Come può la tecnologia influenzare la Privacy dei Dati Personali e le libertà individuali?

Abstract
Tra i temi che più hanno alimentato il dibattito pubblico negli ultimi mesi di pandemia, il controllo dei movimenti e la raccolta di dati privati relativi alle nostre attività quotidiane sono tra i i più controversi e poco chiari a molti di noi. Se diverse sono state le considerazioni fatte per valutare gli impatti causati dai quadri giuridici nazionali nell'affrontare la fase iniziale della pandemia SarS-CoV2 [1], molto resta ancora da esplorare sulle misure tecnologiche adottate in grado di raccogliere i dati personali a salvaguardia della salute pubblica e a scapito della riservatezza dei dati e della libertà personale. In questo articolo passeremo in rassegna le principali tecnologie localizzazione e tracciamento adottate per limitare la diffusione di SarS-CoV2 nel mondo, tenteremo di definire un indice di sensibilità alla riservatezza dei dati classificando alcune delle applicazioni mobili in uso in tre paesi (USA, Italia e Cina) e analizzeremo, attraverso il parere di un esperto del settore, il caso italiano del sistema Immuni nel quadro giuridico europeo del GDPR.

Introduzione
Tra le tecnologie sanitarie digitali implementate in questi mesi per contrastare la pandemia da COVID-19, quelle utilizzate per la localizzazione e il tracciamento dei contatti hanno suscitato diversi interrogativi soprattutto per questioni di privacy. Infatti, se da un lato queste tecnologie mirano a identificare e bloccare rapidamente persone potenzialmente infette, perché sono state a stretto contatto con casi positivi accertati e poter quindi limitare la diffusione del virus, tuttavia sono state rilevate differenze rispetto alla loro sensibilità in tema di riservatezza dei dati.
Fondamentalmente, ci sono 3 approcci tecnologici su cui si basa la maggior parte delle app mobili di localizzazione e tracciamento e questi si basano su:

- Capacità degli operatori di rete di localizzare i dispositivi di comunicazione su reti cellulari (capacità implicita nella tecnologia della radio mobile) anche senza la piena consapevolezza degli utenti, potendo così formulare ipotesi su eventuali situazioni di prossimità tra terminali mobili;

- Capacità dei dispositivi smartphone di determinare autonomamente la propria posizione (ricevitori dei segnali emessi da sistemi di localizzazione globale come il GPS) e di comunicarla ad un centro servizi in grado di raccogliere dati di posizionamento ed elaborarli al fine di individuare eventuali situazioni di prossimità tra i dispositivi;

- Tracciamento di prossimità tramite smartphone in grado di rilevare autonomamente la presenza di altri dispositivi nelle vicinanze ricevendo segnali di identificazione (radiofari) diffusi con tecnologia Bluetooth Low Energy (BLE).

Seguendo le linee guida emanate dalla Commissione Europea [2] e dall'OMS [3], abbiamo dapprima identificato cinque principi comuni per la creazione di un'applicazione solida dal punto di vista della sicurezza sulla privacy. In un secondo momento, l'ottemperanza a tali principi è stata utilizzata per classificare la sensibilità alla riservatezza dei dati di tre applicazioni create in diversi paesi (USA, Italia e Cina) secondo quanto segue:

Principi	Descrizione
Volontarietà	Il download e l'utilizzo dell'applicazione avviene unicamente su base volontaria
Uso dei dati	I dati raccolti sono utilizzati per uno scopo predefinito e strettamente legato alla salvaguardia della salute pubblica. La vendita o riutilizzo di tali dati deve essere severamente vietata.
Conservazione dei dati	Il tempo di conservazione dei dati deve essere limitato al solo periodo dell'emergenza pandemica ad eccezione dell'utilizzo per fini statistici o epidemiologici. Le tempistiche di conservazione dei dati devono essere basate su rilevanze mediche. I dati di prossimità devono essere conservati sul dispositivo, cancellati entro un mese o immediatamente in caso di test negativo e caricati sul server solo su base volontaria.

