GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Memoria del Presidente del Garante sul ddl di conversione in legge del decreto-legge 7 ottobre 2020, n. 125, recante misure urgenti connesse con la proroga della dichiarazione dello stato di emergenza epidemiologica da COVID-19 e per la continuità operativa del sistema di allerta COVID

Memoria del Presidente del Garante per la protezione dei dati personali sul ddl di conversione in legge del decreto-legge 7 ottobre 2020, n. 125, recante misure urgenti connesse con la proroga della dichiarazione dello stato di emergenza epidemiologica da COVID-19 e per la continuità operativa del sistema di allerta COVID, nonché per l'attuazione della direttiva (UE) 2020/739 del 3 giugno 2020

Commissione 1a (Affari Costituzionali) del Senato della Repubblica

(19 ottobre 2020)

1. Il contesto e i precedenti interventi del Garante

Desidero anzitutto ringraziare la Commissione per il contributo richiesto, che consentirà di evidenziare alcuni profili di particolare interesse del “contact tracing” realizzato attraverso il sistema di allerta nazionale di cui all’art. 6 del decreto-legge n. 28 del 2020 convertito, con modificazioni, dalla legge n. 70 del 2020.

Il tema del tracciamento digitale dei contatti, sviluppato in Italia mediante l’app “Immuni”, ha rappresentato e tuttora rappresenta una questione dirimente nel governo dell’emergenza, espressiva come poche altre del bilanciamento tra libertà individuali e interessi collettivi, reso tanto più complesso quanto più rilevante nel contesto pandemico.

In gioco vi sono due diritti fondamentali, quali quello alla salute, anche nella sua componente metaindividuale di “interesse della collettività” alla sanità pubblica e quello alla protezione dei dati personali, qualificato come diritto “di libertà”, autonomo dal tradizionale diritto al rispetto della vita privata, dall’articolo 8 Cdfue.

Non potendosi configurare gerarchie ‘tiranniche’ tra i diritti fondamentali (Corte cost., sent. 85/2013), anche quelli alla salute e alla protezione dati esigono un bilanciamento tale da salvaguardarne il contenuto essenziale, che l’art.. 52 Cdfue qualifica come inviolabile.

La ricerca di tale equilibrio ha rappresentato, appunto, uno dei tratti qualificanti le posizioni assunte dall’Autorità, rispetto alle varie disposizioni adottate nei mesi scorsi per il contrasto della pandemia: da quelle inerenti l’ambito di circolazione dei dati personali, anche sanitari, tra i soggetti coinvolti nell’azione di prevenzione (artt. 14 d.l. 14/2020 e, poi, 17-bis d.l. 18/2020) sino, appunto, al sistema di tracciamento digitale dei contatti disciplinato dall’art. 6 del d.l. 28, che si è modellato sulle indicazioni rese dal Garante,

sin dall'audizione in Commissione trasporti della Camera, l'8 aprile.

Già in quella sede si erano indicati, infatti, i parametri essenziali di legittimità degli strumenti di contact tracing, individuabili in primo luogo nella funzionalizzazione a fini di utilità sociale (contenimento dei contagi), piuttosto che a fini repressivo-sanzionatori, nella necessaria parzialità- dovendo tali soluzioni integrarsi in una più ampia e complessa strategia di prevenzione sanitaria- nonché nel rispetto delle norme di protezione dati quale condizione, oltretutto, indispensabile per la necessaria fiducia sociale in tali misure.

Il Garante aveva, quindi, sottolineato l'esigenza che il sistema di contact tracing fosse normato per legge, per l'impatto della misura sulla privacy individuale e per l'esigenza di un modello unitario di disciplina tale da assorbire (anche in ragione della attribuzione della materia alla potestà legislativa statale) iniziative degli enti territoriali che allora si annunciavano come potenzialmente disfunzionali. Il sistema, a titolarità pubblica, avrebbe dovuto basarsi – sottolineava il Garante – su di un'adesione realmente volontaria (escludendo dunque ogni tipo di pregiudizio nei confronti di quanti non intendessero prestarla), su dati non di geolocalizzazione ma di mera prossimità dei dispositivi (assai meno significativi e "invasivi" dei primi), quantomeno pseudonimizzati, su di un meccanismo delocalizzato di archiviazione delle informazioni, nonché su solide garanzie di sicurezza informatica. Si sottolineava poi l'esigenza di temporaneità del sistema, da definirsi per relationem con riferimento alla persistenza della condizione emergenziale e la necessaria limitazione della raccolta ai soli dati e al solo periodo di conservazione indispensabile a fini epidemiologici.

