto credo non sia difficile capire perché la normativa italiana emergenziale di questo ultimo mese possa sollevare molti dubbi, anche oltre il tema della compressione della protezione dati, che peraltro è più un pericolo che una realtà effettivamente verificatasi, salvo che per il caso della Lombardia.

Il fatto è che l'impostazione seguita fin dal decreto 23 febbraio 2020 n. 6, che ha dichiarato lo stato di emergenza e definito i poteri di ordinanza di urgenza, compreso l'ambito di operatività dei dpcm e delle ordinanze adottate ai sensi dell'art. 3 del medesimo decreto, ha aperto la via a quella che credo dobbiamo definire la "cascata delle fonti" nel quadro della risposta all'emergenza coronavirus.

Giova ricordare l'art.3 del decreto legge n. 6 del 2020 che recita "Le misure di cui agli articoli 1 e 2 sono adottate, senza nuovi e maggiori oneri per la finanza pubblica, con uno o più decreti del Presidente del Consiglio dei Ministri, su proposta del Ministro della salute, sentiti il Ministro dell'Interno, il Ministro della difesa, il Ministro dell'economica e delle finanze e gli altri ministri competenti per materia, nonché i Presidenti delle regioni competenti nel caso in cui riguardino esclusivamente una regione o alcune specifiche regioni ovvero il Presidente della conferenza delle regioni e delle provincie autonome, nel caso in cui riguardino il territorio nazionale".

La norma in questione appare del tutto ragionevole e accettabile, salvo forse il fatto di assegnare ai dpcm un potere di intervento, basato sulla lotta all'emergenza, che permetterebbe a questa fonte di intervenire anche sull'applicazione delle norme contenute in fonti di rango legislativo, cosa questa peraltro prova delle ordinanze contingibili e d'urgenza come conosciute dall'ordinamento generale.

Il fatto è che sia alcuni dpcm adottati in attuazione di queste norme, sia soprattutto il d. l. n.14 del 2020 con l'art. 14 già richiamato hanno esteso sia il numero dei soggetti titolari di un potere emergenziale di intervento sia gli strumenti normativi utilizzabili, individuandoli in tutti i provvedimenti di urgenza che chiunque avesse compiti relativi alla lotta al Codiv-19 può adottare.

In questo quadro hanno trovato anche ulteriore ratifica le numerose ordinanze di Presidenti di regione o di sindaci di comuni, adottate nel

quadro emergenziale anche prima del c.l. n. 14 del 2020.

Gli effetti delle tante diverse norme locali

Gli effetti di questo intricato sistema normativo e di questa “cascata di fonti” sono evidenti.

WHITEPAPER

Come è cambiato in Italia il quadro normativo dei pagamenti digitali verso la PA?



Consenso cessione dati a terzi

Consente all'invio di comunicazioni promozionali inerenti i prodotti e servizi di soggetti terzi rispetto ai Titolari con modalità di contatto automatizzate e tradizionali da parte dei terzi medesimi, a cui vengono comunicati i dati.

SI No

SCARICA IL WHITEPAPER

Da un lato si è dato molto rilievo al potere del Presidente del Consiglio di adottare provvedimenti derogatori anche delle norme di legge attraverso i dpcm, e con ciò gli strumenti a sua disposizione per far fronte alle situazioni emergenziali che richiedono l'adozione di provvedimenti legati al concetto di “ordinanze contingibili e di urgenza” ben note nel nostro ordinamento amministrativo. Dall'altro, avendo di fatto valorizzato così tanto lo strumento delle ordinanze di urgenza si è di fatto convalidato quanto già da tempo regioni ed enti locali avevano iniziato a fare in merito ai provvedimenti di lotta alla epidemia.

