Il diritto nella pandemia

Temi, problemi, domande

a cura di
Ermanno Calzolaio, Massimo Meccarelli,
Stefano Pollastrelli

eum

Il diritto nella pandemia

Temi, problemi, domande

a cura di Ermanno Calzolaio, Massimo Meccarelli, Stefano Pollastrelli

eum

Studi Superiori

6

Collana della Scuola di Studi Superiori "Giacomo Leopardi" dell'Università di Macerata

ISBN 978-88-6056-661-4 (print)
ISBN 978-88-6056-662-1 (on-line)
DOI 10.13138/ss-60566621

Prima edizione: luglio 2020

Corso della Repubblica, 51 – 62100 Macerata
info.ceum@unimc.it
http://eum.unimc.it

Impaginazione: Carla Moreschini
Copertina: +studiocrocevia

Indice

Il prisma dell'interazione

Simone Calzolaio

Sistema di allerta Covid-19. Osservazioni sull'art. 6, d.l. 28/2020

Sommario: 1. Elogio della prudenza – 2. Il fondamento giuridico-costituzionale del 'motivo di interesse pubblico' (c. 1) – 3. Il sistema di allerta, i suoi elementi costitutivi e le differenti esigenze di disciplina (commi 1, 5, 6) – 4. Il ruolo delle Regioni e dei Servizi sanitari regionali nel sistema di allerta (c. 1) – 5. I rischi derivanti dal trattamento e dalla costituzione della piattaforma, per l'interessato (protezione e sicurezza dei dati personali) e per la sicurezza cibernetica dello Stato – 6. Diritti da non dimenticare. Minori e persone decedute – 7. Conclusioni, cioè domande aperte

1. *Elogio della prudenza*

Il presente contributo ha ad oggetto una breve analisi dell'art. 6, d.l. n. 28/2020, di cui meglio si dirà appresso.

C'è tuttavia una considerazione preliminare e di metodo che si intende focalizzare, da cui proviene il titolo del paragrafo.

L'attuale momento storico è caratterizzato da una emergenza pandemica e quanto sta accadendo rende evidente che «non c'è niente da fare, siamo nati per aspettare che qualcosa si muova e che ci venga a cercare» (*Giovani disponibili*, Carboni, 1984). Questa sollecitazione della realtà ha prodotto e produce una incessante e disordinata produzione normativa, un altrettanto disorganico riassetto dei ruoli istituzionali e del fluire delle prassi applicative [Luciani 2020; Cardone 2020], che a sua volta evidenzia la fragilità della nostra società e delle nostre persone (molto prima della debolezza, che ne è il riflesso, delle nostre istituzioni e del sistema politico). Si tratta del manifestarsi della

cd. società signorile di massa [Ricolfi 2019] applicata ad una pandemia di una certa gravità [Lord Sumption 2020].

Non di meno, si assiste ad un moltiplicarsi a tratti caotico di commenti e orientamenti di carattere tecnico-scientifico, in cui ciascuno tenta di decifrare il reale con gli strumenti della branca scientifica di cui si occupa. La facilità con cui è possibile pubblicare on line i propri contributi, nella migliore delle ipotesi dopo veloci referaggi, fa il resto. Anche questo è un effetto – poco studiato e ancor meno meditato – del processo rivoluzionario che prende il nome di digitalizzazione e di società dei dati [Calzolaio 2017].

In questo contesto è francamente difficile discernere se l'impegno a 'scrivere di diritto' (*law in pandemic*) costituisca il proprio contributo ad affrontare l'emergenza, come ciascuno intimamente desidera, ovvero sia un contegno atto ad aumentare la confusione, frutto forse di un altro contagio, quello del *publish or perish*.

Non si riesce in questa sede a risolvere tale dilemma. Ma lo si ritiene utile a offrire una indicazione di metodo, che consiste nell'accorgersi del proprio limite di fronte all'esorbitanza di quanto sta accadendo rispetto alla ordinaria capacità di analisi giuridica.

In sintesi, pertanto, quel che accade, quel che si legge, il molto che non si comprende appieno o affatto, induce a riscoprire la prudenza, a parlare e scrivere meno del solito.