Con il parere (del 29 aprile) sullo schema di disposizione che sarebbe stata inserita nel decreto-legge n. 28/20 per la disciplina del sistema di contact tracing digitale, si è preso favorevolmente atto della scelta del Governo in favore di un sistema di notifica da esposizione a contatti significativi con soggetti positivi, fondato sulla libera adesione di quanti scarichino sul proprio dispositivo una specifica app e su di una piattaforma di allerta nazionale istituita presso il Ministero della salute, con forte grado di pseudonimizzazione dei dati, nonché divieto di comunicazione dei dati a terzi .

Sono state, inoltre, positivamente valutate le misure previste dalla norma per assicurare la determinatezza ed esclusività dello scopo: il tracciamento dev'essere finalizzato esclusivamente al contenimento dei contagi, escludendo fini ulteriori, ferme restando le possibilità di utilizzo a fini di ricerca scientifica e statistica, purché nei soli termini generali previsti dal Regolamento Ue 2016/679, valorizzando dunque anche in questo senso la destinazione solidaristica dei dati.

Infine, si è condivisa (in quanto conforme alle indicazioni già rese) la previsione della temporaneità del sistema, con interruzione delle attività della piattaforma alla data di cessazione dello stato di emergenza e termine finale di salvaguardia, nonché con cancellazione o definitiva anonimizzazione dei dati raccolti.

Con il provvedimento autorizzatorio sulla valutazione d'impatto del 1° giugno, inoltre, l'Autorità, preso favorevolmente atto della scelta in favore di un sistema di gestione in locale delle notifiche di esposizione, ha indicato misure ulteriori volte a rafforzare le garanzie del trattamento anche sotto il profilo della sicurezza informatica, della trasparenza e dell'informazione degli utenti.

Essi devono essere, in particolare, resi edotti di profili non secondari quali ad esempio il rischio di falsi positivi (o anche negativi), non potendo il sistema distinguere tra contatti pericolosi perché avvenuti, ad esempio, in assenza di dispositivi di protezione e contatti, pur qualificati per durata e vicinanza, ma sicuri perché tenutisi all'aperto o in condizione di protezione. Va infatti ricordato che, a rigore, Immuni rappresenta un'app funzionale a un sistema di notifica rispetto ad esposizioni rischiose, che dunque non segue movimenti, ma riconosce eventi (il contatto qualificato e significativo, almeno in astratto, sotto il profilo epidemiologico).

Si è avuto modo di rilevare anche come, in caso di positività del tampone, l'avvio del sistema di tracciamento dei contatti sia comunque subordinato a una scelta volontaria del soggetto, che dovrà fornire all'operatore sanitario la propria OTP per consentire appunto al sistema di inviare gli alert ai potenziali contagiati. Tale profilo non è stato modificato dal dPCM del 18 ottobre, che si limita a intervenire sugli adempimenti degli operatori sanitari.

Questo tassello ulteriore della disciplina (concretamente attuata con decreto ministeriale su cui, parimenti, è stato acquisito il parere del Garante) rappresenta il completamento e la garanzia finale della effettiva volontarietà del sistema di contact tracing digitale, l'adesione al quale esprime, in ogni sua fase e in ogni sua conseguenza, una scelta libera (tanto quanto responsabile) del singolo, con espressa esclusione normativa di ogni possibile pregiudizio in caso di mancata adesione al sistema stesso.

Più nel dettaglio, ai fini della valutazione dell'ottemperanza alle prescrizioni rese, con il provvedimento del 1° giugno il Garante ha richiesto al Ministero della salute di fornire riscontro, nei successivi trenta giorni, sui seguenti profili:

- indicazione puntuale dell'algoritmo e dei parametri di configurazione utilizzati dal sistema;

- adeguata informazione degli utenti in ordine alla possibilità (di cui si è detto sopra) che, per le particolari circostanze del contatto, la notifica da esposizione non rifletta un'effettiva condizione di rischio;

- accessibilità della funzione di temporanea disattivazione dell'app;

- adeguata protezione degli analytics nel backend di Immuni, evitandone ogni forma di riassociazione a soggetti identificabili;

- precisazione, nell'informativa, delle operazioni effettuate con riferimento agli analytics di tipo Epidemiological Info e ai dati personali raccolti in relazione alle diverse categorie di interessati;

- adeguatezza dell'informativa e del messaggio di allerta anche con riferimento alla capacità di discernimento degli utenti minorenni, ancorché ultra-quattordicenni;

- adeguatezza delle informazioni rese agli utenti in relazione alle caratteristiche della fase di sperimentazione;

- integrazione della valutazione d'impatto e dell'informativa in relazione alle modalità di esercizio dei diritti di cancellazione e di opposizione;

- integrazione, sulla base del principio di responsabilizzazione, della valutazione d'impatto con la descrizione del ruolo e delle operazioni ascrivibili ad altri soggetti suscettibili di coinvolgimento nel Sistema Immuni;

- commisurazione dei tempi di conservazione degli indirizzi ip nella misura strettamente necessaria al rilevamento di anomalie e di attacchi;

- garanzia del tracciamento delle operazioni compiute dagli amministratori di sistema sui sistemi operativi, sulla rete e sulle basi dati;

- adozione di misure tecniche e organizzative per mitigare i rischi derivanti dall'upload di TEK non riferite a soggetti positivi a seguito di eventuali errori materiali o diagnostici.