Col successivo decreto n. 6/2020 e in particolare con l'art. 14, si è scelto, lodevolmente, di dare un ordine sistematico a tutto questo, demandando specificamente al potere di ordinanza e agli strumenti giuridici legati all'urgenza già presenti nell'ordinamento, il potere e il dovere di provvedere a adottare i provvedimenti necessari alla lotta all'emergenza, sempre ovviamente che i soggetti titolari di tali poteri

fossero comunque chiamati a operare per contenere il diffondersi dell'epidemia.

Inoltre, si è esteso anche per questi provvedimenti il termine di durata e validità giuridica alla dichiarazione di superamento dello stato di emergenza, in generale fissato nella dichiarazione di fine dello stato o, per i provvedimenti previsti dal d.l.n.6 del 2020, al 3 aprile 2020, salvo ulteriore proroga o diverso limite dei singoli provvedimenti di urgenza.

La situazione che si è di fatto determinata è stata quella di dare una copertura giuridica alle iniziative spesso non coordinate degli amministratori locali, Presidente di regione compresi, che si sono trovati da un lato nella posizione di soggetti che devono essere necessariamente sentiti prima dell'adozione dei dpcm, ove questi riguardino la loro regione, sia di autorità dotate di poteri emergenziali, ovviamente nell'ambito territoriale di loro competenza.

Questo complicato intrigo nel sistema delle fonti ha favorito e ampliato la geopadizzazione del Paese consentendo il convivere in parallelo di provvedimenti a efficacia nazionale (i dpcm innanzitutto) e poteri a efficacia territoriale limitata (le ordinanze di urgenza dei Presidenti di regione e delle altre autorità ammonitive, in primo luogo).

Questo aspetto, tanto evidente quanto poco sottolineato finora ha una notevole incidenza proprio sulle stime delle fonti che possono incidere sui diritti fondamentali e, quindi, per quanto qui interessa anche sul diritto alla protezione dei dati personali.

Le norme privacy non ostacolano la compressione dei diritti in stato di emergenza

Da questo punto di vista è bene innanzitutto chiarire che non vi è alcun dubbio che in caso di emergenza il diritto alla tutela dei dati personali, pur diritto fondamentale ai sensi della Carta dei diritti fondamentali della UE, possa essere compresso.

La Presidente dello **EDPB**, Andrea Jelinek ha diffuso in data 16 marzo 2020 uno Statement col quale, anche con riferimento allo statement adottato in data 19 marzo 2020, specifica che la

protezione dai non è ostacolo al trattamento di dati personali anche in deroga ai principi vigenti quando si tratti di far fronte a emergenze in settori di pubblico interesse e, quindi, maggior ragione nella lotta al coronavirus.

Allo Statement Jelinek come a quello dello EDPB si rinvia, dunque, per dire con chiarezza che non può sussistere dubbio alcuno circa la legittimità di una compressione da parte degli Stati membri del diritto come tutelato dal **GDPR** quando si tratti di combattere una emergenza legata all'interesse pubblico e, quindi, a maggior ragione nel caso della lotta al COVID-19.

In questa sede basterà richiamare a questo proposito quanto previsto dall'art. 9 comma 2, lettera j) secondo il quale il divieto di trattare dati relativi alla salute senza il consenso dell'interessato non si applica quando il trattamento "è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale".

Dunque, non vi è dubbio che, come dice il Considerando 19 del Regolamento UE, è opportuno che gli Stati membri possano "mantenere o introdurre disposizioni specifiche per adattare l'applicazione delle disposizioni del presente Regolamento". Ovviamente si precisa anche che "tali disposizioni possono determinare con maggiore precisione requisiti specifici per il trattamento di dati personali da parte di dette Autorità competenti per altre finalità, tenuto conto della struttura costituzionale, organizzativa e amministrativa dei rispettivi Stati membri".

Dunque, è doveroso sottolineare che la protezione dati è cedevole rispetto alle esigenze proprie degli Stati, tanto più se legate un quadro emergenziale che tocca anche la protezione di alti diritti individuali e fondamentali come il diritto alla salute e alla vita.

Infine, sia consentito tornare ancora e più specificamente sulla possibilità di tracciare i comportamenti delle persone facendo

riferimento ai loro dati telefonici conservati da provider telefonici o da fornitori di servizi on line.

