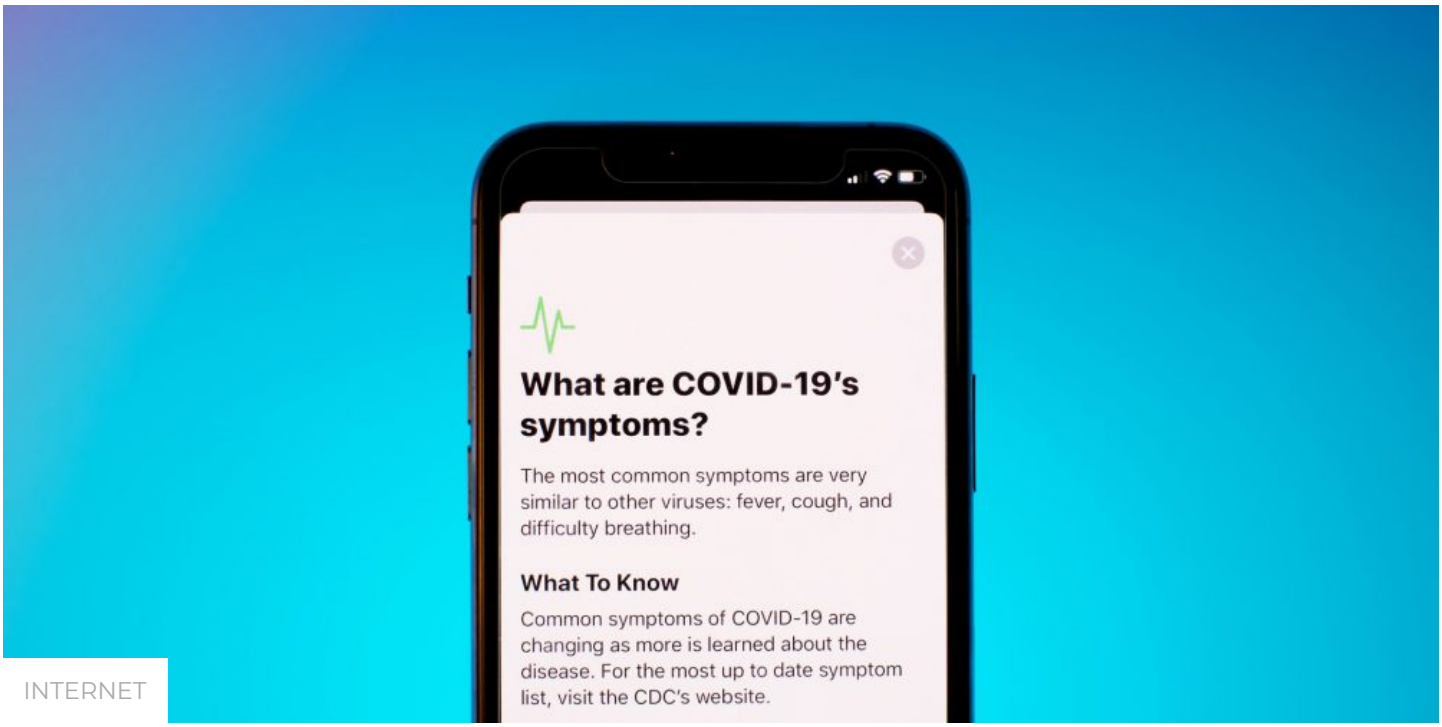
key4biz

ANALISI

Immuni, le 7 domande a cui il Governo deve ancora rispondere

di **prof. avv. Alessandro Del Ninno, Studio Legale Tonucci & Partners,**
4 Maggio 2020, ore 9:20



INTERNET

> *Ecco di seguito elencati una serie di dubbi sulla nuova disciplina normativa, con le relative richieste indirizzate al Ministero della Salute che, nella sua qualità di Titolare del trattamento dei dati personali, dovrebbe risolvere (i dubbi) ed esaminare (le richieste) ai fini di risposte concrete e trasparenti.*

Non cessa l'attività del Legislatore, che ha pubblicato sulla Gazzetta Ufficiale il testo del decreto legge 28/2020 che reca all'articolo 6 la disciplina del "*Sistema di allerta Covid-19*", con la istituzione di una piattaforma informatica nazionale unica che dialogherà con la *app* di *contact tracing* (di cui oggi apprendiamo che i test partiranno solo a fine mese....).

del trattamento dei dati personali, dovrebbe risolvere (i dubbi) ed esaminare (le richieste) ai fini di risposte concrete e trasparenti.