A questo riguardo, l'art. 6, d.l. 28/2020, per chi si è occupato prevalentemente di diritto costituzionale regionale e di diritto dell'informazione e della comunicazione (che oggi è il diritto delle nuove tecnologie e della protezione dei dati personali), è come un vulcano in eruzione e tocca in soli sei commi molti dei più scottanti problemi aperti del diritto pubblico italiano e contemporaneo. Solo per citarne alcuni: il fluire disordinato della decretazione d'urgenza, la confusione e la competizione istituzionale nei rapporti fra Stato e Regioni, la difficoltà a inquadrare il tema (e il regime giuridico) dello sfruttamento pubblico per finalità di interesse generale dei dati e di coordinarlo con il diritto alla protezione dei dati personali, il problema della sicurezza cibernetica dello Stato, della sovranità sui dati e la connes-

sa assenza di investimenti pubblici e privati nella pianificazione infrastrutturale e strategica.

L'elogio della prudenza richiede che questi temi siano evocati e restino sullo sfondo. Per contribuire a risolvere il problema epocale del rapporto fra diritto alla salute e protezione dei dati personali nella società dei dati è invece opportuno procedere dal basso, analizzare le disposizioni della norma citata e mettere in comune – sommessamente – le principali (e brevi) osservazioni che provengono dalla propria limitata esperienza di studio.

Il presente contributo pertanto si sviluppa in una serie di osservazioni, di norma contenenti una breve spiegazione e argomenti per una meditazione critica sulla formulazione del testo normativo.

2. *Il fondamento giuridico-costituzionale del 'motivo di interesse pubblico' (c. 1)*

Il c. 1 dell'art. 6 statuisce chiaramente che il sistema di allerta Covid-19 è costituito dalla piattaforma unica nazionale e dalla applicazione per dispostivi di telefonia mobile ed è finalizzato ('al solo fine') a allertare le persone entrate in contatto con soggetti positivi al virus e a tutelarne la salute. Si tratta di un sistema cui si accede e permane su base volontaria. Come specifica il c. 4, il mancato utilizzo della applicazione non comporta conseguenze pregiudizievoli.

Quindi, l'utilizzo della applicazione è permanentemente volontario.

Inoltre, nessuna disposizione dell'art. 6 richiede che l'utente (l'interessato) presti il proprio consenso all'utilizzo in sede di installazione della applicazione e di avvio del trattamento dei propri dati personali, ancorché si tratti di dati attinenti alla salute (art. 9, par. 1, GDPR).

Se la base giuridica del trattamento non è il consenso [Pagnanelli 2020], allora deve necessariamente rinvenirsi nell'esecuzione di un compito di interesse pubblico (art. 6, par. 1, lett. e, GDPR) ovvero, più precisamente, nei motivi di interesse pubblico di cui all'art. 9, par. 2, lett. g) e i), GDPR (cfr. art. 75, Codice protezione dati personali; cons. 46, GDPR).

La disposizione in parola, tuttavia, non definisce in dettaglio quale sia il motivo di interesse pubblico in base al quale l'ordinamento interviene a predisporre un sistema di allerta di carattere esclusivamente volontario.

In altri termini, l'art. 6 stabilisce qual è il fine e quali sono i caratteri del sistema di allerta, ma non si diffonde a delineare quale sia il fondamento giuridico in base al quale lo Stato interviene a disciplinare ed a costituire tale sistema di allerta.

Se il motivo di interesse pubblico fosse di adottare misure di contrasto alla diffusione del virus, allora risulterebbe peculiare, e anche contraddittorio, un trattamento dei dati personali non obbligatorio per tutti. Si tratterebbe infatti di un caso assimilabile in qualche modo a quello delle cd. vaccinazioni obbligatorie o, al ricorrere dei presupposti, della cd. quarantena.

Invece, l'art. 6 sembra disciplinare e prefigurare uno strumento diverso e non assimilabile alle vaccinazioni obbligatorie e in effetti va sottolineato che le fattispecie, allo stato, differiscono sensibilmente: la funzionalità del sistema di allerta è in grado, al massimo, di accertare di essere stati prossimi a persone infette, di anticipare in tal modo la diagnosi e, se del caso, la cura. Il vaccino invece evita, di norma, di contrarre la malattia.

Pertanto, è necessario rileggere il c. 1 dell'art. 6 e individuare altre ipotesi plausibili sull'effettivo 'motivo di interesse pubblico' che anima la costituzione del sistema di allerta.

In questa prospettiva è opportuno osservare – come si è già autorevolmente rilevato [Colapietro, Iannuzzi 2020] – che il sistema di allerta si basa, con ogni evidenza, sulla iniziativa spontanea e sulla collaborazione *in chiave solidaristica* fra gli utenti: installando e mantenendo istallata la app e, qualora ve ne siano i presupposti, inserendo il codice che segnala il proprio contagio, essi consentono di tracciare i contatti con gli altri utenti e quindi di venire a (e offrire) conoscenza di un possibile contatto con persone contagiate, con tutto quanto ne consegue.

