Prof. Avv. Giovanni Comandé
Professore Ordinario di Diritto Privato Comparato
Scuola Superiore Sant'Anna, Pisa (Italy)

Sintesi Audizione presso Commissione Giustizia della Camera dei Deputati 19 maggio 2020 in materia di Covid-19 e trattamento dei dati personali.

Molti dei dubbi legittimamente sollevati in questi giorni rispetto all'adozione di Sistema di allerta Covid-19 di cui all'art. 6 D.L. 28/2020 sono tecnicamente chiariti dalla documentazione resa pubblica anche a vantaggio della comunità scientifica (https://github.com/immuni-app/documentation), dal Garante Privacy, nonché dalla documentazione delle istituzioni comunitarie.

1. ***Sul diritto fondamentale alla protezione dei dati.***

Tale diritto è strumentale alla protezione del principio di uguaglianza perché **preserva le informazioni da abusi e discriminazioni** che alimentano le diseguaglianze. Esso in linea con il diritto alla salute ed alla tutela della vita permette di avvisare i potenziali contagiati - salvando vite - senza esporli a limitazioni di accesso ai servizi sanitari, per esempio, inaccettabili sul piano costituzionale. Così, il diritto fondamentale alla protezione dei dati personali declinato dall'art. 8 della Carta dei diritti fondamentali dell'Unione Europea **riflette il volto "dei doveri inderogabili di solidarietà politica, economica e sociale"** e della centralità della **dignità della persona** insiti nella nostra architettura costituzionale. La privacy non impedisce: abilita!

I principi. In questo quadro, l'**art. 6 del D.L. 28/2020** non prefigura un diritto eccezionale ma **gestisce le eccezionali esigenze di una pandemia** in linea con il Reg. Europeo 2016/679, di seguito **"GDPR"**, con le indicazioni del Parlamento Europeo e della Commissione Europea, e con quelle tecniche del Comitato europeo per la protezione dei dati.

Per questo **i principi operativi** in cui il sistema di allerta Covid-19 si declina, a partire **dall'art. 5 GDPR** («liceità, correttezza e trasparenza, finalità, esattezza, minimizzazione, limitazione della conservazione, integrità e riservatezza dei dati) costituiscono punti di riferimento ineludibili e strumentali all'effettività del servizio offerto dalla App in questione.

In questo senso, i suddetti principi sono riflessi nell'**art. 6 del DL 28/2020**. *Al comma 3, appare* ***opportuno modificare la dizione*** *"ai sensi degli articoli 5, paragrafo 1, lettera a) e (...)"* ***in "ai sensi degli articoli 5 e (…)"***, stante la permanente (e necessaria applicabilità) di tutti i principi descritti dall'art.5 GDPR per evitare confusioni interpretative.

2. *Sul trattamento di "dati sufficientemennte anonimi".*

La "**identificabilità di una persona**" (ovvero ciò che rende personale il dato e dunque **non anonimo**) dipende da tutti i mezzi "di cui il titolare del trattamento o un terzo può ragionevolmente avvalersi per identificare detta persona fisica direttamente o indirettamente", "tra cui i costi e il tempo necessario per l'identificazione…[le] tecnologie disponibili al momento del trattamento, …[e gli] sviluppi tecnologici" (così il Considerando 26 GDPR, poi riassunto nel c.d. Breyer test dalla Corte di giustizia dell'Unione europea). In questo senso l'art. 6 D.L. 28/2020 offre una base normativa per il dispiegamento di una piattaforma basata su **dati "sufficientemente anonimi"**, minimizzando i rischi per la privacy dei cittadini.

Email: g.comande@santannapisa.it - tel.. +39--050-7916947
Website: www.lider-lab.eu -Webpage: https://www.santannapisa.it/it/giovanni-comande

Prof. Avv. Giovanni Comandé
Professore Ordinario di Diritto Privato Comparato
Scuola Superiore Sant'Anna, Pisa (Italy)

Le **condizioni** del sistema indicate nell'art. 6 (anche e grazie al monitoraggio continuo della Valutazione di Impatto sui dati Personali ai sensi dell'art. 35 GDPR operata dall'Autorità Garante per la protezione dei dati personali) allineano il sistema di allerta al principio di **miniminizzazione** e ai criteri di *privacy by design e by default* prevedendo **la raccolta** dei soli **dati di prossimità** dei dispositivi, il loro trattamento **in forma anonima** o (quando non è possibile) in **forma pseudo anonima escludendo il ricorso a dati di geolocalizzazione** (NB l'indicazione della provincia in fase di registrazione *non* è un dato di geolocalizzazione[1] e *non* permette *per se* la reidentificazione) e limitandone la **conservazione** al **tempo strettamente necessario** ai fini del perseguimento dello scopo indicato (cancellazione dei dati ogni 16 giorni sui dispositivi, immediatamente dopo l'uso nel server di allerta e ritenzione solo di dati aggregati ed anonimi).

3.Volontarietà del sistema.

Per quanto attiene al tema dell'**obbligatorietà di adesione** a sistemi di tracciamento, la stessa è **da escludersi** tra l'altro per 1) limiti costituzionali (che sarebbero molto forti nel nostro ordinamento, così come lo sono nel resto dell'UE); 2) impraticabilità tecnico-giuridica di ogni forma di coercizione all'uso; 3) elevati rischi di abuso e creazione di precedenti contrari alle regole democratiche; 4) contrarietà al rispetto della "essenza dei diritti e delle libertà fondamentali", ed in particolare assenza di necessità e proporzionalità della misura in una società democratica; 5) impossibilità dovuta al *digital divide* che minerebbe il principio di uguaglianza (art. 3 Cost.) interferendo con i principi di inclusività e solidarietà emergenti dall'architettura costituzionale, non trovando giustificazione in termini di bilanciamento tra diritti e libertà. Al contrario, la **facoltatività** dell'adesione all'App (unita alle salvaguardie sopra chiarite) rispetta i criteri di **efficacia, necessità e proporzionalità** nell'intervenire sul diritto fondamentale alla protezione dei dati personali. **Nessun Paese europeo ha adottato/sta adottando la obbligatorietà** dell'App di Tracciamento.

4. Decentralizzazione del sistema

Solo il Regno Unito e forse e (solo in parte) la Francia hanno adottato un sistema più centralizzato di tracciamento. Entrambi i sistemi comportano una serie di vantaggi e svantaggi sia per la prevenzione sia per la privacy. La differenza fondamentale tra ***sistema** c.d. **centralizzato e sistema c.d. decentralizzato*** consiste nei dati (sempre pseudoanonimi nella peggiore delle ipotesi) inviati al server (presente in entrambi i modelli). Nel sistema **decentrato** l'applicazione invia ad un server **un elenco dei propri pseudoidentificatori assieme ad alcune informazioni epidemiologiche**. Nel sistema accentrato l'applicazione invia al server una lista dei pseudoidentificativi con cui si è entrati epidemiologicamaente in contatto. In ogni caso le comunicazioni avvengono in modo anonimo.

Quanto sopra detto, permette di concludere che **la norma in oggetto** (e la relativa App di allerta di rischio di contagio) **rispetta i criteri di efficacia, necessità e proporzionalità** nell'intervenire sul diritto fondamentale alla protezione dei dati personali.

[1] Dati di geolocalizzazione sono la latitudine, longitudine o altitudine del luogo in cui si trova l'attrezzatura terminale; la direzione di movimento dell'utente; oppure l'ora in cui sono state registrate le informazioni sulla località e questi non sono condivisi col server centrale