



**UNIVERSITÀ  
DI TRENTO**

DIPARTIMENTO

**FACOLTÀ DI GIURISPRUDENZA**



**Università di Trento  
Facoltà di Giurisprudenza  
Diritto civile A-J  
2020-2021  
Prof. Roberto Caso**

**Lezione 19 – Contrasto alla pandemia,  
tracciamento digitale e protezione dei dati personali**

Questa lezione ha tre scopi:

1. accennare a come cambia il bilanciamento tra tutela della salute e protezione dei dati personali nel diritto dell'emergenza;
2. introdurre il tema della sorveglianza digitale come mezzo di prevenzione e contrasto all'epidemia con particolare riferimento alle app di tracciamento di contatti tra persone;
3. descrivere sommariamente i problemi posti sul piano della protezione dei dati personali dall'app Immuni.

## **Parte 1 – Il bilanciamento tra tutela della salute e protezione dei dati personali nel diritto dell'emergenza**

A proposito del bilanciamento tra tutela della salute e protezione dei dati personali nel diritto dell'emergenza da COVID-19 Giorgio Resta scrive quanto segue [Resta 2020]:

“Una componente importante di questo nuovo diritto dell'emergenza, la quale merita una particolare attenzione, è costituita dalla disciplina 'semplificata', o a seconda dei punti di vista 'd'eccezione', della tutela dei dati personali. Questa, composta da tasselli normativi promananti da fonti diverse e operanti su diversi registri (sovranazionale, nazionale, regionale), è essenzialmente preordinata a rendere più capillare ed efficace la sorveglianza epidemiologica, più agevole lo scambio di informazioni tra le autorità sanitarie, più rapido e meno oneroso il processo di sperimentazione clinica di nuovi medicinali e dispositivi medici, in ultimo più fluido ed effettivo l'intero sistema di gestione della crisi sanitaria in atto” [...].

“Ovviamente quanto maggiore è la compressione del livello ordinario delle garanzie, sia pure per inoppugnabili fini di interesse pubblico, tanto più alto è il rischio che il diritto alla protezione dei dati personali – pilastro centrale del sistema contemporaneo dei diritti fondamentali – soffra delle limitazioni eccessive e non facilmente revocabili (anche sul piano cognitivo e culturale, che non è certo il meno rilevante, perché meno effimero rispetto al periodo di vigenza di una norma) una volta terminata l'emergenza”.

In Italia il sistema delle fonti del diritto dell'emergenza è basato essenzialmente sui seguenti strumenti normativi [Resta 2020]:

- a) Dichiarazione dello stato di emergenza, deliberata dal Consiglio dei Ministri il 31 gennaio 2020 ai sensi dell'art. 7, comma 1, lett. c), d.lgs. n. 1 del 2018 (prorogata il 7 ottobre 2020);
- b) Ordinanze emanate dal Capo del Dipartimento della protezione civile “in deroga a ogni disposizione vigente e nel rispetto dei principi generali dell'ordinamento giuridico”;
- c) Decreti legge;
- d) DPCM.

Il quadro normativo è volto a “limitare il godimento di diritti e libertà fondamentali con la finalità di contenimento dell'epidemia e contrasto dei rischi per la sicurezza e la salute dei cittadini”. Alcune limitazioni toccano il sistema della protezione dei dati personali” [Resta 2020].

Le finalità delle limitazioni del diritto alla protezione dei dati personali sono le seguenti [cfr. Resta 2020]:

I) disporre di maggiori possibilità di condividere dati personali tra soggetti pubblici e privati per il contrasto dell'epidemia, nonché di maggiori possibilità di condividere dati personali con altri paesi europei e organizzazioni internazionali;

II) porre obblighi di comunicazione di dati personali da parte dell'interessato;

III) semplificare gli obblighi del titolare del trattamento dei dati personali (ad es. sul piano della trasparenza e degli obblighi informativi).

“Siamo quindi in presenza di una pluralità di norme che integrano e in parte modificano il sistema della protezione dei dati, al fine di bilanciare il rispetto dell'autodeterminazione informativa con le esigenze impellenti di tutela della salute pubblica in una situazione di emergenza sanitaria” [Resta 2020].

Ma va precisato che già i principi del GDPR consentono di svolgere attività di tracciamento.