1. Dobbiamo aspettarci decreti e circolari per l'alert?

Primo: dobbiamo aspettarci decreti e circolari per le "*le modalità operative del sistema di allerta tramite la piattaforma informatica*" di cui parla l'articolo 6, comma 1 del decreto legge 28/2020? Difatti, la stessa nota del Commissario Arcuri con cui si dava atto della selezione di Bending Spoons come assegnatario dell'incarico di sviluppo della *app* di *contact tracing*, specificatamente menzionava la necessità di completare e "*definire il sistema di tracciamento nazionale*", che quindi si compone di una piattaforma unica nazionale e di app. Ma una cosa è una "*piattaforma unica nazionale per la gestione del sistema di allerta*", un'altra è una app di *contact tracing* che di quel sistema è una componente e che con la piattaforma dialoga: in che modo, nessuno ancora lo ha specificato...

2. Sui siti del ministero della Salute e dell'Innovazione cosa manca ancora

Secondo: vorremmo vedere pubblicata sul sito del Ministero della Salute e su quello del MIT, nell'ambito di una trasparenza fin qui totalmente mancata:

1. la Valutazione di Impatto preventiva che evidenzi tutte le "*misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato*" della piattaforma unica nazionale che sono promesse ai cittadini all'articolo 6.3;
2. gli atti di nomina a Responsabile del trattamento con tutte le specifiche istruzioni che il Ministero della Salute, come titolare del trattamento con riferimento a quelli svolti sulla piattaforma deve obbligatoriamente fornire ai sensi dell'articolo 28 GDPR e articolo 6.1 del decreto legge 28/2020 ai soggetti operanti nel Servizio nazionale della protezione civile, ai soggetti attuatori (per esempio: le Forze dell'ordine), all'Istituto Superiore di Sanità e alle strutture pubbliche e private accreditate che operano nell'ambito del Servizio sanitario nazionale (e che non siano atti di nomina burocratica e inutili, ma che contengano specifiche istruzioni a tutela dei cittadini i cui dati finiscono nella orwelliana "piattaforma unica nazionale").

Va comunque ricordato, sul tema della trasparenza, che almeno l'articolo 6, comma 5 prevede che "*I programmi informatici di titolarità pubblica sviluppati per la*

del decreto legislativo 7 marzo 2005, n. 82.".

3. Nello stesso server anonimi riferiti ad un soggetto e "*informazioni aggiuntive*" che consentono la reidentificazione?

Terzo: sembra quasi passata in secondo piano nel testo del decreto la questione centrale della anonimità o anonimizzazione del dato: l'articolo 6, comma 2 lettera a) del decreto 28/2020 chiarisce che nella Informativa da rendere ai cittadini ai sensi dell'articolo 13 del GDPR devono essere illustrate le (sole) "*tecniche di pseudonimizzazione*" utilizzate. Va ricordato che la "pseudonimizzazione" è un qualcosa di assai diverso dalla "anonimizzazione" (su cui basterebbe utilizzare come "bussola" il chiarissimo Parere 5/2014 dei Garanti europei sulle tecniche di anonimizzazione); l'articolo 4, n. 5 del GDPR chiarisce di fatti che per «pseudonimizzazione» si intende: *il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile*". Qui c'è tutto il tema della centralizzazione o decentralizzazione dei dati (è ovvio che se io in uno stesso server o piattaforma conservo codici anonimi riferiti ad un soggetto e "*informazioni aggiuntive*" che consentono la reidentificazione del codice anonimo del medesimo soggetto, non ho affatto alcuna anonimizzazione, ma solo dati pseudonimi e dunque personali); e di conseguenza:

4. Anonimità solo tanto sbandierata per convincere i cittadini ad utilizzare la piattaforma unica e a scaricare la app?

Quarto: il pericoloso articolo 6, comma 2, lettera (c) "*il trattamento effettuato per allertare i contatti sia basato sul trattamento di dati di prossimità dei dispositivi, resi anonimi oppure, ove ciò non sia possibile, pseudonimizzati*": il Ministero della salute chiarisca: 1) le tecniche che dovranno essere adottate per rendere anonimi i dati; 2) quali casi tecnici rendono impossibile il trattamento anonimo, poiché semplicemente asserire nella norma che se non è possibile (senza chiarire quando) è ammesso l'uso di dai pseudonimi e dunque personali e identificativi in via indiretta, svuota del tutto la anonimità tanto sbandierata per convincere i cittadini ad utilizzare la piattaforma unica e a scaricare la app. Ciò soprattutto se leggiamo l'impegno di cui all'articolo 6,

interessati cui si riferiscono i dati pseudonimizzati oggetto di trattamento". Ci spieghi anche il Ministero della Salute (lo può fare pubblicando la DPIA) come funzionerà tecnicamente e nello specifico il principio di *privacy by default* di cui si legge all'articolo 6, comma 2, lettera (b) ed in base al quale per impostazione predefinita i dati personali raccolti dall'applicazione di *contact tracing* dovranno essere esclusivamente quelli necessari ad avvisare gli utenti dell'applicazione di rientrare tra i contatti stretti di altri utenti accertati positivi al COVID-19;