A seguito del riscontro fornito (in termini) il 23 giugno, si sono avviati incontri tra gli Uffici volti a individuare le migliori soluzioni – tuttora all'esame dell'Autorità - ad alcune difficoltà emerse nell'adempimento, in particolare, delle prescrizioni di cui ai punti quarto, nono, decimo, undicesimo e dodicesimo del precedente elenco. Medio tempore, l'esigenza di garanzia dell'interoperabilità ha reso necessaria l'adozione di una nuova valutazione d'impatto, che risulta pervenuta all'Autorità il giorno 16 ottobre.

E' stata inoltre svolta, dall'Ufficio, un'analisi in ordine ai rischi- paventati da notizie di stampa- di vulnerabilità del sistema rispetto a c.d. replay attack, idonei a ingenerare false notifiche di esposizione al rischio. Allo stato non pare ravvisabile tale specifica vulnerabilità (e la conseguente esigenza di ulteriori misure), in quanto questo tipo di attacchi, presupponendo l'illecito impossessamento del dispositivo mobile e la conseguente modifica della configurazione, sarebbe imputabili a condotte penalmente illecite realizzate nel contesto (che non pare ipotizzabile come rischio tipico o connaturato al sistema) di una più ampia serie di delitti, anche contro la riservatezza informatica e delle comunicazioni, la fede pubblica ecc.

E', invece, tuttora in corso l'istruttoria relativa ad alcuni casi, riportati da notizie di stampa, relativi all'omessa attivazione della procedura di caricamento delle Tek dei soggetti risultati positivi al Covid-19 prevista dal sistema di allerta. A superare queste omissioni mira, evidentemente, la previsione del dPCM del 18 ottobre relativa agli adempimenti degli operatori sanitari rispetto a pazienti i quali dispongano dell'app Immuni.

Va infine sottolineato come il 2020 Data Protection Report, adottato in questo mese dal Consiglio d'Europa, in ordine alle soluzioni digitali per il contrasto della pandemia, riconosca il contributo positivo fornito dal Garante nel procedimento legislativo e, in termini più generali, nell'ambito dell'elaborazione, da parte del Governo, di un sistema di contact tracing fondato su di una sinergia e un equo bilanciamento tra sanità pubblica e privacy.

2. La novella apportata del decreto-legge

In tale contesto si inserisce la novella di cui all'articolo 2 del decreto-legge in conversione, che reca due essenziali innovazioni: la previsione dell'interoperabilità- previa valutazione d'impatto privacy- del sistema di allerta nazionale con le piattaforme che operano, con le stesse finalità, nel territorio dell'Unione europea (comma 1, lettera a), nonché il differimento del termine finale per l'utilizzo dell'applicazione e della piattaforma- prima commisurato al termine di efficacia della dichiarazione dello stato di emergenza nazionale, comunque non oltre il 31 dicembre 2020 – sino alla cessazione delle esigenze di protezione e prevenzione della sanità pubblica, individuate con dPCM e, comunque, entro il 31 dicembre 2021.

Come rilevato nella Relazione illustrativa del disegno di legge di conversione, la redazione della norma è stata preceduta dal parere del Garante reso, sia pur informalmente, dapprima con nota del 21 settembre, con la quale sono state fornite alcune indicazioni sul testo inizialmente proposto, alle quali poi il Governo, nella stesura finale della disposizione, si è sostanzialmente conformato.

In quella sede, in particolare, si è ricordata l'opportunità di verificare l'uniformità, rispetto a quelle accordate dal nostro sistema di allerta, delle garanzie assicurate dalle piattaforme utilizzate negli altri Stati. Si è inoltre sottolineata l'esigenza di limitare, ai soli necessari, i dati scambiati, comunque in forma pseudonimizzata, relativi agli utenti risultati positivi al virus, con le piattaforme degli altri Stati.

Infine, si è rappresentata l'opportunità di integrare tali garanzie ulteriori nella specifica valutazione d'impatto da sottoporre alla valutazione del Garante, precedentemente all'inizio del trattamento.

Con riferimento, invece, alle modifiche originariamente proposte al regime di efficacia temporale dell'attività della piattaforma, si è manifestata l'esigenza di non sganciare il termine finale dalla condizione emergenziale, in ragione del carattere derogatorio (e quindi eccezionale, appunto non ordinario) della disciplina sul contact tracing.