Minimizzazione dei dati	Il trattamento dei dati deve essere limitato nello scopo e relativo ai soli dati necessari al perseguimento degli obbiettivi di salute pubblica. I dati devono essere trattati comunque in forma anonima e aggregata.
Trasparenza del trattamento	Il collezionamento dei dati e i fini del trattamento cui essi son sottoposti devono essere chiari, di semplice lettura e non ambigui. Deve essere chiaro il funzionamento dell'applicativo anche nel caso in cui questo utilizzi modelli decisionali automatizzati e del margine di errore ad esso associato.

Tabella 1: Principi guida per la creazione di applicazioni mobili per il tracciamento dei contatti durante la pandemia da COVID-19

Un punto è stato assegnato per ciascuno dei principi soddisfatti dalle applicazioni prese in esame e la sommatoria di questi usata per definirne la classificazione riportata nella tabelle sottostanti:

DPS (Data Privacy Sensibility)	Conditions
HIGH	≥ 4 points – l'applicazione soddisfa pienamente tutti o molti dei cinque principi
MEDIUM	2-3 points – l'applicazione soddisfa parzialmente alcuni dei cinque principi
LOW	≤ 1 points - l'applicazione supporta in minima parte o per nulla i cinque principi

Tabella 2: Indice di Sensibilità alla Data Privacy

Country	App Name	Technology	Data Privacy Sensibility	Notes
Italy	Immuni	BLE	4	Minori rischi tecnici sono stati valutati nel processo di anonimizzazione dei dati
USA (Utah)	Healthy Together	BLE, GPS	3	La geolocalizzazione è stata considerata un eccesso rispetto al principio di minimizzazione dei dati. Il periodo di conservazione dei dati non menziona l'eliminazione dei dati in caso di test negativi.
China	Chinese Health Code System	GPS, Data Mining	1	La natura obbligatoria del sistema fa cadere il principio di volontarietà. La geolocalizzazione, il data mining e altri trattamenti di dati (ad esempio cartelle cliniche e cronologia dei viaggi registrati sul codice QR assegnato) sono stati considerati un eccesso rispetto ai principi di minimizzazione e trasparenza dei dati. [4][5]

Tabella 3: Classificazione e comparazione di alcuni esempi di applicazioni basate su diverse tecnologie

Chi è Alessandro Di Fazio?

Alessandro Di Fazio, laureato in Scienze dell'Informazione presso l'Università di Pisa, classe '61. Nel tempo libero ama sporcarsi le mani con il grasso di moto e auto d'epoca. É cresciuto come consulente delle soluzioni integrative nell'ambito delle Telecomunicazioni in HP (Hewlett-Packard), è stato dirigente dei sistemi informativi in AIFA, responsabile e promotore dei servizi di GDPR Compliace, Data Privacy e Cybersicurity presso DOTS fino allo scorso Febbraio. Ora lavora come Data Protection Officer del gruppo Tinexta SpA.

Cos'è Tinexta?
Tinexta S.p.A. quotata nel segmento STAR di Borsa Italiana è una holding. Il gruppo è leader in Italia in tre principali aree operative (Digital Trust, Credit Information and Management, Innovazione e Marketing). Tinexta Group conta circa 1300 dipendenti.

Intervista:
MARCO: Data Privacy, GDPR and Personal Freedom.
Numerosi sono stati i provvedimenti in materia di Protezione dei dati personali necessari per ovviare alla situazione generatasi a causa del diffondersi del Sars-Cov-2.

1. **Quali sono gli ambiti in cui il quadro normativo esistente si è più dovuto riadattare?**