5. Come sarà messo in sicurezza il server? Gli hacker non attendono altro se non attaccare piattaforme pubbliche

Quinto: visto che con riferimento alla piattaforma unica nazionale e alla app sono dirimenti e fondamentali le misure di sicurezza, vorremmo vedere nella DPIA in che modo il Ministero della Salute ha attuato nella pratica funzionale ed operativa di piattaforma ed app le misure idonee a garantire quanto promesso all'articolo 6, comma 2, lettera (d) del decreto 28/2020 e cioè la garanzia "*permanente*" della riservatezza, della integrità, della disponibilità dei dati e dei sistemi e della – importantissima, vista la misera fine di piattaforme pubbliche, tipo INPS, a cui di recente abbiamo assistito e visti i tanti hacker che non attendono altro se non attaccare piattaforme pubbliche...- "*resilienza dei sistemi e dei servizi di trattamento*". Leggendo questo comma a me pare – in assenza di dettagli tecnici – di leggere una vuota e burocratica formula (tra l'altro è un copia/incolla dell'articolo 32 del GDPR);

6. Sistema centralizzato o decentralizzato?

Sesto: sembra ancora non chiaro se si adotterà nel rapporto tra app e piattaforma pubblica (che ai sensi del comma 5 sarà gestita da SOGEI, la società pubblica che fornisce alla PA reti, infrastrutture e servizi di comunicazione elettronica) un sistema centralizzato o decentralizzato, visto che le opzioni restano aperte nella formula normativa di cui all'articolo 6, comma 2, lettera (e) "*i dati relativi ai contatti stretti siano conservati ANCHE nei dispositivi mobili degli utenti*," per il periodo strettamente necessario al trattamento, la cui "*durata è stabilita dal Ministero della salute*" (che dunque può anche modificare con decreto ministeriale il termine ultimo del 31 dicembre 2020 previsto per la definitiva cancellazione – che dovrà avvenire in automatico, ma non sappiamo come – di tutti i dati trattati);

Settimo: infine, altri dubbi emergono sull'articolo 6, come 3: che prevede – da un lato – che i dati raccolti attraverso l'applicazione di *contact tracing* possano essere utilizzati esclusivamente "*al solo fine di allertare le persone che siano entrate in contatto stretto con soggetti risultati positivi e tutelarne la salute attraverso le previste misure di prevenzione nell'ambito delle misure di sanità pubblica legate all'emergenza COVID-19*", ma dall'altro apre e fa salva la possibilità di utilizzo "*in forma aggregata o comunque anonima*" (opzione alternativa e duplice, e ancora una volta va ricordato che il trattamento aggregato può ben essere identificativo e non anonimo) dei dati raccolti su app e piattaforma unica nazionale per: 1) motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da 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; 2) fini di archiviazione nel pubblico interesse; 3) ricerca scientifica; 4) ricerca storica; 5) fini statistici.

È ovvio che in questa filiera di trattamenti rientrino anche soggetti privati (anche per motivi di sanità pubblica: si pensi ai soggetti privati convenzionati o accreditati al Sistema Sanitario Nazionale di cui pure parla la norma emergenziale di cui all'articolo 14, del decreto legge 14/2020) e non solo pubblici. Si pensi alla utilità di poter accedere – da parte di centri sanitari privati di ricerca, parte del SSN – ai dati sanitari di milioni di cittadini (sì aggregati, ma non certamente anonimizzati poiché tale certezza la norma non la dà assolutamente né obbliga ad una vera anonimizzazione, se solo per la cancellazione si parla all'articolo 6, comma 6 di "*dati resi definitivamente anonimi*"...).

Come cittadini dovremo confidare nell'articolo 6, comma 6 che anche per questi diversi trattamenti prevede che l''utilizzo dell'applicazione e della piattaforma, nonché ogni trattamento di dati personali (quindi anche il trattamento rappresentato dalla mera conservazione di dati raccolti precedentemente ai sensi del decreto) debbano interrompersi al massimo entro la data del 31 Dicembre 2020.

Ma nel Paese dei decreti milleproprorghe la certezza del rispetto dei termini non esiste...

prof. avv. Alessandro Del Ninno, Studio Legale Tonucci & Partners,

Quotidiano online sulla digital economy e la cultura del futuro

Direttore: ***Raffaele Barberio***
© 2002-2020 - Registrazione n. 121/2002. Tribunale di Lamezia Terme - ROC n. 26714 del 5 ottobre 2016
Editore ***Supercom*** *- P. Iva 02681090425*