Si sarebbe portati a ritenere, pertanto, che lo Stato, istituendo l'infrastruttura digitale necessaria, disciplina, promuove e sostiene questo sistema di allerta, fondato sull'autonoma e volontaria adesione degli utenti, in quanto espressione del generale principio di solidarietà applicato, in questo caso, al settore del

diritto alla salute (artt. 2 e 32 Cost.) e del principio di sussidiarietà orizzontale (art. 118, c. 4, Cost.).

Mentre il riferimento agli artt. 2 e 32 Cost. appare facilmente comprensibile, forse è opportuno spendere qualche parola sull'art. 118, c. 4 Cost. Infatti, la disposizione costituzionale da ultimo citata è chiarissima nell'affermare che lo Stato e gli altri enti territoriali hanno il compito di favorire l'iniziativa dei cittadini per lo svolgimento di attività di interesse generale. In questo caso, invece, è lo Stato che assume l'iniziativa e i cittadini, semmai, liberamente aderiscono. Tuttavia, in assenza di una infrastruttura di base come sarebbe pensabile che i cittadini possano promuovere una attività di interesse generale di questo tipo?

In questo settore, in assenza di un preliminare e pregiudiziale intervento pubblico, che ha ad oggetto la parte regolatoria e la parte infrastrutturale del sistema di allerta, francamente può rivelarsi arduo immaginare la realizzazione di un sistema di allerta nazionale da parte dei cittadini. Una volta realizzata e disciplinata l'infrastruttura necessaria, la sua operatività può essere – come avviene esattamente nel caso di specie – interamente lasciata all'autonoma iniziativa dei cittadini, che i poteri pubblici favoriscono proprio attraverso l'istituzione dell'infrastruttura del sistema di allerta. In altri termini, pertanto, con la creazione del sistema di allerta lo Stato pone le condizioni affinché la libera iniziativa dei cittadini, per il perseguimento di finalità di interesse (particolare e) generale, possa essere esercitata. E in effetti la disciplina positiva dettata dall'art. 6 lascia chiaramente intendere che il sistema di allerta, essendo esclusivamente su base volontaria, potrebbe essere costituito ma non utilizzato da nessuno.

Queste considerazioni, appena accennate, in merito al fondamento giuridico-costituzionale del motivo di interesse pubblico del trattamento dei dati personali derivante dal sistema di allerta di cui all'art. 6, e in particolare il riferimento non scontato al principio di sussidiarietà orizzontale, possono avere una funzione rilevante, in quanto costituiscono un parametro ed un criterio formale utile a delineare il contenuto e l'ambito dell'intervento statale in materia e, soprattutto, a verificare il rispetto del principio di proporzionalità nel trattamento dei dati personali

degli utenti per finalità di tutela della salute. Si intende ipotizzare pertanto che il fondamento giuridico e la ratio della disciplina dell'art. 6 risiedono nel favorire l'esercizio del principio di solidarietà fra le persone e nell'incentivare l'utilizzo in ambiente digitale di forme ulteriori di tutela del diritto alla salute, fondate sulla iniziativa autonoma delle persone, in base agli articoli 2, 32, 118 c. 4, della Costituzione, e nel rispetto degli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione europea.

Un ultimo inciso. La esplicita individuazione del motivo di interesse pubblico in riferimento all'art. 6 sarebbe importante anche come 'precedente normativo'. Qualora, in un futuro che nessuno auspica, dovesse rivelarsi necessario utilizzare questi stessi strumenti, o strumenti analoghi, con modalità e per finalità diverse da quelle attuali, il legislatore non potrebbe utilizzare questa stessa base giuridica e dovrebbe individuarne una nuova e diversa. Ciò potrebbe rivelarsi, sotto molteplici aspetti, rilevante per l'evoluzione dell'ordinamento e per identificare i tratti del bilanciamento normativo fra i diritti fondamentali in gioco intorno al tema del cd. *digital tracing*.

3. *Il sistema di allerta, i suoi elementi costitutivi e le differenti esigenze di disciplina (c. 1, 5, 6)*

L'art. 6 è rubricato "Sistema di allerta Covid-19". Si tratta – a quanto consta – del primo esperimento del genere nel nostro Paese.

È particolarmente importante, di conseguenza, specificare con chiarezza da quali componenti è costituito questo sistema di allerta, poiché ciò ha conseguenze rilevanti, ai fini della protezione degli interessi pubblici e privati e di una corretta e ragionevole disciplina normativa.

