DIPARTIMENTO SPGI

# Le conseguenze della pandemia da Covid-19

## Una riflessione multi-disciplinare del Dipartimento di Scienze Politiche, Giuridiche e Studi internazionali

a cura di Elena Pariotti e Antonio Varsori

PADOVA UP

PADOVA UNIVERSITY PRESS

## Collana del Dipartimento di Scienze Politiche, Giuridiche e Studi Internazionali

La collana dei *Quaderni del Dipartimento di Scienze Politiche, Giuridiche e Studi Internazionali* intende rispondere a precisi criteri di qualità, serietà e scientificità, attraverso un processo di selezione e valutazione orientata ai parametri individuati dall'ANVUR nel quadro della Valutazione della Qualità della Ricerca, ed esprime nelle pubblicazioni in essa ospitate la prospettiva interdisciplinare che caratterizza composizione e attività di ricerca del Dipartimento

*Volume realizzato con il contributo del*
*Dipartimento di Scienze Politiche, Giuridiche e Studi Internazionali (SPGI)*

Prima edizione 2022, Padova University Press
Titolo originale: *Le conseguenze della pandemia da Covid-19.* Una riflessione multi-disciplinare del Dipartimento di Scienze Politiche, Giuridiche e Studi internazionali


Università degli Studi di Padova
via 8 Febbraio 2, Padova
www.padovauniversitypress.it

Redazione Padova University Press
Progetto grafico Padova University Press

ISBN 978-88-6938-312-0

# Le conseguenze della pandemia da Covid-19

## *Una riflessione multi-disciplinare del Dipartimento di Scienze Politiche, Giuridiche e Studi internazionali*

a cura di
Elena Pariotti e Antonio Varsori

PADOVA UP

## Indice

# App di contact tracing e principio di privacy by design[1]

*Daniele Ruggiu*

## 10.1 App di *contact tracing* come campo privilegiato del principio di privacy by design

L'attuale pandemia da Covid-19 ha portato ad una grande diffusione delle tecnologie digitali pressoché ovunque imponendo una rapida digitalizzazione dei servizi a tutti i livelli: ricerca, sanità, amministrazione, industria, trasporti, scuola, università, ambiente etc.

Ad esempio, in seguito allo scoppio della pandemia di Sars-Cov2 nel 2019 è emersa chiaramente l'esigenza di indirizzarsi verso la telemedicina in un periodo in cui i contatti tra medico e paziente costituiscono sempre più un rischio e vi è, tra l'altro, la necessità di decongestionare gli ospedali oltremodo sollecitati dai ricoveri collegati al Covid. Si è avuta poi una forte spinta verso la digitalizzazione della Sanità con l'implementazione del Fascicolo sanitario elettronico necessario per accedere ad alcune documentazioni essenziali come, *inter alia*, il Green pass. Sempre in ambito sanitario, il Covid ha portato poi alla realizzazione di vaccini di ultima generazione risultanti, guarda caso, dalla convergenza di sistemi di intelligenza artificiale, Big Data e tecnologia blockchain (Ruggiu 2021). Senza la pandemia, forse, sarebbero trascorsi ancora anni prima che fossero commercializzati, e fondamentali ricerche sui vaccini contro il can-

[1] Questo contributo è anche l'esito del ciclo di seminari tenuti nell'ambito del corso di Informatica giuridica di Diritto dell'economia a Rovigo a cui ha partecipato tra gli altri Simone Milani senza le cui delucidazioni sarebbe stato impossibile comprendere il funzionamento, l'impatto e l'efficacia delle app di tracciamento.

cro, strettamente legate ai vaccini mRNA, non sarebbero state così vicine dal realizzarsi.

In ambito sanitario, durante la pandemia si è avuta inoltre una spinta verso sistemi digitalizzati di monitoraggio dei contatti delle persone contagiate. Mentre in ambito scolastico e universitario si è andati sempre più verso una digitalizzazione di tutta l'attività didattica e accademica attraverso la diffusione di webinar e varie forme di didattica a distanza (asincronica, sincronica, blended, duale) a cui oggi ormai siamo tutti abituati.

Ma questo fenomeno di digitalizzazione capillare delle nostre vite ha fatto sentire i propri effetti anche sulla macchina burocratica del paese, dall'apparato amministrativo alla giustizia e, per forza di cose, anche sul settore privato che ha dovuto rafforzare i propri prodotti, sviluppare nuovi servizi digitali per stare al passo con le necessità del momento fornendo, ad esempio, app essenziali nella cosiddetta "sharing economy" (servizi di consegna a domicilio, app di *food delivery*, forme di mobilità condivisa etc.), automatizzando sempre di più i nostri mezzi di trasporto (veicoli elettrici, veicoli autonomi e semiautonomi etc.), le nostre case attraverso l'implementazione dell'Internet of things e dalla domotica, potenziando tutto il settore dei dispositivi elettronici.

Tanto nel privato quanto nella pubblica amministrazione si sono infine introdotte forme di lavoro a distanza come lo "smart working" e di riorganizzazione del lavoro che senza lo sviluppo delle nuove tecnologie digitali non sarebbero possibili.

Questa rivoluzione sotterranea, appena visibile al grande pubblico, non ha fatto altro che accrescere enormemente l'impatto su un settore come quello della privacy dei cittadini europei, che costituisce dal 2016 il fulcro di una regolazione unica al mondo.