La domanda è complessa e con una forte valenza legale. In generale, piuttosto che riadattare si è dovuto **soprattutto reinterpretare.** Se possiamo riferirci all'**Europa** il riferimento normativa entro cui bisogna muoversi è chiaramente quello **del GDPR**. Tutti gli attori coinvolti hanno interpretato le leggi già definite all'interno di questo contesto normativo. I vari enti regolatori hanno provveduto a diffondere le comunicazioni e FAQ che di fatto investivano anche altri ambiti operativi. Primo tra tutti è stato l'ambito **sanitario**, per cui una serie di provvedimenti emergenziali sono andati a definire quali potessero essere i limiti e le finalità da parte del Garante. Un altro ambito è stato quello degli **enti locali** (Regioni, Comuni, Polizia). Decisamente più corposo è stato l'intervento in ambito **giuslavoristico. In particolare,** la definizione del nuovo ruolo attivo del datore di lavoro nella gestione del così detto "evento di contagio" per il quale esso è tenuto a conoscere la patologia. Poi altri ambiti sono stati quello scolastico, delle sperimentazioni cliniche e infine quello tecnologico con l'intervento relativo al "contact tracing".

2. **Quindi è corretto dire che non c'è stato alcun tipo di rilassamento dei vincoli normativi vigenti?**

Più che rilassamento dei vincoli si sono date interpretazioni. Nell'ambito della sicurezza del trattamento si distinguono generalmente due approcci: "É lecito tutto ciò che non è vietato oppure è lecito solo ciò che esplicitamente viene definito lecito"? Per definire queste chiarificazioni e interpretazioni possiamo dire che si è privilegiato questo secondo approccio.

3. **É chiaro che il principio sia quello del salvaguardare l'interesse pubblico, ma in molti temono restrizioni della propria libertà personale, quali sono i principi che dovrebbero guidare il trattamento dei nostri dati in questi tempi?**

I principi sono due. Il primo è quello di **pertinenza e non eccedenza** nel trattamento del dato personale. Questo significa che è necessario minimizzare il trattamento dei dati a quanto basta per il conseguimento della finalità del trattamento. In particolare, il principio di non eccedenza si muove anche sull'asse temporale. Quando sentiamo dire che un certo dato verrà utilizzato ai fini pandemici per la durata dell'emergenza sanitaria, ecco questo di fatto è un rischio. Il secondo principio riguarda la **sicurezza del trattamento dei dati** il quale si impianta su tre assi: **Integrità** cioè che il dato deve essere corretto lungo tutto il suo ciclo di vita, **Disponibilità** cioè che il dato non deve essere perso e infine **Riservatezza** cioè che il dato sia reso disponibile solamente alle persone autorizzate e non a terzi. Questo significa che quando diciamo che i dati verranno utilizzati fino alla fine dello stato di emergenza, il titolare del trattamento dei dati personali deve essere in grado di gestire una sorta di metadato sul dato personale cioè la "data di scadenza del trattamento". Questo

potrebbe non essere un requisito semplice da implementare. Non a caso è uno dei punti di maggiore attenzione.

4. **Quali sono i requisiti tecnologici ed organizzativi che governi e aziende private possono porre in essere per mantenere flessibilità operativa e, allo stesso tempo, garantire la conformità ai vari requisiti di legge?**

La **Data Integrity** che già si applica nell'ambito farmaceutico è un modello di riferimento unico in termini di gestione dei dati a livello tecnologico e organizzativo. Essa fa tipicamente riferimento ai metadati o all'attribuzione di responsabilità sulla gestione del dato. Declinare la Data Integrity nel mondo della privacy è chiaro che determini una forte spinta **alla digitalizzazione quindi dematerializzazione dei dati**. Questo è un primo fondamentale requisito tecnologico. Un altro aspetto che per altro è comune alla Data Integrity e alla GDPR è l'**Accountability**. Cioè il fatto che io debba essere in grado di capire chi ha trattato un certo dato. Ovvero che ci siano degli addetti al trattamento dei dati che siano identificabili, tracciabili e che abbiano una formazione adatta al ruolo che devono svolgere nell'ambito del trattamento del dato. La vogliamo chiamare **segregation of duty**?