Questo tema, molto discusso in questi giorni proprio per la iniziativa assunta dalla Regione Lombardia e resa nota, come già ricordato, dall'assessore Icardi, non può però essere valutata solo nel quadro del GDPR. Infatti, la tutela dei dati personali nella sfera digitale è specifico oggetto anche della direttiva ePrivacy che riguarda proprio i dati di localizzazione telefonica.

La direttiva ePrivacy e la direttiva 2020/58

Nelle intenzioni della Commissione e del WP29 **anche la direttiva ePrivacy avrebbe dovuto essere trasformata in un Regolamento ed essere approvata in modo da entrare in vigore contemporaneamente al GDPR. Peraltro, anche per questo, il GDPR fa esplicitamente salva la direttiva ePrivacy (direttiva 58/200 CE), come specifica l'art. 95 del GDPR.**

Tuttavia, poiché non c'è stato il Regolamento, come sottolinea nella sua Opinione la presidente dello EDPB Jelinek, l'eventuale trattamento di dati di traffico telefonico anche a fini di geolocalizzazione ricade ancora sotto quanto previsto dalla direttiva **2020/58/CE**, che prevede che gli Stati membri possono adottare disposizioni legislative volte a limitare i diritti e gli obblighi di cui agli art.5 e 6, all'articolo 8 paragrafi da 1 a 4, e dell'articolo 9 della presente direttiva qualora tale restrizione costituisca, ai sensi dell'articolo 13, paragrafo 1, della direttiva 95/46, "una misura necessaria, opportuna e proporzionata all'interno di una società democratica per la salvaguardia della sicurezza nazionale (cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica; e la prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell'uso non autorizzato di sistemi di comunicazione elettronica".

"A tal fine gli Stati membri possono adottare tra l'altro per un periodo di tempo limitato misure per i motivi enunciati nel presente paragrafo. Tutte le misure di cui al presente paragrafo sono conformi ai principi generali del diritto comunitario, compresi quelli di cui all'articolo 6, paragrafi 1 e 2, del trattato sull'Unione Europea".

È chiaro che questa norma apre la via alla deroga delle disposizioni

di tutela dei dati personali, ed è appunto in questo senso che la Presidente Jelinek la richiama.

Si potrebbe obiettare che le ragioni per le quali gli Stati possono derogare sono enumerate e legate tutte alla sicurezza nazionale, alla difesa e alla sicurezza pubblica nonché alla ricerca, accertamento e perseguimento dei reati, ovvero dell'uso non autorizzato di sistemi di comunicazione elettronica. Tuttavia l'art. 15, proprio per il suo contenuto, va interpretato anche tenendo conto della direttiva ePrivacy, che comprende deroghe alla normativa di protezione dati anche in presenza di rischi per la sicurezza dello Stato: una formula così ampia che certamente possiamo ritenere, confortati anche dalla Opinione della Presidente Jelinek e dell'EDPB, comprenda anche i rischi alla salute pubblica quando questi siano tali da mettere a rischio la stessa sicurezza dello Stato intesa come mantenimento e rafforzamento della comunità nazionale.

Non può esservi dubbio che il combinato disposto dell'art.15 della Direttiva 2002/58/CE e dell'art.9 del GDPR consente allo Stato membro di prevedere, per ragioni attinenti alla sicurezza dello Stato anche la deroga alle disposizioni della ePrivacy e quindi, in sostanza alla normativa che tutela la protezione dei dati nel settore delle comunicazioni elettroniche.

Così ragionando, tuttavia, è evidente che gli Stati debbono disporre le deroghe (nel caso che ci interessa la possibilità di tracciare i dati anche senza consenso dell'interessato) solo con disposizioni legislative e qualora la restrizione costituisca una misura necessaria, opportuna e proporzionata all'interno di una società democratica per la salvaguardia della sicurezza nazionale (in questo caso interpretata in modo ampio e coerente con l'art. 9 del GDPR e dunque estesa anche al caso di epidemie e altri eventi che possano disgregare l'unità nazionale).