Da questo punto di vista, di particolare interesse, soprattutto all'inizio della pandemia, è il caso delle app di contact tracing. La necessità di realizzare una rapida individuazione di possibili focolai e di intervenire altrettanto rapidamente isolando subito tutti i contatti di un soggetto risultato positivo per evitare che il contagio si propaghi ha portato a sviluppare applicazioni che hanno avuto una sensibile diffusione soprattutto all'inizio, quando i vaccini dovevano ancora arrivare (Santoro 2020). L'utilizzo delle app di tracciamento serve appunto ad ottimizzare la lotta al virus, ma con chiare implicazioni per quanto riguarda la privacy.

Quello delle applicazioni di tracciamento rappresenta, infatti, un campo privilegiato di applicazione del Regolamento 2016/679/UE (General Data Protection Regulation – in sigla GDPR), in particolare del principio di "privacy by design" che costituisce l'idea guida di tutta la normativa e che trova nelle forme

di tracciamento automatizzato un'applicazione esemplare. Con il principio di "privacy by design" l'implementazione delle misure atte a rafforzare la privacy di un individuo viene a modellare e a ridefinire profondamente un certo quadro tecnologico. Integrare la privacy "by design" comporta, in questo senso, l'abbandono di una logica meramente antagonista tra diritti e sviluppo tecnologico per approdare ad una logica che individua una modalità alternativa dello sviluppo della tecnologia, una modalità che faccia sostanzialmente dei diritti un fattore propulsivo dell'innovazione[2]. Da questo punto di vista, le applicazioni di *contact tracing* rappresentano un'eccellente esemplificazione del modello di innovazione che vige in Europa alla luce della nuova normativa in tema di privacy, un modello che fa appunto dei diritti un booster dell'innovazione e non semplicemente un limite.

## 10.2 Il tracciamento dei contatti: manuale o automatico

Due sono sostanzialmente i modi per controllare la diffusione di una epidemia mediante il tracciamento (Santoro 2020). O attraverso il tracciamento manuale grazie ad una mappatura il più possibile accurata fatta dagli operatori sanitari dei contatti stretti degli ultimi 14 giorni di un soggetto risultato positivo ad un test molecolare. O attraverso il tracciamento automatico grazie al download di un'apposita applicazione sul proprio smartphone. Anche in questo secondo caso vi è l'intervento di operatori sanitari ma questo è ridotto al minimo e in certi casi persino assente grazie alla tecnologia. La reale differenza sta nel fatto che, nel primo caso, la mappatura individuale porta ad individuare solo i contatti noti del soggetto, mentre nel secondo, si raggiungono tutti i contatti anonimi con cui il soggetto positivo sia entrato inavvertitamente in contatto nei luoghi pubblici, al supermercato, sul tram, sul bus, in un negozio etc. Purché ovviamente tutti abbiano provveduto a scaricare l'applicazione su un telefono sufficientemente recente. La diffusione degli smartphone non fa che agevolare l'efficacia di questi servizi. È però necessario che il download di queste app abbia interessato un numero adeguato di popolazione tale da garantire una copertura sufficientemente accurata di tutto il territorio. Cosa avvenuta solo parzialmente in Italia.

[2] Considerando 78 del GDPR recita: «La tutela dei diritti e delle libertà delle persone fisiche relativamente al trattamento dei dati personali richiede l'adozione di misure tecniche e organizzative adeguate per garantire il rispetto delle disposizioni del presente regolamento. Al fine di poter dimostrare la conformità con il presente regolamento, il titolare del trattamento dovrebbe adottare politiche interne e attuare misure che soddisfino in particolare i principi della protezione dei dati fin dalla progettazione e della protezione dei dati per impostazione predefinita».

## 10.3 Il caso Cambridge Analytica

L'utilizzo di queste applicazioni implica comunque dei rischi, non solo per la privacy, ma anche per altri diritti che possono dipendere dal controllo più o meno esteso delle informazioni delle persone, come appunto il caso Cambridge Analytica ci ricorda (Ma, Gilbert 2019).

Nel 2016 una società inglese, la Cambridge Analytica, attraverso un semplice questionario sulle attitudini caratteriali delle persone fatto circolare su Facebook, raccolse una serie di informazioni essenziali da cui fu possibile profilare, a partire da circa duecentomila persone, non solo queste, ma tutti i loro contatti sino ad arrivare coprire una platea di oltre 87 milioni di persone sparse in tutto il mondo. In questo modo poterono influenzare col concorso della società di Mark Zuckenberg, prima, il referendum sulla Brexit e, poi, le elezioni americane che portarono alla presidenza di Donald Trump.

Questo significa che la forma di controllo esercitata attraverso le attività di tracciamento, anche quelle per la gestione di un'epidemia, per intenderci, non necessariamente comporta una minaccia per le sole informazioni sanitarie interessate (il fatto o meno di essere positivi, che ci si possa esporre a forme di stigmatizzazione se positivi etc.). Poiché attraverso il capillare tracciamento dei nostri movimenti, la contestuale raccolta di altre informazioni trovate sul web e suoi social network, tutta la nostra vita può essere profilata e più o meno indirettamente condizionata. Esattamente come si è visto nel caso di Cambridge Analytica.

