Seconda Commissione (Giustizia)
del Senato della Repubblica italiana
(14.5.2020)

Nota in merito all'art. 6, d.l. 28/2020

(di Simone Calzolaio)

Indice-sommario:

***

1. **Oggetto e metodo** della nota.

La presente nota ha ad oggetto *esclusivamente* l'analisi dell'art. 6, d.l. n. 28/2020.
Si è inteso scrivere nel modo più essenziale e sintetico possibile, evitando di inserire riferimenti bibliografici, di sviluppare analiticamente le tematiche evocate, di ridurre al minimo indispensabile i riferimenti normativi.
Il testo si sviluppa in una serie di *Osservazioni*, di norma contenenti una breve spiegazione e suggerimenti per la modifica del testo normativo.
Lo stile sintetico e assertivo non deve ingannare. Il tema oggetto di analisi è nuovo e sfuggente. Pertanto le osservazioni sono da considerarsi tutte come "sommessamente proposte".
Accanto alla presente nota, sono depositate 4 brevi *note di sintesi* concernenti quanto sta accadendo in ordinamenti diversi dal nostro, ma spesso evocati (Germania, Francia, Regno Unito, Sud Corea), in ordine all'utilizzo degli strumenti digitali per il contrasto al covid-19.

2. ***Osservazione 1***: il fondamento giuridico-costituzionale del "motivo di interesse pubblico" (**comma 1**)

Il comma 1 dell'art. 6 statuisce chiaramente che il sistema di allerta Covid-19 (piattaforma + applicazione) 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 può accedere su base volontaria. Come specifica il comma 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, 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).
Tuttavia la disposizione in parola 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.
Se il motivo di interesse pubblico fosse di adottare misure di contrasto alla diffusione del virus, allora risulterebbe peculiare, e anche contraddittorio, che il trattamento dei dati personali non fosse obbligatorio per tutti. Si tratterebbe infatti di un caso analogo a quello delle cd. vaccinazioni obbligatorie o, al ricorrere dei presupposti, della cd. quarantena. Invece, l'art. 6 sembra disciplinare uno strumento diverso e non assimilabile alle vaccinazioni obbligatorie (la app al massimo anticipa la diagnosi e la cura; il vaccino evita di contrarre la malattia!): dal comma 1 dell'art. 6 sembra trasparire quale sia l'effettivo "motivo di interesse pubblico" che anima la costituzione del sistema.
Il sistema di allerta si basa infatti sulla collaborazione *in chiave solidaristica* fra gli utenti: installando e mantenendo istallata la app, 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.
Lo Stato, istituendo l'infrastruttura digitale necessaria (cd. sistema di allerta) disciplina, promuove e sostiene questo sistema di allerta, fondato sull'autonoma e volontaria iniziativa degli utenti, in quanto espressione del **principio di solidarietà** applicato nel settore del **diritto alla salute** (art. 2 e 32 Cost.) e del **principio di sussidiarietà orizzontale** (art. 118, c. 4, Cost.).
Sul piano del fondamento giuridico-costituzionale, considerati i caratteri del sistema di allerta, questo appare il motivo di interesse pubblico che giustifica l'intervento in base al quale lo Stato interviene in materia, in modo equilibrato e rispettoso del principio di proporzionalità.
Sarebbe opportuno che venisse esplicitato nell'articolato.
Si suggerisce, pertanto, all'inizio del comma 1 aggiungere "*Per favorire l'esercizio del principio di solidarietà fra le persone e 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 comma 4, della Costituzione, e nel rispetto degli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione europea,….*".

3. ***Osservazione 2***: la necessità di distinguere fra sistema di allerta, dati personali/trattamento, piattaforma, applicazione (**commi 1, 5, 6**);

L'art. 6 è rubricato "Sistema di allerta Covid-19".
E' decisivo riuscire a specificare esattamente 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 comma 1" o solo "piattaforma" …), 2) un'apposita applicazione e, per definizione, 3) i dati degli utenti.
Si ha un trattamento di dati personali, che conduce all'esigenza di adottare il presente articolo 6 quale base giuridica del trattamento, 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 dati degli 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 ad es. 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 osservazioni, derivano una serie cospicua di conseguenze stringenti in ordine alla disciplina di cui all'art. 6.