“I principi stabiliti dal Regolamento 2016/679 agli artt. 6, 9 e 23 possono di per sé legittimare non soltanto il trattamento dei dati relativi a persone infette, ma anche le attività di ricerca della catena di contagio intraprese a vari livelli dal medico di famiglia, dalle strutture ospedaliere, o dalle altre strutture sanitarie coinvolte” [Resta 2020].

## **Parte 2 – La sorveglianza digitale come mezzo di prevenzione e contrasto all'epidemia: le app di tracciamento**

La capacità di tenere sotto controllo l'epidemia dipende, oltre che dai comportamenti personali, dalla forza e dall'efficienza di un sistema sanitario. Per questo, le soluzioni tecnologiche possono aiutare ma di per sé stesse non sono risolutive [cfr. Resta 2020].

Il tracciamento delle persone entrate in contatto con infetti (*contact-tracing*) è ritenuto – fin quando l'epidemia non è fuori controllo – uno strumento efficace.

Il tracciamento può essere fatto solo da personale sanitario specializzato oppure può essere basato sul tracciamento digitale (*tracking*) mediante software (app da scaricare su smartphone).

La via del tracciamento digitale per diverse finalità – non solo legate alla ricostruzione della catena dei contagi – è stata imboccata precocemente nei paesi asiatici come Cina, Taiwan, Corea del Sud, Singapore. I risultati delle strategie basate sul tracciamento digitale sono altalenanti. Di sicuro, si tratta di uno strumento che, come si accennava all'inizio di questa seconda parte della lezione, da solo non può esaurire le misure di prevenzione e contrasto. Inoltre, c'è da tener presente che alcuni dei paesi asiatici nominati non si fondano su sistemi democratici e che in ogni caso in Asia il contesto culturale e tecnologico è marcatamente differente da quello occidentale.

Perché ricorrere al tracciamento digitale? Lo spiega Giorgia Bincoletto [2020] con riferimento ai benefici di un tale approccio:

- i. supplire ai possibili vuoti di memoria del soggetto potenzialmente contagioso sui soggetti che ha incontrato;
- ii. far emergere i vari contatti sconosciuti al soggetto potenzialmente contagioso, che potrebbero essere a rischio;
- iii. comunicare rapidamente il rischio di contagio alla rete di contatti [...].”

Accanto ai benefici, occorre tener presenti i maggiori rischi di violazione della protezione dei dati personali. Si tratta infatti di strumenti che, se non correttamente regolamentati, possono instaurare un capillare e permanente sistema di sorveglianza di massa.

Inoltre, occorre considerare i seguenti punti:

- a) i dati sanitari sono una tipologia di “petrolio” (materia prima fondamentale) particolarmente appetibile per il capitalismo digitale [Bincoletto, 2020];
- b) i rischi in termini di sicurezza informatica sono riducibili ma non eliminabili; all’aumentare della diffusione delle app aumenta anche la minaccia alla sicurezza.

Le architetture di tracciamento digitale basate su app sono essenzialmente due [Resta 2020].

Centralizzata: le autorità sanitarie, accedendo direttamente ai dati conservati su una piattaforma centralizzata (auspicabilmente pubblica) e adoperando una chiave di decrittazione in loro possesso, possono identificare i contatti a rischio e contattarli con celerità per assumere le misure conseguenti.

Decentralizzata: la app invia automaticamente un segnale anonimo di avviso ai contatti stretti, i quali vengono invitati a rivolgersi al personale sanitario per le opportune valutazioni.

L’Unione Europea è intervenuta nella materia con una serie di documenti. I principali sono i seguenti:

- Raccomandazione della Commissione UE dell’8 aprile 2020 C (2020)2296 final, 8/04/20;
- EDPB, Linee guida 04/2020;
- Parlamento Europeo, Risoluzione 17 aprile 2020 n.2020/2616(RSP).

Da tali documenti si deducono alcuni orientamenti degli organi europei sulle basi giuridiche e alcuni punti fermi sui requisiti del trattamento dei dati personali che non dovrebbero essere travalicati dalle regolamentazioni interne ai paesi membri.

Le basi giuridiche del trattamento sono alternativamente le seguenti [Resta 2020]:

- il consenso dell’interessato (art. 6 e 9 GDPR; art. 5 Direttiva 2002/58/CE);
- o la finalità di contrasto all’epidemia, nell’interesse pubblico rilevante, in particolare, per fini di tutela della salute (art. 6, p.1, lett. d), e), e 9, par. 2, lett. i) GDPR; art. 15 Direttiva 2002/58/CE).