In altre parole, controllare le informazioni può rappresentare oggi una sensibile minaccia per la nostra libertà. A maggior ragione se si muove dalle informazioni relative alla salute delle persone. Per evitare questo è quindi necessario adottare delle contromisure intervenendo alla radice dei problemi già nella fase di progettazione in modo da minimizzare i rischi per la privacy ab origine o come si dice "by design".

## 10.4 Il principio di privacy by design nel GDPR

Il principio di "privacy by design", come noto, si ritrova al centro del GDPR. Oltre che nei considerando 78 e 108, il principio di "privacy by design" modella in particolare l'articolo 25 del Regolamento nella sezione 1 del capo IV dedicata agli obblighi del titolare e del responsabile del trattamento imponendo loro di considerare in anticipo i rischi alla luce della natura e delle finalità del trattamento e di adottare tutte le misure tecniche e organizzative idonee ad attuare i

principi di protezione dei dati quali la minimizzazione, la garanzia per la protezione dati, dei diritti dell'interessato già nella fase della progettazione[3].

## 10.5 Dall'approccio *design thinking* al principio di privacy by design

Il principio di "privacy by design" può essere fatto risalire a quando a partire dagli anni '80, '90 si è iniziato ad adottare nell'ambito della *business ethics* una prospettiva ispirata d*esign thinking* secondo la quale i problemi complessi, cosiddetti *wicked problems*, richiedono che le loro soluzioni debbano essere affrontate contestualmente nello sviluppo di una certa piattaforma e non quando questa è già ultimata (Hustinx 2010). Questo a maggior ragione per quelle tecnologie note anche come *privacy-enhancing technologies* (PET), quali sono le applicazioni di *contact tracing* (van Rossum et al. 1995).

## 10.6 Contenuto del principio di privacy by design: "protezione dati by default" e "by design"

Il principio di privacy by design implica, da una parte, di non raccogliere dati in misura sovrabbondante agli scopi dichiarati con sistemi di rete a strascico (cd. "protezione dati by default"), dall'altra di impiegare sin dalla progettazione di un certo sistema di trattamento tutte le misure tecniche e organizzative necessarie alla protezione dei dati personali in modo che i rischi di sicurezza dei dati personali affinché siano anticipati, ovvero affrontati subito contestualmente allo sviluppo di una certa tecnologia ("protezione dati by design") (d'Acquisto, Naldi 2018).

---

[3] "1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.

[2]. «Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica».

## 10.7 Le app di *contact tracing*

Appare subito evidente come quello delle applicazioni di *contact tracing* rappresenti un banco di prova esemplare per il principio della "privacy by design", la cartina di tornasole per un'innovazione che sia davvero innovativa ma allo stesso tempo venga a ruotare attorno ai diritti delle persone.

Diversi sono infatti i modi con cui queste possono essere realizzate e di conseguenza l'impatto sulla privacy può risultare più o meno importante (Ciaffi 2020). Tutto dipende da quali soluzioni si decide di implementare.

Ci sono soluzioni tecnologiche basate appunto su sistemi di geolocalizzazione, applicazioni che invece utilizzano interfacce bluetooth e vi sono, infine, applicazioni volontarie basate su meccanismi di *data sharing* sul web e sui social network.

A livello mondiale sono state sviluppate diverse app che utilizzano sistemi spesso molto diversi tra loro. La *HaMagen* in Israele, *StoppCorona* in Austria, *Swiss Contact Tracing app* in Svizzera, *Corona App* in Germania, *StopCovid* in Francia, *Chinese Health Code system* in Cina (obbligatoria), *NHS Covid-19 app* in Gran Bretagna e *Immuni* in Italia.

Tutte queste app devono, in genere, essere in grado di: i) ricostruire la rete delle relazioni di un individuo positivo; ii) far sì, poi, che il processo di tracciamento sia automatico; iii) garantire, infine, la non identificabilità delle persone per evitare forme di stigmatizzazione, la diffusione di dati sensibili, la raccolta e la profilazione degli individui al di là del fine del mero contenimento di un'epidemia.

Da quest'ultimo punto di vista il MIT ha pubblicato nel 2020 un lavoro con cui valuta le diverse app sulla base di cinque criteri fondamentali: il fatto che un'app sia o meno volontaria; quanto questa possa essere invasiva; il fatto che alla fine dell'utilizzo i dati vengano o meno distrutti; il fatto che vi sia una minimizzazione dei dati tralasciando quelli non necessari; il fatto che vi sia una certa trasparenza garantita attraverso la condivisione del codice[4]. Appare chiaro, dunque, che il modo in cui un'applicazione viene sviluppata e poi implementata non sia affatto indifferente. In altri termini, non esiste una tecnologia neutrale, soprattutto dal punto di vista dei diritti.

## 10.8 App basate sulla geolocalizzazione

Ad esempio, le applicazioni basate sulla geolocalizzazione sono app che manifestano tutta una serie di criticità per quanto riguarda la privacy proprio per-

[4] https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker/.

ché hanno come priorità quella di assicurare un tracciamento efficace. Queste sono utilizzate in Cina (*Chinese Halth System*), ad esempio, in Iran (*Mask.ir*), in Bulgaria (*VirusSafe*), in Islanda (*Rakning-19*).