5. **In molti casi le aziende si sono ritrovate a ricoprire un nuovo ruolo nel gestire i dati sanitari del proprio personale. Come DPO di Tinexta, quali sono state le contromisure prese?**

- Per prima cosa abbiamo definito un modello di DPIA (Data Protection Impact Assessment), si tratta di un processo che si attua preventivamente al trattamento dei dati personali qualora questo trattamento abbia un profilo caratteristiche di rischiosità elevate. Tale modello è stato applicato per tutti i dipendenti di Tinexta.
- Altra area di intervento è stato definire misure organizzative a fattor comune parametrizzabili. In pratica si è trattato di creare istruzioni di lavoro comuni per gli addetti al trattamento tenendo conto della diversità tra le varie aziende del gruppo, in particolare le diversità legislative locali. É stato complesso.
- Infine, mi sono occupato della creazione di una soluzione tecnologica, tramite un'azienda del gruppo, che si chiama DizMe basata su Blockchain. La soluzione garantisce la gestione in sicurezza dei dati dell'azienda proprio perché basata su un meccanismo di pseudonimizzazione forte.

6. **In USA, Google e altri colossi del digitale stanno promuovendo la definizione di uno nuovo impianto giuridico per la gestione dei dati personali e la GDPR Europea è stata portata a modello. Il GDPR è effettivamente un modello solido che sta garantendo, anche in nella situazione corrente, una protezione maggiore? Quali sono i punti critici?**

Il GDPR è di certo è un ottima regolamentazione e in quanto tale tenta di trovare il punto di equilibrio tra la libertà dell'interessato e la circolazione dei dati personali come linfa vitale delle organizzazioni e dei mercati. Il principio di portabilità dei dati previsto dal GDPR è un esempio chiaro. Voglio un offerta energia migliore e più adatta ai miei profili di consumo, richiedo questo profilo all'azienda fornitrice e lo sottopongo ad un 'altra azienda per ottenerne uno per me più vantaggioso. Questo è un esempio chiarificatore, **il rischio privacy è un rischio sulla libertà degli interessati, mancando questa cadono una serie di presupposti di convivenza**. Un punto del GDPR critico è **l'integrazione in un contesto internazionale**. Di recente la corte di giustizia europea ha cancellato il Privacy Shield. L'accordo fatto tra commissione europea e Governo americano che riconosceva i sistemi di garanzia della privacy tra i due stati come assimilabili, equivalenti. In pratica, era lecito trattare i dati dei cittadini europei negli stati uniti. Questo ora è stato cancellato con un impatto dirompente in tutti gli ambiti quello farmaceutico ma anche quello del digitale e consumer, penso ad esempio all'outsourcing dei grandi provider di Data Center.

7. **Tra i provvedimenti presi per il contenimento della diffusione del virus, maggiore interesse hanno suscitato quelli relativi al monitoraggio e tracciamento degli individui. Quali sono i mezzi che abbiamo a disposizione per monitorare nel lungo termine il rientro alla normalità? O anche in questo ambito è meglio dire "New Normal"?**

Parlando di mezzi per monitorare il rientro alla normalità parliamo in pratica di indicatori. Gli indicatori sono sociali ed economici e sono gestiti a livello governativo. Per quanto riguarda il tracciamento, questo è un trattamento di dati personali. La geolocalizzazione, i social network sono metadati che sono in essere da tanto tempo. Quello che emerge oggi da questa situazione di pandemia forse è proprio una maggiore consapevolezza dell'importanza e del rischio associati al tracciamento e all'uso dei dati personali. In particolare all'uso secondario di questi dati di tracciamento. Se per l'App Immuni il tracciamento ha una finalità ben definita cioè quella del contenimento della diffusione del COVID19 è chiaro d'altra parte che se il principio della sicurezza viene meno il trattamento di questi dati diviene del tutto illegale e persino pericoloso per la libertà. Basti pensare ad esempio all'evento di Cambrige Analitica, dove a partire da dati pubblici presenti sui profili Facebook è stato eseguito un trattamento di profilazione degli utenti. Pensando ad uno scenario di "New Normal" in cui sicuramente i tracciamenti continueranno, intravedo da una parte maggiore consapevolezza e di conseguenza anche da parte di tutti gli attori della Privacy una necessità di una trasparenza e sicurezza maggiore dei trattamenti. In un contesto futuribile, mi aspetto maggiore consapevolezza nell' uso migliore del consenso informato da parte di chi lo chiede. Un altro aspetto dello scenario New Normal sarà l'attuazione della politica di conservazione dei dati quindi di una capacità tecnologica per saper gestire il consenso e la conservazione dei dati in maniera idonea. Consapevolezza e gestione del consenso dovrà essere rivista, in questo senso l'armonizzazione delle legislazioni internazionali è importante.