La precisazione è importante perché l'art. 15 impone anche agli Stati di assicurare, sempre mediante dismissioni legislative, misure relative alla conservazione dei dati e le modalità che assicurino la proporzionalità delle deroghe alla finalità di tutelare la sicurezza nazionale, fermo restando il rispetto dei principi, in primis la necessità, proporzionalità e accuratezza dei dati, nonché

l'opportunità delle misure adottate con riguardo a una società democratica.

Occorre una nuova legge e che le misure siano adeguate ai principi di una società democratica

Questo dunque è il punto: non vi è ostacolo alla limitazione dell'applicazione della normativa a tutela dei dati personali (e quindi anche all'uso senza consenso dei dati di traffico per tracciare gli spostamenti delle persone). **Ma perché questo sia conforme alle regole UE occorre che lo Stato provveda con legge e che le misure legislative adottate siano adeguate a garantire la necessità, proporzionalità e adeguatezza delle norme e delle deroghe adottate rispetto ai principi d'una società democratica.**

Il che significa certamente che la legislazione derogatoria dovrà indicare chi possa trattare i dati telefonici di altri per tali fini, con quale procedimento, in quali casi, ricorrendo quali condizioni, il tutto al fine di rendere la legislazione derogatoria compatibile con i principi democratici. In questo quadro dovrà essere anche definito se e da parte di chi e in quali tempi si debbano informare gli interessati che si sono fatti trattamenti relativi ai loro dati, indicandone anche i motivi e gli eventuali tempi per ricorrere nonché l'Autorità alla quale presentare il ricorso, la cui individuazione può anche andare oltre l'Autorità di protezione dei dati.

Siamo dunque arrivati al punto nodale del tema che stiamo trattando.

L'analisi svolta ci dice, ripercorrendo il sentiero già tracciato alla Presidente Jelinek e da tutto lo EDPB, che deroghe alla normativa di protezione dei dati a tutela della sicurezza dello Stato sono certamente legittime e possono estendersi anche al trattamento di dati telefonici, compresi quelli di geolocalizzazione. Questo però ad almeno due condizioni: la prima che si proceda con legge; la seconda che si assicuri che le modalità derogatorie sono comunque compatibili con una società democratica e dunque che queste perseguano l'alto scopo di pubblico interesse per cui le si invoca, secondo le indicazioni di un comitato tecnico che si muova nel solco di metodologie di comprovata efficacia scientifica, e che rispettino i principi di trasparenza verso l'interessato, di procedimentalizzazione

dell'esercizio dei poteri di deroga, di individuazione dell'Autorità alla quale può essere presentato ricorso e delle ulteriori tutele assicurate, anche successivamente al trattamento, agli interessati.

Il problema: le modalità scelte per limitare le libertà

Insomma, e per essere chiari: **il problema non è la compressione della normativa di tutela dei dati personali in caso di emergenza o di messa in pericolo della sicurezza nazionale, come certamente accade con COVID-19, ma il modo col quale tali compressioni sono avvenute.**

Ne è dimostrazione proprio il caso della Lombardia rispetto al quale la domanda ineludibile è: a parte le legislazioni UE e nazionale in materia di tutela del diritto fondamentale alla privacy, è ragionevole e conforme alla Costituzione immaginare che in materia di diritti fondamentali la loro sospensione e riduzione avvenga con atti amministrativi quali sono le ordinanze contingibili e d'urgenza sulla base di una norma autorizzatoria generica e indeterminata?

E ancora: è possibile che la compressione e rimodulazione dei diritti fondamentali dei cittadini, così indicati dalla Costituzione e dalla normativa UE possa avvenire a geometria variabile come inevitabilmente accade quando la loro compressione avvenga per atto amministrativo di una Autorità a competenza territoriale definita e non coincidente con tutto il territorio nazionale? Si è consapevoli dell'effetto di questa disomogeneità?