Queste app si basano essenzialmente su meccanismi di geolocalizzazione e sulla rete cellulare per misurare, grazie all'antenna gps che comunica con il satellite, la posizione dell'individuo sulla terra e la sua vicinanza da altre persone. Ogni cellulare misura costantemente l'intensità del segnale rispetto ad una pluralità di satelliti nel mondo in modo che possa essere associato attraverso un meccanismo di triangolazione a delle precise coordinate spazio-temporali (latitudine, longitudine e un orario). Grazie alle antenne dei ripetitori di telefonia cellulare distribuite sul nostro territorio, poi, questo meccanismo di tracciamento può funzionare anche se la funzione gps è spenta misurando comunque il percorso seguito dagli individui ed evidenziando tutti i contatti con i dispositivi delle persone che possano essere risultate positive al tampone molecolare. Quando questo avviene l'app manda un messaggio e chi è entrato in contatto con queste sa se deve farsi un tampone.

## 10.9 Criticità della geolocalizzazione

Questo tipo di soluzione presenta però diverse criticità. Di tipo tecnico innanzitutto, in quanto è un sistema poco accurato che non funziona in ambienti chiusi mentre all'aperto ha un margine di errore di circa 5 metri. Può poi essere facilmente ingannato con dei segnali falsi (cd. *gps spoofing*). Ma ha anche gravi criticità relative proprio alla privacy. Innanzitutto, poiché in ogni istante si sa dove si trova una persona, e si basa solo su meccanismi di pseudonimicità per cui non è possibile garantire che gli individui non vengano reidentificati come l'anonimità (almeno in teoria) garantisce. Non a caso, quando ci spostiamo utilizzando l'applicazione maps, spesso ci viene richiesto di valutare un certo posto, un negozio, un ristorante, un monumento, una piazza, anche se non ci siamo mai stati. Quindi è problematica perché raccoglie indiscriminatamente tutta una serie di informazioni personali. Ad esempio, dal fatto che si sosta dalle 10 di sera alle 8 della mattina in un certo posto, il gps è in grado di evincere dove la nostra abitazione, altri spostamenti rivelano il luogo di lavoro, la nostra fede e le abitudini religiose etc. Infine, un'ultima criticità deriva dal fatto che i sistemi di geolocalizzazione potendo appoggiarsi anche alla rete cellulare vengono per forza di cose a condividere informazioni private con gli operatori telefonici, che, in quanto privati, potrebbero non essere i migliori soggetti nel garantire la privacy degli individui. Specie se in gioco vi sono le informazioni sanitare a cui

il mercato è oggi fortemente interessato. Per queste ragioni garantire la minimizzazione dei dati risulta davvero arduo con la geolocalizzazione.

## 10.10 Applicazioni basate su tecnologia Blootooth

Le app basate su sistemi bluetooth, non cercano invece di privilegiare il tracciamento a scapito della privacy, ma di sviluppare la tecnologia garantendo nello stesso momento la privacy delle persone. Queste applicazioni si basano su protocolli come DP3-T o Blue Trace che, a differenza del gps, funzionano a corto raggio mettendo in comunicazione più dispositivi tra loro. Il bluetooth non serve a individuare un dispositivo grazie ai satelliti o alla rete cellulare che si trova nelle vicinanze del posto in cui ci troviamo, ma a mettere in comunicazione diversi dispositivi (come telefoni, stampanti, auricolari, smartwatch, healthtracker etc.) geograficamente vicini a partire dalla cd. Internet delle cose (*Internet of Things* o IoT) con cui gli oggetti della nostra vita si trovano tutti interconnessi e in grado di dialogare tra di loro. Le moderne versioni di bluetooth, quelle 4.0 e oltre, vengono a basarsi su soluzioni LTE, *low energy*, meno energiovore, e su un sistema migliore di criptazione dei dati. Il dispositivo bluetooth non è altro che un'antenna che emette un segnale che rimane locale, limitato geograficamente alle vicinanze, in cui viene indicato solo l'identificativo del dispositivo, il tipo di dispositivo, quali servizi sono attivati e una serie di informazioni tecniche. Nient'altro. La bluetooth ID non è altro che la carta di identità del dispositivo e fornisce una serie di indicazioni essenziali, relative alla nostra persona, non così ampie come il gps. Il bluetooth inoltre non solo fornisce un'indicazione sull'identità del dispositivo, ma anche sull'intensità del segnale, facendo così capire quanto vicini siano stati i dispositivi e quindi permettendo una valutazione del livello di rischio a cui il soggetto è stato esposto. Chiaramente l'identità del dispositivo risulta palese solo nel momento in cui due dispositivi entrano in contatto tra loro, mentre in tutti gli altri momenti non è possibile arrivare ad alcuna identificazione. Per evitare l'identificazione del soggetto nel momento in cui entra in contatto con un'altra persona esistono poi più soluzioni tecniche, da cui viene a dipendere l'implementazione del principio di "privacy by design". Si possono avere, infatti, o sistemi centralizzati in cui tutti i dati vengono memorizzati su un server centrale oppure sistemi decentrati dove il server non conosce l'identità degli utenti che si sono scaricati l'applicazione.