Il sistema di allerta è costituito da 3 elementi fondamentali: 1) la piattaforma unica nazionale (poi anche denominata 'piattaforma informatica', 'piattaforma di cui al c. 1' o solo 'piattaforma'), 2) un'apposita applicazione e, per definizione, 3) i dati degli utenti che volontariamente la utilizzano.

Si ha un trattamento di dati personali, che conduce all'esigenza di adottare l'articolo 6 quale base giuridica del tratta-

mento, proprio in quanto si realizza l'interazione fra i 3 fattori costitutivi del sistema di allerta (piattaforma, applicazione, dati personali).

Tuttavia, deve essere sottolineato che l'esistenza della piattaforma e della applicazione, in assenza di informazioni personali riferibili agli utenti, non darebbe luogo ad alcun trattamento di dati personali e quindi non sarebbe soggetta alla disciplina del GDPR.

La piattaforma, infatti, costituisce un *asset* materiale e immateriale che di per sé è neutro, e potrebbe essere utilizzato per trattare dati non personali. Così come – in astratto – l'applicazione informatica che se ne avvale. Ad es. l'applicazione potrebbe utilizzare la piattaforma per trattare dati non personali derivanti dallo scambio di informazioni *machine to machine* – si pensi agli strumenti applicativi della cd. industria 4.0.

Da queste considerazioni derivano una serie di osservazioni in ordine alla disciplina di cui all'art. 6.

La prima. La formulazione attuale del c. 1 è migliorabile, in quanto questi tre autonomi elementi del sistema non sembrano individuati in modo sufficientemente chiaro. Infatti, parafrasando con qualche licenza poetica il c. 1, il sistema di allerta Covid-19, è costituito da (1) una piattaforma unica nazionale (2) per la gestione dei dati personali dei soggetti che, a tal fine, hanno installato, su base volontaria, (3) un'apposita applicazione sui dispositivi di telefonia mobile. È l'interazione fra questi tre fattori costitutivi che costituisce il sistema di allerta.

La seconda. Chiariti gli elementi costitutivi del sistema di allerta è opportuno individuare con altrettanta chiarezza i soggetti che sono responsabili della gestione della piattaforma e della gestione della applicazione, sia ai fini della applicazione del GDPR (poiché si tratta di una informazione che, con ogni probabilità, è opportuno fornire a tutti gli interessati), sia ai fini della corretta gestione di *asset* di titolarità o disponibilità pubblica.

A questo riguardo, il Ministero della Salute è titolare del trattamento e si coordina con una ampia seria di altri soggetti «per gli ulteriori adempimenti necessari alla gestione del sistema di allerta» (c. 1); il c. 5 stabilisce che la piattaforma è realizzata dal Commissario straordinario con infrastrutture gestite da SOGEI.

Tuttavia, nulla si dice in ordine al soggetto che gestisce la piattaforma, una volta realizzata.

Su questo aspetto sarebbe opportuno identificare, almeno, il soggetto cui spetta la gestione della piattaforma, in modo da creare un quadro chiaro in ordine alla realizzazione, gestione, titolarità del trattamento dei dati personali raccolti attraverso le infrastrutture materiali e immateriali della piattaforma.

La terza attiene ad un aspetto centrale e strategico. Il c. 6 stabilisce che «l'utilizzo della applicazione e della piattaforma nonché ogni trattamento di dati personali … sono interrotti alla data di cessazione dello stato di emergenza» e che «non oltre il 31 dicembre 2020 … tutti i dati personali trattati devono essere cancellati o resi definitivamente anonimi».

La disposizione costituisce senz'altro una garanzia importante per quanto concerne il trattamento dei dati personali. Potrebbe essere ragionevole in riferimento all'utilizzo dell'applicazione, se non è possibile sfruttarla ad altri fini (ovviamente estranei al trattamento di dati personali).

Ma – una volta cancellati tutti i dati personali – non si comprende per quale ragione dovrebbe essere interrotto l'utilizzo della piattaforma in quanto tale, cioè di una infrastruttura materiale e immateriale pubblica funzionante, localizzata sul territorio nazionale. Certamente, non si tratta di una disposizione a tutela dei dati personali, che a quel punto sono stati cancellati o resi definitivamente anonimi.