Si noti che il primo decreto legge sembrava consapevole di questi problemi e infatti sembrava aver centrato ogni potere derogatorio e di urgenza in capo al Presidente del Consiglio, sia pure sentiti i Presidenti di regione interessati.

Solo con i provvedimenti successivi, come anche qui si è ricostruito, si è dato vita a una catena di rinvii da una fonte all'altra che ricorda molto le matrioske russe.

Solo che questo, oltre ad aver prodotto obiettivamente una geopardizzazione anche nel settore delicatissimo dei diritti fondamentali (di circolazione, domicilio, riunione, ecc.) **ha determinato il fondare il potere di derogare alla normativa di tutela**

dei dati personali a atti sostanzialmente amministrativi, del tutto inadeguati a quanto la normativa UE richiede.

Sembra urgente quindi che il Governo e il Parlamento riflettano sulla situazione che si è creata, come pare stia già avvenendo se si tiene conto che non a caso il decreto Cura Italia si è trasformato in una ordinanza del Ministro della Salute.

La legge che ci serve dopo l'emergenza

Quello che occorre, e non solo per coerenza col quadro UE ma anche con la Costituzione italiana, è procedere, magari dopo che la epidemia sarà cessata, **ad approvare una legge che definisca in modo generale e preventivo disciplinare in materia di emergenze che possono incidere anche sui diritti fondamentali, avendo cura di coinvolgere sempre il Parlamento, di operare sempre sulla base di una valutazione della proporzionalità e adeguatezza delle misure che si intendono prendere e di riservare in linea generale al Presidente del Consiglio, che è pur sempre legato al Parlamento dal rapporto di fiducia, il potere emergenziale di adottare provvedimenti di urgenza anche quando essi possano incidere sui diritti fondamentali.**

Inoltre, sarà bene che la **legge in questione definisca anche il procedimento da adottare, la Autorità giudiziaria alla quale i cittadini possano fare ricorso contro il provvedimento e le garanzie da assicurare ai cittadini.**

La legge che ci serve subito

Nelle more di tutto questo, tenendo conto che una legge così complessa non è certo affare di tempi come questi, sarà bene cercare almeno di operare assicurando coerenza sia col quadro UE che con quello costituzionale italiano.

Infine, una **norma di legge, anche transitoria in attesa d'una legislazione organica, è assolutamente necessaria per capire se i provider telefoni possano o debbano conservare i dati di traffico oltre al tempo necessario per fornire il servizio e dimostrare di averlo fornito.**

In tale senso un modello al quale si può far riferimento è quello

adottato in passato dell'UE per la normazione nazionale in materia di data retention per ragioni di giustizia. Non sfugge la questione legata alla proporzionalità dei trattamenti eccepita dalla Corte di Giustizia Europea, tuttavia almeno metodologicamente si trattava di un ottimo strumento e che oggi può essere ripreso per finalità di lotta all'epidemia, imponendo ai provider telefonici di conservare i dati di traffico e di metterli a disposizione del servizio sanitario nazionale. Ciò che di quell'esperienza può utilmente essere ripreso è lo sforzo del legislatore di individuare le categorie di dati da trattare, le finalità, le misure di sicurezza e, aggiungiamo oggi, la validità scientifica dei modelli epidemiologico-previsionali adottati.

In conclusione: serve una manovra di rientro sui diritti

Insomma, e per concludere, **la possibilità di trattare dati di geolocalizzazione telefonica degli italiani per finalità di limitazione dell'epidemia COVID-19 non è in contrasto, nella sostanza, con la protezione dei dati personali.** Ma questo vale dal punto di vista sostanziale; dal punto di vista formale invece molte osservazioni si possono fare, come qui si è fatto, alle forme scelte e alle modalità adottate.