## 10.11 Sistemi centralizzati

Nei sistemi centralizzati (basati sul protocollo Pan-European Privacy-Preserving Proximity Tracing, o PEPP-PT) il server centrale viene a conoscere

l'identità di tutti coloro che si sono scaricati l'applicazione. Qui l'elemento di debolezza sta nel fatto che avvengono due comunicazioni, una tra i due cellulari che sono entrati in contatto tra loro (cd. comunicazione "client to client") e una con il server centrale (cd. comunicazione client to server). Quando ci si scarica l'applicazione ogni cellulare viene associato ad una ID permanente quindi il server centrale, che conosce tutto di tutti, invia una serie di identità fittizie (dette "ephemeral ID") che non servono altro che a nascondere l'identità del proprietario del dispositivo ogni qualvolta entra in contatto con gli altri utenti che si sono scaricati l'applicazione. Attraverso questo meccanismo di pseudonimizzazione il server centrale può però sempre ricollegare ogni identità fittizia a chi si è scaricato l'app. Se un utente che si è scaricato l'applicazione è positivo, il server allora invia un segnale a tutti coloro che quel giorno si sono imbattuti in quella persona, allertandoli. Questo significa però che, da una parte, il server centrale può sempre reidentificare ogni utente e che, dall'altra, se i dati sono conservati in un solo punto (il server centrale, appunto) questi dati sono vulnerabili perché potrebbero essere hackerati, soggetti ad abusi venendo trattati, ad esempio, per scopi diversi da quelli per i quali sono stati raccolti etc. Come appunto nel caso Cambridge Analytica.

Nella versione dei sistemi centralizzati basati su tecnologia Blue Trace, usata per esempio a Singapore e in Australia, o in Israele, vi è poi la possibilità che il dispositivo oltre ad inviare l'informazione della propria ID, invii contestualmente informazioni riguardanti il proprio sistema sanitario così che il server centrale, possa inviare l'informazione della positività anche a sistemi sanitari di altri paesi, in cui l'individuo venga a trovarsi, per lavoro, vacanza etc. senza però rivelare l'identità del soggetto che appunto è conosciuta solo dal server. Questo però, come si può immaginare, amplia a dismisura le vulnerabilità dell'intero sistema.

Nei sistemi centralizzati i problemi per la privacy derivano quindi dal fatto che la sicurezza viene garantita dal server centrale, dal fatto che si basa sempre su un meccanismo solo pseudoanonimo, dal fatto che analizzando il traffico dati della comunicazione del cellulare col server centrale è sempre possibile sapere se qualcuno è risultato positivo (perché è possibile identificare i picchi di traffico col server in un certo momento cd. "traffic profiling"), infine è sempre possibile inserire dei dati falsi (notifiche di esposizione o di positività false, falsi allarmi) per portare così il sistema al collasso ("data pollution"). Per questo di solito si inserisce una procedura di autentificazione con l'autorità sanitaria prima di poter inviare comunicazioni di positività o di esposizione (questo meccanismo, ad esempio è presente in Immuni). È chiaro però che se non viene abilitata la procedura per autorizzare, come è capitato con la Regione Veneto appunto, le comunicazioni di esposizione o di positività, l'app non può funzionare (Longo 2020).

## 10.12 Sistemi decentralizzati

Nei sistemi decentralizzati (con protocollo DP3T o *Decentralized Privacy-Preserving Prozimity Tracing*), come nel caso della app *Immuni*, della Svizzera (SwissContact Tracing App), della Finlandia (Ketju), dell'Estonia (Estonia's App), si segue un approccio "privacy by design", rispondente al nostro GDPR, che garantisce però allo stesso tempo la trasparenza. In questo caso si riesce comunque a far sapere a chi è entrato a contatto con un positivo che è a rischio, e quindi deve fare il tampone, ma si difende allo stesso tempo la privacy, perché non è possibile rivelare l'identità di chi era positivo, perché questa informazione il server centrale non ce l'ha. Anche qui la comunicazione avviene tra client e client e tra client e server. Però, in questo caso non è più il server centrale ma lo stesso dispositivo a generare in maniera ciclica ogni 15 minuti le identità fittizie (*ephemeral ID*), attraverso una chiave che muta anch'essa periodicamente. Le identità quindi, essendo generate dallo stesso dispositivo, non sono note al server centrale. I dati in altri termini sono anonimizzati non pseudoninimizzati, e, quindi, non sapendo nulla il server, le identità non sono esposte ad abusi, né a rischi di hackeraggio come nei sistemi centralizzati. I singoli dispositivi però registrano sia tutte le identità fittizie che generano sia tutte le identità fittizie con cui entrano in contatto. Una volta che si scopre di essere positivi, attraverso una procedura di autentificazione con la Asl è possibile comunicare al server che le identità fittizie generate a partire da quel momento provenivano da un dispositivo di una persona positiva e il server centrale procede ad allertare tutti i dispositivi che dopo la scoperta della positività sono entrati in contatto con il nostro dispositivo. In questo caso la procedura di autentificazione può essere attivata o a livello locale da parte delle singole Asl, o (visto che spesso nel caso della app Immuni tanto le Asl quanto le Regioni possono essere più o meno collaborative di fatto boicottando l'applicazione) a livello nazionale con un call centre unico (Longo 2020) o infine anche da parte degli stessi utenti saltando direttamente il passaggio intermedio dell'autorizzazione (Longo 2021). In questi casi nessuno può sapere la corrispondenza tra l'identità dell'utente e le identità fittizie generate dal dispositivo. Una volta negativizzati al tampone, il dispositivo genererà un'altra chiave e delle altre identità fittizie garantendo anche in questo caso la nostra privacy.