L'aspetto concernente l'infrastruttura e la sua rilevanza strategica appare sottovalutato da questa disposizione e, più in generale, non adeguatamente considerato in questo momento storico in Italia. Non si tratta solo di una considerazione personale, ma di una osservazione che tiene conto di quel che sta accadendo, ad esempio, in seno all'Unione europea. Forse sarà una mera coincidenza temporale, ma il 4 giugno 2020, su iniziativa dei Ministeri dell'economia tedesco e francese, è stata presentata la piattaforma GAIA-X, ovvero *a Franco-German pitch towards a European data infrastructure*. Nella articolata descrizione della piattaforma, presente nell'apposito sito con una molteplicità di dettagliate pubblicazioni, si rende immediatamente noto che l'iniziativa franco-tedesca è volta a istituire una infrastruttura

digitale per accogliere i dati europei in «un sistema sicuro e federato che soddisfa i più alti standard di sovranità digitale».

Un sistema franco-tedesco per i dati europei, che garantirà la sovranità digitale, genericamente intesa: vi si ricomprende anche la sovranità digitale italiana?

Come è evidente, il tema della infrastruttura digitale nazionale e dei connessi temi della disponibilità/titolarità/localizzazione/sovranità dei dati è una questione che in questa fase è venuta prepotentemente alla ribalta, anche perché non è un segreto che i ritardi nella messa in opera della app Immuni sono dovuti anche alla difficoltà di individuare una alternativa infrastrutturale credibile, con il relativo *know-how*, a quella offerta dai giganti del web (Apple e Google, in particolare; sul tema, che qui non si può approfondire: cfr. Colapietro-Iannuzzi). Tuttavia, l'iniziativa franco-tedesca, affidata ai rispettivi Ministeri economici – seppur volendo utilizzare tutta la prudenza che si è premessa – mostra che il tema della piattaforma digitale nazionale è strategico.

Non sembra che la disposizione in commento colga questo profilo, laddove dispone da un lato l'esigenza di realizzazione di una piattaforma digitale, che costituisce una infrastruttura materiale e immateriale nazionale, e poi ne inibisce l'utilizzo pur dopo che si è concluso il trattamento dei dati personali.

In realtà, seppur sommessamente, si osserva che la piattaforma potrebbe essere la base per la costruzione, o l'implementazione, di una infrastruttura nazionale strategica e come tale dovrebbe essere considerata autonomamente e oggetto di specifica disciplina.

4. *Il ruolo delle Regioni e dei Servizi sanitari regionali nel sistema di allerta (c. 1)*

Il sistema di allerta e la sua effettiva funzionalità poggia sul corretto funzionamento dei Servizi sanitari regionali (SSR).

In particolare, l'allerta derivante dall'utilizzo della app è volta a condurre rapidamente la persona esposta al virus a verificare se ha contratto il virus. In caso di effettivo contagio – come si evince dal sito della app *Immuni* – la persona può decidere di

caricare sulla piattaforma le chiavi crittografiche appositamente associate al suo dispositivo. Questo processo, tuttavia, richiede che l'utente detti il codice OTP (One Time Password o password monouso) che si trova nell'apposita sezione dell'app all'operatore sanitario che gli ha comunicato l'esito del tampone. Solo in quel momento il codice verrà validato e l'utente potrà quindi procedere al caricamento. Pertanto, di fatto è proprio attraverso un operatore sanitario – di norma, un dipendente del SSR – che viene validato il codice attraverso il quale l'utente può attivare il sistema di allerta per tutti gli altri utenti interessati.

Ciò comporta che il modello di verifica del contagio (la modalità e la tempestività con cui i SSR accertano il contagio) è particolarmente rilevante ai fini della corretta funzionalità del sistema di allerta.

A quanto si comprende, le Regioni adottano criteri e metodi diversi per verificare il contagio, che possono comportare sia tempi diversi di accertamento, sia percentuali di errore diverse (falsi positivi e falsi negativi): tutti aspetti che influiscono, in assenza di un coordinamento efficace fra Ministero della salute (Titolare del trattamento) e Regioni (Responsabili del trattamento, ai sensi dell'art. 28, GDPR?), sulla funzionalità del sistema di allerta, sul connesso trattamento dei dati personali e sui diritti degli utenti (fra cui, secondo gli artt. 13 ss. del GDPR, si ricordino: diritto alla trasparenza, diritto di rettifica, diritto di limitazione e cancellazione, diritto di opposizione).

Sotto questo profilo, pertanto, il coinvolgimento delle Regioni appare necessario, al fine di garantire la funzionalità del sistema di allerta e il rispetto dei principi e diritti sanciti dal GDPR.