Peraltro, chiedendo scusa per il gioco di parole, **siamo di fronte a vizi di forma che sono estremamente sostanziali** per quanto riguarda i valori in gioco e i rischi che possono far correre alle libertà dei cittadini. La sospensione di queste libertà non è il prezzo da pagare per uscire da quest'emergenza. Affatto. Semmai si può dire il contrario, come si è argomentato.

Sarà bene dunque che fin da ora si cerchi di mettere a punto una "manovra di rientro" del sistema delle fonti e ci si prepari, anche con aggiustamenti successivi, ad assicurare provvedimenti emergenziali più conformi alla nostra costituzione e, dove necessario, più coerenti col quadro giuridico UE.

 **WHITEPAPER**

**Gestione dei contratti e
GDPR: guida
all'esternalizzazione di**



attività dei dati personali



Legal

Consente all'invio di comunicazioni promozionali inerenti i prodotti e i servizi di soggetti terzi rispetto ai Titolari con modalità di contatto automatizzate e tradizionali da parte dei terzi medesimi, a cui vengono comunicati i dati.

No Si

[SCARICA IL WHITEPAPER](#)



@RIPRODUZIONE RISERVATA

Articolo 1 di 4

Agenda **Digitale**

Seguici



About

Autori

Tags

Rss Feed

Privacy

Cookie

NETWORK **DIGITAL** 360

NetworkDigital360 è il più grande network in Italia di testate e portali B2B dedicati ai temi della Trasformazione Digitale e dell'Innovazione Imprenditoriale. Ha la missione di diffondere la cultura digitale e imprenditoriale nelle imprese e pubbliche amministrazioni italiane.

TUTTE LE TESTATE

Applicazioni e Tecnologie

AI4BUSINESS
 BIGDATA4INNOVATION
 BIG DATA & ANALYTICS ZEROUNO
 BLOCKCHAIN4INNOVATION
 CLOUD COMPUTING ZEROUNO
 CYBERSECURITY CORCOM
 CYBERSECURITY360
 DOCUMENTI AGENDADIGITALE.EU
 ECOMMERCE AGENDADIGITALE.EU
 FATTURAZIONE AGENDADIGITALE.EU
 INDUSTRIA 4.0 CORCOM
 INDUSTRY 4.0 AGENDADIGITALE.EU
 INFRASTRUTTURE AGENDADIGITALE.EU
 INDUSTRY4BUSINESS
 INTERNET4THINGS
 PAGAMENTIDIGITALI
 RISKMANAGEMENT360
 SEARCHDATACENTER ZEROUNO
 SEARCHSECURITY ZEROUNO
 SICUREZZA AGENDADIGITALE.EU
 SMART CITY AGENDADIGITALE.EU
 SMART MOBILITY ECONOMYUP

Digital Transformation

AGENDADIGITALE.EU
 CORCOM
 DIGITAL4EXECUTIVE
 DIGITAL4PMI
 TECHCOMPANY360
 ZEROUNO

Funzioni di Business

DIGITAL4FINANCE
 DIGITAL4HR
 DIGITAL4LEGAL
 DIGITAL4MARKETING
 DIGITAL4PROCUREMENT
 DIGITAL4SUPPLYCHAIN
 PROCUREMENT AGENDADIGITALE.EU

Startup e Open Innovation

ECONOMYUP
 STARTUP AGENDADIGITALE.EU

Industry

AGRIFOOD.TECH
 AUTOMOTIVEUP
 BANKINGUP
 ENERGYUP
 INDUSTRY4BUSINESS
 INSURANCEUP
 MEDIA CORCOM
 RETAILUP
 SANITÀ AGENDADIGITALE.EU
 SCUOLA AGENDADIGITALE.EU
 TELCO CORCOM
 TURISMO AGENDADIGITALE.EU

PA

CITTADINANZA AGENDADIGITALE.EU
 FORUMPA
 PA DIGITALE CORCOM
 SANITÀ AGENDADIGITALE.EU
 SCUOLA AGENDADIGITALE.EU

Studenti

UNIVERSITY2BUSINESS