FABIO: Tecnologie, Conservazione e Uso dei Dati raccolti

Le tecnologie di tracciamento digitale sono state identificate come un potenziale strumento per supportare la modalità tradizionale di tracciamento dei contatti per limitare la diffusione del COVID-19. Tuttavia, queste tecnologie sollevano parecchie preoccupazioni riguardo alla privacy. Gli approcci al tracciamento possono essere diversi (localizzazione su rete cellulare, GPS, Bluetooth), passando da metodi più invasivi quali l'utilizzo della geolocalizzazione ad approcci meno invasivi e utilizzati più ampiamente quali l'utilizzo della tecnologia Bluetooth, come ad esempio in Italia per l'App Immuni.

1. **Puoi spiegarci quali differenze ci sono tra le diverse tecnologie disponibili di track and tracing mobile e cosa ha portato a prediligere l'utilizzo della tecnologia Bluetooth rispetto alle altre?**

   La macro differenza è che con una tecnologia di tipo GPS abbiamo la tracciatura del contatto avvenuto ma non sappiamo dove questo sia avvenuto. Il dove è avvenuto ci consente di qualificare meglio il contatto (luogo pubblico, ecc...). E' evidente che le due tecnologie basate sulle reti cellulari o sul posizionamento geografico geolocalizzato sono sicuramente quelle che danno una maggiore ricchezza di informazioni. Sono state implementate anche soluzioni ibride di tracing che hanno l'una e l'altra modalità, di queste 3 categorie. La scelta della tecnologia BLE (Bluetooth Low Energy) è comune a tanti Paesi, senz'altro a tutti i paesi dell'Unione Europea.
   Come valutato dal Garante italiano della Privacy, mentre in alcune regioni distanti dall'Unione Europea e dai suoi standard di protezione dei dati personali (GDPR, ndr) sono state prese in considerazione le altre categorie, noi abbiamo scelto la BLE per l'implementazione di questa piattaforma. Il motivo è essenzialmente che rispetta un po' il principio del GDPR della **minimizzazione dei dati raccolti** al fine dell'individuazione dei possibili contatti con persone contagiate. Da un punto di vista della minimizzazione dei dati è stato ritenuto più importante tracciare il contatto rispetto al

o il motivo luogo dove questo è avvenuto. Questo è stato il motivo fondamentale della scelta della tecnologia BLE.

2. **Potrebbe essere uno svantaggio tenere solo traccia del contatto avvenuto senza la possibilità di localizzarlo?**

   L'efficacia di questi sistemi di tracciatura è basata essenzialmente sul maggior numero di persone che li utilizzano. Il vero fattore di efficacia è la loro diffusione. E' chiaro che un'informazione ricca da un punto di vista di geolocalizzazione consente dei vantaggi, ma la vera efficacia è data dalla sua diffusione. Attualmente l'app Immuni non ha ancora raggiunto una diffusione molto ampia, ma non è solo il caso italiano. L'efficacia più che alla scelta tecnologica la legherei alla diffusione della app del sistema di tracciatura.