La prima. Si suggerisce di riformulare la prima parte del comma 1 nei termini che seguono: "… *è istituito il **sistema di allerta** Covid-19, costituito da una **piattaforma** unica nazionale per la gestione dei **dati** dei soggetti che, a tal fine, hanno installato, su base volontaria, un'apposita **applicazione** sui dispositivi di telefonia mobile*".
La seconda. E' necessario individuare i soggetti che sono responsabili della gestione della piattaforma e responsabili della gestione della applicazione, sia ai fini della applicazione del GDPR (ad es., 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" (comma 1);
il comma 5 dell'art. 6 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 si ritiene opportuno che l'art. 6 identifichi, 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. Il comma 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".
La disposizione è senz'altro corretta per quanto concerne il trattamento dei dati personali. Potrebbe essere ragionevole in riferimento all'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, 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 e, si ritiene, non ragionevole sotto il profilo della gestione di beni pubblici.
Di conseguenza, si suggerisce di **espungere** dalla norma almeno il riferimento alla piattaforma: "6. ~~*L'utilizzo dell'applicazione e della piattaforma, nonche'*~~ ogni trattamento di dati personali effettuato ai sensi al presente articolo ~~sono interrotti~~ *è interrotto* alla data di cessazione dello stato di emergenza …"

4. ***Osservazione 3***: l'esigenza di delineare un ruolo adeguato delle Regioni e dei Servizi sanitari regionali poiché rilevanti ai fini dell'efficacia del sistema di allerta (**comma 1**)

Il sistema di allerta e la sua effettiva funzionalità poggia sul corretto funzionamento dei SSR.
In particolare, l'allerta derivante dall'utilizzo della app è volta a condurre rapidamente le persone esposte al virus a verificare se hanno contratto il virus e, in tal caso, a quanto sembra, è proprio il medico del SSR che attribuisce e attiva il codice attraverso il quale si attiva 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.
E' noto che 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: diritto alla trasparenza, diritto di rettifica, diritto di limitazione e cancellazione, diritto di opposizione);
Sotto questo profilo, pertanto, il coinvolgimento istituzionale ed il coordinamento delle Regioni appare inevitabile, ai fini di garantire la funzionalità del sistema di allerta e il rispetto del principio di esattezza dei dati personali e del diritto di rettifica dei dati personali. In questo senso, la disposizione del comma 1 appare decisamente confusa e disordinata.
Si suggerisce pertanto una **revisione organica** della medesima disposizione, si ravvisa l'esigenza di un **coordinamento** con le disposizioni di cui alla bozza del Titolo I "Salute e sicurezza" del cd. decreto legge RILANCIO ("diramata" stanotte, con molteplici previsioni in materia di Fascicolo sanitario elettronico) e si

suggerisce, in mancanza, almeno quanto segue: "Il Ministro della salute e il Ministro per gli affari regionali e le autonomie*, sentita* ~~informano periodicamente~~ la Conferenza permanente per i rapporti tra lo Stato, le regioni e le province autonome di Trento e di Bolzano, *determinano* le modalità di accertamento e inserimento dei dati concernenti la verifica del contagio da parte dei servizi sanitari regionali e informano *sistematicamente la medesima Conferenza permanente* sullo stato di avanzamento del *sistema di allerta*".