Nei sistemi decentralizzati quindi i momenti di vulnerabilità della nostra privacy sono ridotti al minimo, essendo state adottate delle soluzioni tecniche a tutela della privacy sin dalla fase di progettazione, "by design".

Ci sono comunque delle vulnerabilità però. Innanzitutto è un meccanismo oneroso poiché la maggior parte dell'elaborazione dati avviene sullo stesso dispositivo. Anche in questo caso si può analizzare l'intensità del traffico dati

(*traffic profiling*) aprendo alla reidentificazione del soggetto con rischi di inevitabili di stigmatizzazione. L'anonimato può essere poi violato nel caso si installi per errore un malware che comunichi ad un server parallelo sia le identità fittizie generate dall'app sia l'identità del dispositivo. Infine, essendo basata sulla prossimità è possibile risalire all'identità dell'individuo. Per questo, per ovviare in parte a questi rischi, l'app Immuni genera delle notifiche finte (che in realtà non comunicano nulla al server) in modo da depistare eventuali tentativi di *traffic profiling*.

Non esiste dunque un sistema bluetooth invulnerabile. Ma vi sono protocolli più o meno buoni e quello DP-3T, realizzato "by design" per proteggere la privacy sin dalla progettazione dell'applicazione, è sicuramente eccellente.

## 10.13 App basate su piattaforme web e social

Vi sono infine applicazioni basate su piattaforme web o sui social networks sviluppate dalle grandi compagnie del digitale (come Google, Amazon, Apple) dove le informazioni di contatto tra gli utenti vengono integrate da altre informazioni generate dalla community (ad esempio la community di Facebook). Google e Apple stanno poi sviluppando una loro app per il tracciamento volontario (Exposure Notification Framework) che appunto viene ad integrare le informazioni generate dal dispositivo con quelle trovate in internet (ad esempio l'esplosione di un focolaio in una certa zona). La stessa app Immuni integra le informazioni sui contatti con altre informazioni ricavate sul web. Nulla vieta in questi casi, però, che essendo sviluppate da una multinazionale, e non da un soggetto terzo, e essendo i dati conservati oltreoceano al di fuori dall'Europa, sulla base di un quadro regolatorio nettamente diverso, questi grandi player mondiali utilizzino le informazioni raccolte per altri scopi.

## 10.14 Immuni

L'applicazione Immuni sviluppata dalla milanese *Bending Spoons,* è un'app gratuita, su base volontaria che in linea con le indicazioni della Commissione europea utilizza non la tecnologia di geolocalizzazione ma la tecnologia *blouetooth low energy* e segue un protocollo decentralizzato che viene ad integrare anche dati provenienti da Google e Apple.

Il codice è stato reso disponibile su github.com, integrando così i requisiti di trasparenza richiesti dal nostro Garante della privacy.

Ad oggi è stata scaricata da 16.618.053 utenti ha portato a oltre 112.001 notifiche per 25.919 casi di positività[5]. Un risultato discreto. Ma non eccezionale. E presto superato dalla maggiore diffusione dei vaccini sul territorio italiano che ne hanno reso l'uso, sempre meno necessario.

L'app Immuni viene a gestire due tipi di dati. Dati epidemiologici: (la data in cui si è venuto a contatto con una persona positiva, durata dell'esposizione (dai 5 ai 30 minuti), distanza espressa dall'attenuazione del segnale, viralità degli individui positivi. Si tratta di informazioni molto più affidabili di quelle del gps (che ha un margine di errore molto più ampio, come si è visto. Vi sono poi dati di tipo operativo come dati sulle notifiche, dati sull'ultima esposizione al rischio, dati sul tracciamento, dati sul bluetooth, dati di sistema che vengono integrati attraverso il meccanismo di tracciamento. Come detto, per proteggere il segnale vengono poi inviate delle comunicazioni finte (cd. *dummy uploads*) per evitare che sia possibile attuare forme di reidentificazione attraverso l'analisi del traffico dati (Traffic profiling). Tutti i dati vengono poi immagazzinati su server italiani (non americani o stranieri), soggetti quindi alla legislazione italiana e europea (GDPR). Il data controller è pubblico, il Ministero della salute, non privato (il che comporterebbe ulteriori rischi). La deadline per la cancellazione dei dati poi era stata fissata al 31 dicembre 2021. Vi è quindi la garanzia che l'applicazione non utilizzi di default il gps. Android, il sistema operativo, però può richiedere per la notifica ad esposizione l'attivazione del gps. In questo caso, comunque è possibile, abbassando la precisione del segnale, disattivare il gps e utilizzare Immuni soltanto con il bluetooth. Infine, grazie alla trasparenza garantita da Immuni attraverso la condivisione continua del codice, è possibile individuare bug o falle di sistema in maniera tempestiva e correggerle. Cosa avvenuta, ad esempio a settembre 2020, grazie alla segnalazione degli utenti.

Tutte queste misure servono quindi a minimizzare i rischi per la privacy e ad implementare il livello di protezione secondo un approccio chiaramente "by design" in linea tanto col GDPR quanto con quanto richiesto dal Garante della privacy col provvedimento di autorizzazione del 1° giugno 2020[6].