3. **Potresti spiegarci meglio il funzionamento dell'app Immuni?**

   Il sistema Immuni è composto da una parte Client che è quella relativa alla app dei dispositivi mobili e una componente Server che ha diverse funzionalità soprattutto quella di gestione delle informazioni legate alla sicurezza e alle transazioni sui contagi in estrema sintesi. Lo scopo di questo sistema è la messa a disposizione degli utenti di uno strumento di allerta relativo all'esposizione al contagio. È un sistema utilizzabile in modo partecipativo, fa sì che i dispositivi interconnessi siano in grado di rilevarsi mutuamente e consente agli utenti di qualificarsi come persona positiva al Covid attraverso una procedura volontaria e assistita da un operatore sanitario. La funzione poi prevede che la app stessa possa presentare un messaggio sui dispositivi degli utenti che avvisa della rilevata vicinanza ad un dispositivo che appartiene ad una persona che ha dichiarato il suo stato di positività al covid, facendo così assumere alla persona che riceve il messaggio una qualifica di "contatto stretto" di un soggetto positivo, quindi informandolo sulle misure necessarie da adottare.
   Questo è il funzionamento in linea di massima, quindi si tratta di un sistema di alerting basato su un modello partecipativo assolutamente volontario.
   C'è un ulteriore parte relativa al trattamento secondario per quanto riguarda la componente backend, quindi la componente server. Questi dati possono essere utilizzati per finalità di sanità pubblica (ricerca scientifica, statistica) per migliorare i modelli di valutazione del rischio e anche per migliorare l'accuratezza degli algoritmi.
   I nostri codici temporanei e randomici RPI (Rolling Proximity Identifiers) e quelli che abbiamo scambiato con le persone con cui siamo stati a contatto restano sul nostro dispositivo per 14 giorni e poi vengono eliminati. Soltanto quando un individuo, risultato positivo al COVID-19, decide di dare il consenso all'uso dei dati raccolti dall'app, questi dati vengono condivisi con il server centrale del sistema.

4. **Hai eventualmente trovato punti deboli in termini di trattamento dei dati dopo la condivisione?**

   In generale, i problemi di sicurezza di questo trattamento stanno principalmente nella parte client, prima ancora che arrivino alla parte server e dipendono dalla tecnologia utilizzata, perché la tecnologia Bluetooth può essere violata. Si parla del cosiddetto "paparazzi attack". Il paparazzi attack evoca la figura del paparazzo, quindi un cyber criminale che si apposta in prossimità di alcuni punti pubblici noti (es. aeroporti, ingressi di alcune zone dove si sa che alcune persone pubbliche passino, proprio come fa un paparazzo). Quando vede passare un individuo interessante dal punto di vista di furto dei dati intercetta le sue informazioni. Parlando della app Immuni sappiamo che c'è un dialogo continuo fra la app e il centro servizi in cui il paparazzo può intercettare un codice pseudonimo e

quindi da quel momento in poi sa che a quell'individuo è associabile quello pseudonimo. Questa tecnica sfrutta la vulnerabilità della tecnologia Bluetooth, proprio perché la tecnologia prevede broadcasting a tutti i dispositivi e nel caso specifico dello sniffer dell'apparato di intrusione del paparazzo.
Il garante della privacy identifica tutti questi rischi, per esempio nel suo documento di "**data privacy impact assessment**". Sul lato client non c'è solo questo, c'è ad esempio la vulnerabilità dello smartphone stesso che potrebbe essere infettato da app che sono in realtà dei **malware** malcelati che fanno altre cose rispetto all'intended use e sono in grado di catturare determinate informazioni. Tutte queste minacce sono state valutate dal garante italiano della privacy che ha dato l'approvazione a Giugno alla app Immuni fornendo però delle prescrizioni che tenessero conto dei rischi ma anche di eventuali eccessi di trattamento non autorizzato nella parte Server. Ha espressamente previsto, richiesto e imposto ai fornitori del servizio per esempio alcune contromisure che riguardano il tempo di conservazione dei dati, la garanzia sulla loro cancellazione effettiva con meccanismi automatici per la **data retention policy**, ha previsto che i ruoli degli amministratori del sistema siano particolarmente sorvegliati e ha minimizzato alcune informazioni di amministrazione raccolte perché non scordiamoci che ad esempio gli indirizzi IP che comunque fanno parte di questo trattamento (o potrebbero farne parte) sono comunque appetibili per altre forme di criminalità informatica. Quindi non c'è solo il dato sanitario di cui parliamo, c'è la così detta "pesca a strascico".