All'esito di ulteriori interlocuzioni, il Governo ha quindi proposto la versione (che sarebbe poi risultata definitiva) della disposizione, ritenuta dal Garante condivisibile per le ragioni di seguito esposte.

La previsione dell'interoperabilità rappresenta la conseguenza coerente della concezione del sistema di allerta nazionale quale parte di una strategia europea di contrasto della pandemia. Tale caratteristica dei sistemi è, infatti, stata prefigurata sin dallo scorso aprile con la raccomandazione (C(2020)2296), relativa a un pacchetto di strumenti comuni dell'Unione europea per l'uso della tecnologia e dei dati, con cui la Commissione, al fine di realizzare un approccio europeo comune alla pandemia, ha sollecitato « l'interoperabilità in tutta l'Unione europea » dei sistemi di tracciamento.

Il 13 maggio scorso gli Stati membri dell'Ue, con il sostegno della Commissione europea, hanno concordato, nell'ambito dell'eHealth Network, gli orientamenti per l'interoperabilità transfrontaliera delle applicazioni di tracciamento nell'Unione.

L'interoperabilità tra le piattaforme di tracciamento nel territorio dell'Unione europea è stata, poi, oggetto della decisione di esecuzione (UE) 2020/1023 della Commissione, del 15 luglio scorso. Tale decisione costituisce la base giuridica che legittima appunto, in ambito europeo, l'interoperabilità delle applicazioni mobili nazionali di tracciamento dei contatti e di allerta (cosiddetto gateway federativo), con riferimento agli Stati membri i quali abbiano aderito a questa forma di collaborazione specifica.

L'interoperabilità dei sistemi di allerta rappresenta dunque, in questo senso, una misura funzionale tanto al rafforzamento delle attività di contenimento dei contagi – in quanto consente di ricostruire la filiera dei contatti anche in caso di mobilità intraeuropea del soggetto – quanto alla libertà di circolazione dei cittadini nel territorio dell'Unione. Tale diritto (e principio, ad un tempo, fondativo dell'ordinamento europeo) rischia, del resto, di essere oltremodo pregiudicato dal contesto pandemico e, in questo modo, può essere in certa misura salvaguardato.

L'impatto che l'interoperabilità dei sistemi di tracciamento inevitabilmente determina sulla protezione dei dati personali è, del resto, adeguatamente bilanciato non soltanto dalla tendenziale analogia delle garanzie adottate dai Paesi membri sul punto – in particolare a seguito della citata decisione di esecuzione- ma anche dalle prescrizioni che il Garante, in sede appunto di esame della valutazione d'impatto, potrà rendere per rafforzare le tutele almeno sotto il profilo interno.

Riguardo, invece, alle modifiche di cui alla lettera b) del comma 1, la previsione del dies ad quem di operatività della piattaforma sino alla cessazione delle esigenze di protezione e prevenzione della sanità pubblica, si conforma alla necessità, rappresentata dal Garante, di ancorare il termine di efficacia, sia pur per relationem, alla perdurante condizione pandemica.

In questo senso, la modifica apportata dal decreto-legge si conforma a tale modello, in quanto assume, tra i parametri cui ancorare l'operatività del sistema, quello sostanziale relativo alla persistenza delle esigenze di prevenzione sanitaria e quello, di ordine formale-normativo, dell'individuazione della sussistenza delle esigenze stesse con dPCM. La garanzia di ultima istanza è, poi, affidata alla previsione, con clausola di salvaguardia, del termine finale di operatività del sistema al 31 dicembre 2021.

Il differimento del termine di efficacia del sistema si fonda, pertanto, su di un doppio ordine di criteri. In primo luogo, rilevano esigenze di sanità pubblica connesse alla necessità di ricostruire, anche digitalmente, la filiera dei contatti, rispetto alla quale il Governo assume la responsabilità di dichiararne la sussistenza con dPCM. In secondo luogo, la garanzia rispetto al rischio di "normalizzazione dell'emergenza" è affidata alla previsione del termine ultimo del 31 dicembre 2021 entro il quale, appunto, prescindendo da ragioni di ordine sostanziale, l'attività del sistema di tracciamento deve cessare.

Così descritte, in estrema sintesi, le ragioni sottese al parere favorevole reso dal Garante sullo schema di norma allora proposta e poi, come anticipato, appunto rifluita nel testo del decreto-legge, non può che confermarsi la posizione allora espressa. Anche per effetto del recepimento delle indicazioni rese dall'Autorità, infatti, entrambe le modifiche apportate alla disciplina del contact tracing sottendono un bilanciamento ragionevole tra esigenze di sanità pubblica e protezione dei dati personali, conforme a quella convergenza tra istanze personaliste e vocazione solidarista su cui si fonda il nostro ordinamento.