I punti fermi sono i seguenti [Resta [2020]:

- volontarietà dell’uso dell’app;
- anonimizzazione dei dati;
- esclusione della geolocalizzazione;
- per le app multifunzione (diagnostica, tracciamento ecc.), possibilità di esprimere consenso differenziato per ciascuna funzione;
- periodo limitato di conservazione dei dati (non oltre l’emergenza);
- conferma del divieto di decisioni a carattere interamente automatizzato (ex art. 22 GDPR).

### **Parte 3 – La app Immuni e la protezione dei dati personali**

In Italia l'introduzione del tracciamento digitale si deve all'art. 6 del d.l. 30 aprile 2020, n.28. Il testo dell'articolo è linkato sul sito pubblico di questo corso di diritto civile.

Il Garante per la protezione dei dati personali è intervenuto più volte durante la fase di avvio e di implementazione del sistema di tracciamento digitale.

Molto rilevante è il Provvedimento di autorizzazione 1° giugno 2020.

Il provvedimento introduce nel modo seguente il funzionamento del sistema di tracciamento digitale:

“Il Sistema di allerta Covid-19, che rappresenta il sistema nazionale di tracciamento digitale dei contatti (contact tracing), è finalizzato al contrasto della diffusione del Covid-19 ed è complementare alle modalità ordinarie di tracciamento dei contatti già in uso nell'ambito del Servizio sanitario nazionale (SSN). Tale Sistema, denominato Immuni, è composto da un'applicazione (di seguito “app” o “app Immuni”) per dispositivi mobili; dai sistemi e dalle componenti tecnologiche e organizzative che ne permettono il funzionamento (di seguito “backend”), nonché da un servizio di interazione con gli operatori sanitari che utilizza il Sistema Tessera Sanitaria (di seguito “Sistema TS”).

Il Ministero della salute è titolare del trattamento dei dati personali raccolti nell'ambito del predetto Sistema e si avvale di Sogei S.p.a. e del Ministero dell'economia e delle finanze, limitatamente all'utilizzo del Sistema TS, che operano in qualità di responsabili del trattamento (art. 28 del Regolamento).

L'applicazione, installata liberamente e volontariamente dagli interessati, consente di avvisare tempestivamente gli utenti di essere entrati in contatto stretto con un soggetto risultato positivo al Covid-19, fornendo raccomandazioni sul comportamento da assumere e invitandoli a consultare il proprio medico.

Accanto a tale meccanismo, è prevista la raccolta di ulteriori dati dai dispositivi degli utenti (c.d. analytics) per fini di sanità pubblica, contribuendo, nel contempo, a migliorare il funzionamento del Sistema di allerta Covid-19.

L'app Immuni si basa sull'utilizzo della tecnologia Bluetooth Low Energy (BLE) e sul Framework di Exposure Notification realizzato da Apple e Google (di seguito “Framework A/G”), reso disponibile su dispositivi mobili con sistema iOS e Android, che include interfacce di programmazione delle applicazioni (API - Application Programming Interface) e tecnologie a livello di sistema operativo per consentire il tracciamento dei contatti, senza ricorrere alla geolocalizzazione dei dispositivi degli utenti”.

Per i dettagli del funzionamento si rinvia alla lettura integrale del provvedimento del Garante. Qui occorre riportare le conclusioni, svolte in un momento in cui si avviava la sperimentazione del sistema, del provvedimento:

“a) ai sensi e per gli effetti degli artt. 36, § 5, e 58, § 3, lett. c), del Regolamento e dell'art. 2-quinquiesdecies del Codice, autorizza il Ministero della salute ad avviare il trattamento relativo al Sistema di allerta Covid-19 di cui all'art. 6 del d.l. 30 aprile 2020, n. 20, nel rispetto delle seguenti prescrizioni:

1) indicare puntualmente nella valutazione d'impatto, l'algoritmo, basato su criteri epidemiologici di rischio e modelli probabilistici, aggiornandolo costantemente, specificando i parametri di configurazione impiegati e le assunzioni effettuate, rendendolo disponibile alla comunità scientifica (§2);