In questo senso, la disposizione del c. 1 non sembra tener conto in modo adeguato della necessaria integrazione del ruolo del sistema (sanitario) regionale nel sistema di allerta nazionale: le singole Regioni sono contemplate solo in quanto ed insieme agli altri soggetti del Servizio nazionale di protezione civile e la Conferenza Stato-Regioni viene solo informata periodicamente sullo stato di avanzamento del progetto.

Il rischio, pertanto, è che alcune delle problematiche nei rapporti Stato-Regioni emerse durante la pandemia riaffiorino nella fase di gestione del sistema di allerta [Di Cosimo, Menegus 2020].

Tutto questo conferma che la visione di fondo del sistema di allerta nazionale, di cui all'art. 6, appare limitata alla gestione del problema della limitazione del contagio e non si apre ad una visione più ampia, in cui la nascente infrastruttura possa sopravvivere alla emergenza ed essere un laboratorio fecondo di una nuova modalità di relazione fra lo Stato e le Regioni. Si pensi, a questo riguardo, che non sembra essere stato previsto, finora, alcun coordinamento fra la disposizione di cui all'art. 6 e le disposizioni del decreto legge n. 34/2020 (cd. Rilancio), che nel Titolo I ("Salute e sicurezza") contiene molteplici previsioni in materia di Fascicolo sanitario elettronico e, più in generale, si occupa diffusamente di digitalizzazione pubblica.

5. *I rischi derivanti dal trattamento e dalla costituzione della piattaforma, per l'interessato (protezione e sicurezza dei dati personali) e per la sicurezza cibernetica dello Stato*

L'art. 6, c. 2, si riferisce ai rischi del sistema di allerta con esclusivo riferimento ai rischi elevati per i diritti e le libertà degli interessati del trattamento di dati personali, presupposto – ai sensi dell'art. 35 del GDPR – per procedere alla valutazione di impatto sulla protezione dei dati.

In realtà, l'istituzione del sistema di allerta di cui all'art. 6 comporta essenzialmente 3 tipologie di rischi, di diversa natura.

I primi due sono connessi con il problema della protezione dei dati personali (la protezione e poi la sicurezza dei dati personali degli utenti), il terzo concerne la tutela della sicurezza cibernetica dello Stato e dell'interesse nazionale a costituire e mantenere una piattaforma nazionale (infrastruttura materiale e immateriale) sicura ed efficace (sicurezza della infrastruttura digitale nazionale).

L'individuazione dei rischi e delle relative tipologie è funzionale ad identificare i soggetti, dotati di specifiche competenze, che debbono coadiuvare il titolare del trattamento e il gestore della infrastruttura a garantire la sicurezza e la protezione dei dati. Nel primo caso si tratta del Responsabile per la protezione dei dati personali (il cd. DPO); nel secondo caso si tratta dei soggetti che garantiscono la sicurezza cibernetica dello Stato.

Sulla base dell'attuale formulazione dell'art. 6, spetta al Ministro della salute, in qualità di titolare del trattamento, considerati i rischi per la protezione e per la sicurezza dei dati derivanti dal trattamento dei dati personali attraverso il sistema di allerta Covid-19, individuare un Responsabile per la protezione dei dati personali, ai sensi degli articoli 37 e seguenti del GDPR. Spetterebbe invece al Commissario straordinario, considerati i rischi per la sicurezza cibernetica dello Stato, individuare opportune misure tecniche e organizzative sin dalla fase di progettazione e realizzazione della piattaforma e dei relativi programmi informatici.

In questo modo, si può tenere conto – come in passato mi era capitato di sottolineare – del fatto che in ambito pubblico il *digital by default standard* e la *privacy by design* e *by default* dovrebbero essere implementati in parallelo, rispondendo a profili ed esigenze di tutela in parte coincidenti, in parte distinte, ma di cui è sempre necessario tenere conto simultaneamente, in anticipo e per impostazione predefinita, per evitare danni gravi alle persone e/o ai non meno rilevanti interessi pubblici.

Sotto questo profilo, si conferma una difficoltà di fondo del nostro ordinamento a coniugare i processi di digitalizzazione pubblica con i principi della protezione dei dati personali. Si tratta infatti di due facce della stessa medaglia, che tuttavia sembrano considerati e disciplinati in modo separato.

6. *Diritti da non dimenticare. Minori e persone decedute*

Alcune osservazioni vanno dedicate agli aspetti meritevoli di tutela nella prospettiva della valutazione di impatto delineata dall'art. 6, c. 2, e in particolare la specifica considerazione dell'informativa da rendere ai minori e l'opportunità di riconoscere esplicitamente la titolarità dei diritti riconosciuti dal GDPR non solo agli interessati, ma anche agli interessati che siano deceduti, come previsto dal vigente Codice per la protezione dei dati personali (ma non dal GDPR).