5. ***Osservazione 4***: la qualificazione del rischio derivante dal trattamento e dalla costituzione della piattaforma, sotto i profili del rischio per i diritti dell'interessato (protezione e sicurezza dei dati personali) e del rischio per la sicurezza cibernetica dello Stato (cd. sovranità sui dati di rilievo pubblico e di interesse nazionale); a tal riguardo, inserire riferimento al Responsabile per la protezione dei dati personali in riferimento al trattamento dei dati personali ed alla struttura pubblica che cura gli aspetti di sicurezza informatica della piattaforma (**comma da aggiungere prima del comma 2**);

Il sistema di allerta istituito dall'art. 6 comporta tipologie di rischi di diversa natura.
L'art. 6, comma 2, fa esclusivo riferimento ai rischi elevati per i diritti e le libertà degli interessati, che rappresentano il presupposto – ai sensi dell'art. 35 del GDPR – in cui è necessario procedere alla valutazione di impatto sulla protezione dei dati.
Si ritiene opportuno che l'art. 6 delinei sinteticamente le tipologie di rischi e offra i criteri per individuare i soggetti tenuti ad affrontarli.
Si ritiene che l'istituzione del sistema di allerta comporti essenzialmente 3 tipologie di rischi.
I primi 2 sono connessi con il problema della protezione dei dati personali (**protezione e 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 (infrastruttura materiale e immateriale) nazionale sicura ed efficace (**sicurezza della infrastruttura digitale nazionale**).
L'individuazione dei rischi è funzionale ad identificare i soggetti, dotati di specifiche competenze, che debbono coadiuvare il titolare del trattamento e il titolare della infrastruttura a garantire la sicurezza e la protezione dei dati. Nel primo caso si tratta del Responsabile per la protezione dei dati personali; nel secondo caso si tratta dei soggetti pubblici che garantiscono la sicurezza cibernetica dello Stato.
Pertanto, si suggerisce di introdurre un breve comma da aggiungere prima del comma 2: "*Il Ministro della salute, 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, individua un Responsabile per la protezione dei dati personali, ai sensi degli articoli 37 e seguenti del Regolamento. Il Commissario di cui all'articolo 122 del decreto-legge 17 marzo 2020, n. 18, convertito, con modificazioni, dalla legge 24 aprile 2020, n. 27, considerati i rischi per la sicurezza cibernetica dello Stato, individua opportune misure tecniche e organizzative sin dalla fase di progettazione e realizzazione della piattaforma e dei relativi programmi informatici*".

6. ***Osservazione 5***: in ordine a singoli aspetti da tutelare (minori, persone decedute, pseudonimizzazione by default) in vista della valutazione di impatto (**comma 2**) e al divieto di trattare dati per finalità diverse da quelle comunicate agli utenti **(comma 3)**;

Al fine di completare il quadro degli aspetti da tutelare nella prospettiva della valutazione di impatto si suggeriscono le seguenti modifiche, concernenti la specifica considerazione dell'informativa da rendere ai minori, l'esigenza di esplicitare il dovere di pseudonimizzare in modo sistematico i dati degli utenti, la titolarità dei diritti riconosciuti dal GDPR non solo agli interessati, ma anche angli interessati che siano deceduti, come previsto dal vigente Codice per la protezione dei dati personali (ma non dal GDPR):

I. c. 2, lett. a), "… e sui tempi di conservazione dei dati; ***tali informazioni devono risultare comprensibili e facilmente accessibili anche a specifiche categorie di utenti, quali i minori***.";
II. c. 2, lett. c), "***pseudonimizzati per impostazione predefinita e, ove possibile, resi anonimi***";

III. c. 2, lett. f), "i diritti degli interessati ***e dei soggetti di cui all'articolo 2-terdecies del Codice in materia di protezione dei dati personali***, di cui agli articoli da 15 a 22 del Regolamento…";

A ciò si aggiunge la breve specificazione seguente:

IV. c. 3, "non possono essere trattati per finalità diverse da quella di cui al medesimo comma 1, ***ancorché compatibili***";

7. ***Allegati (indicazione)***.

Si allegano 4 brevissime note esplicative su app antitracciamento in altri ordinamenti rilevanti (Germania, Regno Unito, Francia, Sud Corea)