2) informare adeguatamente gli utenti in ordine alla possibilità che l'app generi notifiche di esposizione che non sempre riflettono un'effettiva condizione di rischio, in ragione della possibilità di contatto con persone positive al Covid-19 a causa della propria attività lavorativa, in condizioni tuttavia caratterizzate da un adeguato grado di protezione (§2);

3) consentire agli utenti dell'app di disattivarla temporaneamente attraverso una funzione facilmente accessibile nella schermata principale, informando di tale facoltà attraverso le infografiche visualizzate all'atto dell'installazione dell'applicazione (§ 2);

4) individuare modalità adeguate a proteggere gli analytics nel backend di Immuni, evitandone ogni forma di riassociazione a soggetti identificabili, adottando altresì idonee misure di sicurezza e tecniche di anonimizzazione, da individuarsi in ragione delle specifiche finalità in concreto perseguite, nel rispetto dei principi di privacy by design e by default (§3);

5) precisare, nel modello di informativa, la descrizione delle operazioni effettuate con riferimento agli analytics di tipo Epidemiological Info e dei dati personali raccolti in relazione alle diverse categorie di interessati (§ 4.1);

6) dedicare particolare attenzione all'informativa e al messaggio di allerta tenendo conto del fatto che è previsto l'uso del Sistema anche da parte di minori ultra quattordicenni (§ 4.1);

7) fornire adeguate informazioni agli utenti in relazione alle caratteristiche della fase di sperimentazione (§ 4.1 e 8);

8) integrare la valutazione d'impatto e l'informativa in relazione alle modalità di esercizio del diritto di cancellazione e di opposizione (§ 4.2);

9) integrare, sulla base del principio di responsabilizzazione, la valutazione d'impatto con la descrizione del ruolo e delle operazioni ascrivibili ad altri soggetti lì citati o suscettibili, comunque, di coinvolgimento nel Sistema Immuni, evidenziando la sussistenza di eventuali rischi per gli interessati i cui dati siano trattati dal sistema (§ 6);

10) commisurare i tempi di conservazione degli indirizzi ip, per i fini e nei termini richiamati, nella misura strettamente necessaria al rilevamento di anomalie e di attacchi (§ 7.3);

11) introdurre misure volte ad assicurare il tracciamento delle operazioni compiute dagli amministratori di sistema sui sistemi operativi, sulla rete e sulle basi dati (§ 7.3);

12) adottare 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 (§ 7.3)".

Per concludere, anche quando il trattamento dei dati personali avviene nel rispetto delle prescrizioni normative e dell'interpretazione del Garante rimangono alcune questioni sul tavolo [cfr. Bincoletto 2020]:

- i) Non tutti dispongono dei mezzi e delle capacità per scaricare e utilizzare l'app di tracciamento (ci si domanda se ciò non faccia sorgere discriminazioni e disuguaglianze);
- ii) L'efficacia del sistema di prevenzione del rischio di contagio e contrasto all'epidemia dipende da quanto accade dopo aver ricevuto l'avviso di rischio contagio (e questo non ha a che fare con la tecnologia ma con la forza e l'efficienza del sistema sanitario nonché con l'andamento dell'epidemia: v. parte 2 della lezione).

## **Bibliografia**

G. Bincoletto, *App di contact tracing e tracking: privacy e controllo del contagio*, relazione nell'ambito del seminario «App di contact tracing e tracking: privacy e controllo del contagio, 8 giugno 2020», Università, Facoltà di Giurisprudenza, Biodiritto

G. Resta, *La protezione dei dati personali nel diritto dell'emergenza Covid-19*, in *Giustizia civile*, 5.5.2020



E-mail:

[roberto.caso@unitn.it](mailto:roberto.caso@unitn.it)

Web:

<http://www5.unitn.it/People/it/Web/Persona/PER0000633#INFO>

<http://lawtech.jus.unitn.it/>

<https://www.robertocaso.it/>

Copyright by Roberto Caso

Licenza Creative Commons

Quest'opera è distribuita con [Licenza Creative Commons Attribuzione - Condividi allo stesso modo 4.0 Internazionale](#)

La citazione di testi e la riproduzione di immagini costituisce esercizio dei diritti garantiti dagli art. 2, 21 e 33 Cost. e dall'art. 70 l. 1941/633