Sotto il primo profilo, il sistema di allerta si rivolge a tutti, per definizione, ivi compresi i minori. Per costoro sarebbe sensato adottare specifiche modalità informative, come peraltro

previsto proprio dal Codice per la protezione dei dati personali con una disposizione dedicata ai trattamenti per cui è richiesto il consenso del minore (art. 2-quinquies, c. 2, d. lgs. 196/03), ma contenente riferimenti specifici alla modalità con cui il titolare del trattamento è tenuto a redigere l'informativa (e cioè «con linguaggio particolarmente chiaro e semplice, conciso ed esaustivo, facilmente accessibile e comprensibile dal minore»), che in questo caso potrebbero rivelarsi opportuni. In realtà, non mancano – a quanto consta – le competenze all'interno dell'amministrazione statale per svolgere un compito siffatto (cfr., ad es., <https://www.generazioniconnesse.it/site/it/safer-internet-centre/>).

Sotto il secondo profilo, le ragioni che inducono a istituire il sistema di allerta rendono evidente che il problema dei diritti degli interessati poi deceduti potrebbe rivelarsi reale e, purtroppo, non episodico.

Sotto questo profilo, sulla scia di quanto previsto dall'art. 2-terdecies del Codice per la protezione dei dati personali, non sarebbe affatto errato estendere esplicitamente l'esercizio dei diritti riconosciuti agli interessati anche ai soggetti contemplati nella disposizione citata. E, in ogni caso, non sarebbe inutile una disposizione normativa dell'art. 6 che disciplinasse, in modo specifico e se del caso articolato, questa fattispecie.

7. *Conclusioni, cioè domande aperte*

Con ogni probabilità il dibattito parlamentare intorno alla conversione in legge dell'art. 6, d.l. 28/2020, non terrà conto di nessuno degli aspetti e dei temi sin qui evocati. A quanto consta, il Senato ha approvato il disegno di legge di conversione senza introdurre alcuna modifica all'art. 6, ed ora il disegno di legge è all'esame della Camera dei deputati.

Potrebbe non essere un male, in quanto non è facile affrontare temi articolati, che necessitano di un approfondimento, nell'ambito di una discussione frettolosa come quella che tipicamente si sviluppa in sede di conversione in legge di un d.l.

Resta la domanda di come, progressivamente, potrà coniugarsi l'esigenza di approntare le infrastrutture digitali della so-

cietà dei dati, con il tema della sovranità cibernetica dello Stato e della protezione dei dati personali. Questa domanda, come in parte si è cercato di descrivere, si dipana in una molteplicità di quesiti, che spaziano dai rapporti fra lo Stato e le Regioni, ai diritti delle persone, al ruolo dei poteri pubblici, alla poliedricità dei profili connessi con la creazione di una infrastruttura digitale pubblica o di interesse pubblico.

È un bene che questi quesiti restino aperti, perché ci accompagneranno nei prossimi anni, ed è un bene che, andando come a tentoni, si avvii un lavoro certosino di indagine volto a prefigurare chiavi interpretative. Come per la pandemia, nessuno ha la risposta in tasca, ma tutti possiamo contribuire a cercarla. Perché queste domande, ormai, sono venute a cercarci.

Bibliografia essenziale

S. Calzolaio, *Digital (and privacy) by default. L'identità costituzionale dell'amministrazione digitale*, «Giornale di Storia costituzionale», 1, 2016, pp. 185 ss.;

S. Calzolaio, *Protezione dei dati personali (voce)*, «Dig. disc. pubbl»., agg., UTET, 2017, pp. 594 ss.;

A. Cardone, *Il baratro della necessità e la chimera della costituzionalizzazione: una lettura della crisi delle fonti del sistema di protezione civile contro le battaglie di retroguardia*, «Osservatorio sulle fonti» (online), Fascicolo Speciale, 2020;

C. Colapietro, A. Iannuzzi, *App di contact tracing e trattamento dei dati con algoritmi: la falsa alternativa fra tutela del diritto alla salute e protezione dei dati personali*, «Dirittifondamentali.it», 2, 2020, pp. 803 ss., <http://dirittifondamentali.it/2020/06/10/app-di-contact-tracing-e-trattamento-dei-dati-con-algoritmi-la-falsa-alternativa-fra-tutela-del-diritto-alla-salute-e-protezione-dei-dati-personali/>, giugno 2020;