## 10.15 Una sovrabbondanza di applicazioni in Italia

L'app Immuni non ha avuto vita facile, però. Basti pensare che mentre veniva lanciata contemporaneamente in Italia tutte le Regioni hanno lanciato una miriade di applicazioni concorrenti, con caratteristiche a volte simili, spesso diverse ma comunque in grado di ingenerare una certa confusione. Nell'aprile

[5] Immuni – I numeri di Immuni (italia.it)

[6] Provvedimento di autorizzazione al trattamento dei dati personali… – Garante Privacy

2020 l'Alta Scuola di Economia e Management dei Servizi Socio-Sanitari dell'Università Cattolica (Milano) aveva calcolato che a quella data esistevano ben quasi 90 app in 17 Regioni[7] per il monitoraggio a distanza di chi ha contratto il virus o ha altre patologie e aveva bisogno di controlli.

Questa proliferazione di app in Italia ha rischiato di abbassare sensibilmente il livello di efficacia dell'app Immuni, perché queste app possono interferire tra loro e perché chi si è scaricato un'altra applicazione che ha una funzione diversa potrebbe pensare di essere coperto, mentre non lo è.

### 10.16 Autorizzazione del 1° giugno 2020 del Garante della privacy

Sulla base della valutazione d'impatto trasmessa dal Ministero, il trattamento di dati personali effettuato nell'ambito del sistema può essere considerato proporzionato, essendo state previste misure volte a garantire in misura sufficiente il rispetto dei diritti e le libertà degli interessati, che attenuano i rischi che potrebbero derivare da trattamento. E il 1° giugno 2020 l'app Immuni è stata autorizzata dopo un periodo di rodaggio in quattro regioni nel mese di maggio (Liguria, Marche, Abruzzo e Puglia).

### 10.17 Le condizioni poste dal Garante della privacy

Per la sua autorizzazione il Garante della privacy ha posto una serie di condizioni per poter rilasciare l'autorizzazione. Cioè che gli individui ricevano delle informazioni complete e chiare (art. 13). Che i dati raccolti siano adeguati, pertinenti e limitati allo stretto necessario per le finalità dell'App (art. 5,1 let. c). Che i dati siano trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti (art. 5, 1 let. f). Che il governo sia in grado di dimostrare tali requisiti (art. 5,2). Che l'applicazione esista solo per il tempo necessario al proprio scopo (art. 5,1 let. e).

---

[7] La Regione Calabria ha lanciato a marzo 2020 *RCovid 19* per stimare il livello di diffusione del contagio e creare un collegamento diretto tra istituzioni e cittadini.
La Sicilia ha la sua App (*SiCura*) dal primo luglio 2020 che permette ai cittadini di essere immediatamente in contatto col sistema sanitario regionale.
In Campania è operativa *e-Covid*.
Nel Lazio c'è *Lazio Doctor* per l'autodiagnosi e per essere contattati da un medico.
In Veneto si pensava a lanciare una App obbligatoria per tracciare i contatti, progetto annunciato diverse volte e poi abbandonato.

## 10.18 Le richieste del Garante

In questo senso, il Garante della privacy ha quindi richiesto: che gli utenti siano informati adeguatamente in ordine al funzionamento dell'algoritmo di calcolo utilizzato per la valutazione del rischio di esposizione al contagio; che siano portati a conoscenza del fatto che il sistema potrebbe generare notifiche di esposizione che non sempre riflettono un'effettiva condizione di rischio (falsi positivi); che sia loro garantita la possibilità di disattivare temporaneamente l'App attraverso una funzione facilmente accessibile nella schermata principale.

Tutte queste richieste hanno contribuito, anche grazie ad un'attenzione mediatica senza precedenti favorita da un intenso dibattito politico, di implementare "by design" l'applicazione riducendo al minimo i rischi per la privacy degli utenti, e di adottare soluzioni con il minor impatto possibile sulla protezione dei loro dati e anticipando le possibili minacce in modo da correggere le vulnerabilità di sistema prima che si potessero palesare.

## 10.19 Un bilancio in chiaroscuro

La diffusione dell'app Immuni può presentare oggi un bilancio in chiaroscuro. Nata in un momento di forte tensione politica che si è presto focalizzato sulla lotta di contrasto al virus, sugli strumenti messi in campo dal governo e sugli obiettivi da raggiungere, l'app ha avuto un discreto successo. Essere scaricata da oltre 16 milioni di persone non è poco. In genere, si ritiene che per essere efficaci queste applicazioni dovrebbero coprire il 60% della popolazione. In questo senso, immuni avrebbe mancato il bersaglio. Uno studio Oxford-Google del 2020 stimava che con un'adozione del 15% sulla popolazione c'è un calo fino al 15% dei contagi e fino all'11.8% dei decessi. Se l'adozione sale al 75% della popolazione la riduzione è rispettivamente dell'81% e del 75% (Abueg, *et al.* 2020). In questo senso, la valutazione di Immuni cambia. Certo è che anche grazie alla confusa distribuzione delle competenze in materia sanitaria al livello costituzionale (la sanità è, come noto, ex art. 117 Cost. una materia di competenza concorrente tra Stato e Regioni), alla proliferazione di una miriade di app concorrenti a livello regionale, alla scarsa collaborazione di numerose Regioni (evidente nel caso, ad esempio, della mancata attivazione delle procedure di autorizzazione nel caso di positività che ha costretto il Governo ad attivare prima un sistema nazionale e poi a rendere possibile avviare in autonomia il tracciamento dei contatti stretti), Immuni ha avuto vita tutt'altro che facile. In questo senso il fatto che diversi milioni di italiani l'abbiano scaricata nonostante tutto non è affatto un cattivo risultato.