5. **Potresti farci esempi di potenziale utilizzo fraudolento di questi dati, di questi indirizzi IP per altri scopi oltre a quello di avere accesso a dati sanitari?**

   Sono in generale tutte le informazioni di dati personali associabili ad esempio allo stesso smartphone. Sappiamo che lo smartphone è il punto di accesso ad una pletora di servizi da parte dei cittadini. Sullo smartphone ci sono funzionalità di firma digitale, di accesso ai sistemi bancari, ai sistemi di prenotazione di voli, per non parlare dell'ambito della sensoristica prevista all'interno dello smartphone. E' un po' come entrare con un cavallo di Troia, entri nello smartphone e da lì puoi vedere qualsiasi cosa. Certo che nella mia esperienza di DPO fino ad ora ho avuto modo di verificare che non sempre questi attacchi di cyber criminali hanno una finalità utilitaristica, spesso hanno una forma di azione dimostrativa (ad esempio la pubblicazione dei numeri riservati dei parlamentari). Chiaramente si tratta di una grave violazione dei dati personali, ma non ha una finalità immediatamente di lucro o riconducibile ad un'azione utilitaristica, ha un fine dimostrativo. Questi potrebbero essere alcuni degli effetti collaterali di un'eventuale intrusione attraverso questo sistema.

6. **Riassumendo quindi vedi maggiori punti deboli della tecnologia per quanto riguarda la privacy a livello della app (client) che a livello server?**

   Sì, molti rischi sono concentrati a livello client perché parlando ad esempio dei malware che possono essere su uno smartphone questi sono difficilmente controllabili a livello centrale perché non c'è una garanzia come può invece avvenire negli smartphone aziendali dove c'è un controllo maggiore (es. non si possono installare alcune app, etc....).

Conclusioni

Il mondo sta affrontando una grave crisi sanitaria che richiede risposte forti, il cui impatto si manifesterà oltre la fine di questa emergenza. È chiaro che il posizionamento della tecnologia può giocare un ruolo chiave in uno scenario pandemico, ma grande attenzione deve essere prestata dai governi nell'adozione di mezzi di sorveglianza che possono diventare dannosi in termini di privacy dei dati e libertà personale. In questi termini, la promozione di linee guida comuni e di solidi quadri normativi è fondamentale per definire

a livello internazionale un uso della tecnologia commisurato ai rischi reali e che tenga conto dell'equilibrio tra due diritti fondamentali come la salute e la libertà personale.
Le misure straordinarie adottate per contrastare la diffusione di SarS-CoV2 possono essere giustificate da interessi a tutela della Salute Pubblica solo laddove l'utilizzo dei dati personali è limitato nel tempo, minimizzato e costantemente monitorato.

Bibliografia:

[1] Pucci T., Hodovsky J. What did WHO, EC and each country have in terms of a legal framework already in place to combat the virus?. (3 August 2020); https://www.pqegroup.com/blog/2020/08/what-did-who-ec-and-each-country-have-in-terms-of-a-legal-framework-already-in-place-to-combat-the-virus/
[2] European Commission – Communication from the Commission "Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection" Brussels, 16.4.2020 C(2020) 2523 final https://ec.europa.eu/info/sites/info/files/5_en_act_part1_v3.pdf
[3] World Health Organization (WHO) – Ethical considerations to guide the use of digital proximity tracking technologies for COVID-19 contact tracing: Interim guidance, 28 May 2020 https://apps.who.int/iris/bitstream/handle/10665/332200/WHO-2019-nCoV-Ethics_Contact_tracing_apps-2020.1-eng.pdf?sequence=1&isAllowed=y
[4] Mozur, P., Zhong, R. & Krolik, A. In coronavirus fight, China gives citizens a color code, with red flags. The New York Times (1 March 2020); https://go.nature.com/2yfrKLI
[5] Yang, Y., Liu, N., Wong, S.-L. & Liu, Q. China, coronavirus and surveillance: the messy reality of personal data. Financial Times (2 April 2020); https://go.nature.com/3cfvvzG

Key Notes:

- Data Protection Officer (https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en)
- Data Minimisation (https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1528874672298&uri=CELEX:02016R0679-20160504)
- GDPR (https://it.wikipedia.org/wiki/Regolamento_generale_sulla_protezione_dei_dati)