G. De Minico, *Virus e algoritmi. Impariamo da un'esperienza dolorosa*, «laCostituzione.info», <http://www.lacostituzione.info/index.php/2020/04/01/virus-e-algoritmi-impariamo-da-unesperienza-dolorosa/>, aprile 2020;

G. Di Cosimo, G. Menegus, *La gestione dell'emergenza coronavirus tra Stato e Regioni: il caso Marche*, «Biolaw Journal», 2, 2020, <https://www.biodiritto.org/content/download/3768/45243/version/1/file/03+Di+Cosimo+Menegus.pdf>, giugno 2020;

M. Luciani, *Il sistema delle fonti del diritto alla prova dell'emergenza*, «Rivista AIC», 2, 2020, <https://www.rivistaaic.it/it/rivista/ultimi-contributi-pubblicati/massimo-luciani/il-sistema-delle-fonti-del-diritto-alla-prova-dell-emergenza>, giugno 2020;

M. Plutino, "*Immuni*". *Un'exposure notification app alla prova del bilanciamento tra tutela dei diritti e degli interessi pubblici*, «Dirittifondamentali.it», 2, 2020, pp. 553 ss., <http://dirittifondamentali.it/2020/05/26/%EF%BB%BFimmuni-unexposure-notification-app-alla-prova-del-bilanciamento-tra-tutela-dei-diritti-e-degli-interessi-pubblici/>, giugno 2020;

G. Resta, *La protezione dei dati personali nel diritto dell'emergenza COVID-19*, «Giustizia Civile.com», Editoriale del 5 maggio 2020, <http://giustiziacivile.com/soggetti-e-nuove-tecnologie/editoriali/la-protezione-dei-dati-personali-nel-diritto-dellemergenza>, giugno 2020;

L. Ricolfi, *La società signorile di massa*, Milano, La nave di Teseo, 2019;

J. Sumption, *Coronavirus lockdown: we are so afraid of death, no one even asks whether this 'cure' is actually worse*, «The Sunday Times», 5 maggio 2020;

V. Pagnanelli, *Immuni: spunti per una riflessione privacy-oriented*, «Questione giustizia», <https://www.questionegiustizia.it/articolo/immuni-spunti-per-una-riflessione-privacy-oriented_11-05-2020.php>, maggio 2020;

S. Torregiani, *Il dato non personale alla luce del Regolamento (UE) 2018/1807: tra anonimizzazione, ownership e Data by Design*, «federalismi.it», 18, 2020.

Il diritto nella pandemia

Temi, problemi, domande

Il coronavirus (Covid-19) ha colpito direttamente la vita e la salute di un alto numero di persone e ha imposto a tutti un cambiamento che nessuno avrebbe mai immaginato: il confinamento, per limitare al massimo le possibilità di contagio. La situazione inedita che ne è conseguita costituisce una sfida per il giurista, suscitando domande e acuendo l'esigenza di un confronto al di là degli angusti confini dei rispettivi settori disciplinari. Il presente volume raccoglie l'esito delle prime riflessioni presentate in occasione di un seminario di studi promosso nell'ambito delle iniziative dei Corsi di dottorato giuridici e del progetto di Dipartimento di eccellenza su "Diritto e Innovazione" dell'Università di Macerata. I contributi spaziano dalla storia del diritto al diritto costituzionale, dal diritto dell'Unione Europea al diritto comparato e internazionale privato, dal diritto dei trasporti al diritto del lavoro, dal diritto penale al diritto commerciale, dalla medicina legale al diritto processuale.

Ermanno Calzolaio è professore ordinario di Diritto Privato Comparato e coordinatore del progetto del Dipartimento di Eccellenza finanziato dal Miur (2018-2022)

Massimo Meccarelli è professore ordinario di Storia del Diritto e coordinatore dei corsi di dottorato di ricerca in "Scienze giuridiche" e in "Diritto e innovazione"

Stefano Pollastrelli è professore ordinario di Diritto della Navigazione e Direttore del Dipartimento di Giurisprudenza dell'Università di Macerata

unimc UNIVERSITÀ DI MACERATA
l'umanesimo che innova

DIPARTIMENTO DI GIURISPRUDENZA

DIPARTIMENTO DI ECCELLENZA MIUR 2018 - 2022

SDA scuola di dottorato

Corsi di dottorato in SCIENZE GIURIDICHE E LAW AND INNOVATION

eum edizioni università di macerata

ISBN 978-88-6056-662-1