## 10.20 Conclusioni

Le app di *contact tracing* hanno rappresentato un campo privilegiato di applicazione del principio di "privacy by design". In Europa l'esistenza di una regolazione che imponeva il contestuale sviluppo di applicazioni che rispettassero l'esigente normativa in fatto di privacy, ha di fatto imposto una serie di soluzioni che fossero in grado di garantire sin dalla loro fase di progettazione un alto livello di protezione della privacy. Il fatto che l'ampia diffusione dei vaccini sul nostro continente e in Italia abbia reso superfluo il loro uso è di per sé irrilevante dal momento che queste piattaforme (le modalità con cui sono state sviluppate e l'esperienza che ne abbiamo tratto) potranno rendersi utili in futuro nel caso ce ne fosse bisogno.

È evidente che la tecnologia di per sé non è affatto neutra, esattamente come non è neutra la regolazione sulla tecnologia. Le possibilità di sviluppare ogni tecnologia in molteplici direzioni con soluzioni tecniche che diversamente possono impattare sui diritti in gioco mostrano che pressoché è sempre possibile un modo in cui una certa tecnologia può essere realizzata in modo da realizzare contestualmente il quadro di diritti che il sistema intende preservare. Non esiste alcuna alternatività, alcun aut aut, tra innovazione e diritti. Ma diverse forme di innovazione più o meno in sintonia con i diritti implementati in una certa regione (Ruggiu 2018).

La lezione che si trae appunto dal Regolamento Generale Protezione Dati Personali, tutto imperniato sul principio di "privacy by design", cioè con una chiara opzione *rights-based* (Ruggiu 2016), così come emerge dal quadro delle app di *contact tracing*, è che in Europa vige un ecosistema dell'innovazione in cui i diritti sono posti al centro dell'innovazione e non ne rappresentano un limite o un ostacolo da aggirare o superare in qualche modo. È sempre possibile una modalità che concilia perfettamente sviluppo e diritti, la crescita con il quadro assiologico e giuridico che ci siamo dati. Fatto questo che rappresenta un unicum al mondo.

## Riferimenti bibliografici

Abueg M., *et al.*, (2020), *Modeling the combined effect of digital exposure notification and non-pharmaceutical interventions on the COVID-19 epidemic in Washington state*, «medRxv», https://www.medrxiv.org/content/10.1101/2020.08.29.20184135v1.full.pdf

Ciaffi D. Y., (21.05.2020), *Covid-19 e app di tracing nel mondo: tecnologie e impatti privacy nella lotta al coronavirus*, «Cyber cecurity», 360, https://

www.cybersecurity360.it/legal/privacy-dati-personali/covid-19-e-app-di-contact-tracing-nel-mondo-tecnologie-e-impatti-privacy-nella-lotta-al-coronavirus/

D'Acquisto G, Naldi M., (2018), *Big Data e privacy by design. Anonimizzazione, pseudonimizzazione, sicurezza*, Torino, Giappichelli.

Hustinx P., (2010), *Privacy by design: delivering the promises*, «Identity in the Information Society» 3(2), pp. 253–255.

Longo A., (18.10.2020), *Coronavirus, per la app Immuni nasce il call center unico nazionale*, «Repubblica», Immuni, per la app nasce il call center unico nazionale – la Repubblica

Longo A., (09.04.2021), *Nuova vita per l'app Immuni, ecco l'aggiornamento per il tracking Covid fai da te*, «ItalianTech», Nuova vita per l'app Immuni, ecco l'aggiornamento per il tracking Covid fai da te – Italian Tech

Ma A., Gilbert B., (23.08.2019), *Facebook understood how dangerous the Trump-linked data firm Cambridge Analytica could be much earlier than it previously said. Herès everything that's happened up until now*, «Business Insider», https://www.businessinsider.com/cambridge-analytica-a-guide-to-the-trump-linked-data-firm-that-harvested-50-million-facebook-profiles-2018-3?r=US&IR=T

Ruggiu D., (2016), *Modelli di governance tecnologica e diritti fondamentali in Europa. Per un "rights-based model of governance*, «Rivista di Filosofia del Diritto», 5(2), pp. 341-362.

Id., (2018), *Human Rights and Emerging Technologies. Analysis and Perspectives in Europe*, con prefazione di R. Brownsword, Singapore, Panstanford Publisghing.

Id., (2021), *Vaccini anti Covid con blockchain: pro e contro*, «Agenda digitale.eu», https://www.agendadigitale.eu/sanita/vaccini-anti-covid-la-rivoluzione-blockchain-tra-processi-piu-rapidi-e-sfide-privacy/

Santoro E., (2020), *Covid-19: il tracciamento dei contatti e il supporto delle nuove tecnologie*, «R&P», 36, p. 78.

van Rossum H. *et al.*, (1995), *Privacy-enhancing Technologies: the path to anonymity*, The Hague, Registratiekamer.