

IL CONFRONTO

Tutti i rischi delle app anti-covid "concorrenti" a Immuni

[Home](#) > [Sicurezza Digitale](#) > [Privacy](#)

A fronte della scelta dell'app Immuni quale piattaforma software nazionale per il contrasto all'epidemia Covid-19, è corretto l'utilizzo di app regionali, comunali, aziendali, o di altri sistemi neanche sottoposti a una valutazione del Garante in merito alla loro idoneità a non ledere dati personali degli utenti? Il punto

3 giorni fa

Federica LamorattaAvvocato, [Pirola Pennuto Zei & Associati](#)**Mario Valentini**Avvocato e DPO, [Pirola Pennuto Zei & Associati](#)

Dalle decine di **app regionali** e comunali usate per la sorveglianza sanitaria ai dispositivi indossabili e alle app aziendali, sono diverse le alternative tecnologiche all'app **Immuni** disperate nel nostro Paese per tentare di contenere la diffusione del Covid-19.

Ma qual è – se c'è – il vantaggio e, soprattutto, sono profilabili **rischi per la privacy** dall'uso di questi sistemi "concorrenti" all'app scelta dal Governo e approvata dal Garante?

I dubbi restano, ed è stato in primis lo stesso presidente dell'Autorità garante per la Privacy, **Antonello Soro** a sollevare qualche perplessità sull'uso di app "alternative". Da ultimo, nelle [faq](#) recentemente pubblicate dal Garante in merito a queste app e che

confermano l'impostazione precedente.

Indice degli argomenti

Le app regionali, comunali e aziendali
I dispositivi indossabili
Garante Privacy e app aziendali: le faq
L'app AllertaLOM
Immunì, come funziona e la privacy
Conclusioni

Le app regionali, comunali e aziendali

Lo scenario desta attenzione perché si moltiplicano le app siffatte.

A partire dall'8 giugno fino al 30 settembre, in Sicilia è stato avviato il protocollo sanitario "**SiciliaSiCura**", contenuto nell'ordinanza n. 24 del 6 giugno 2020 emanata dal Presidente della Regione.

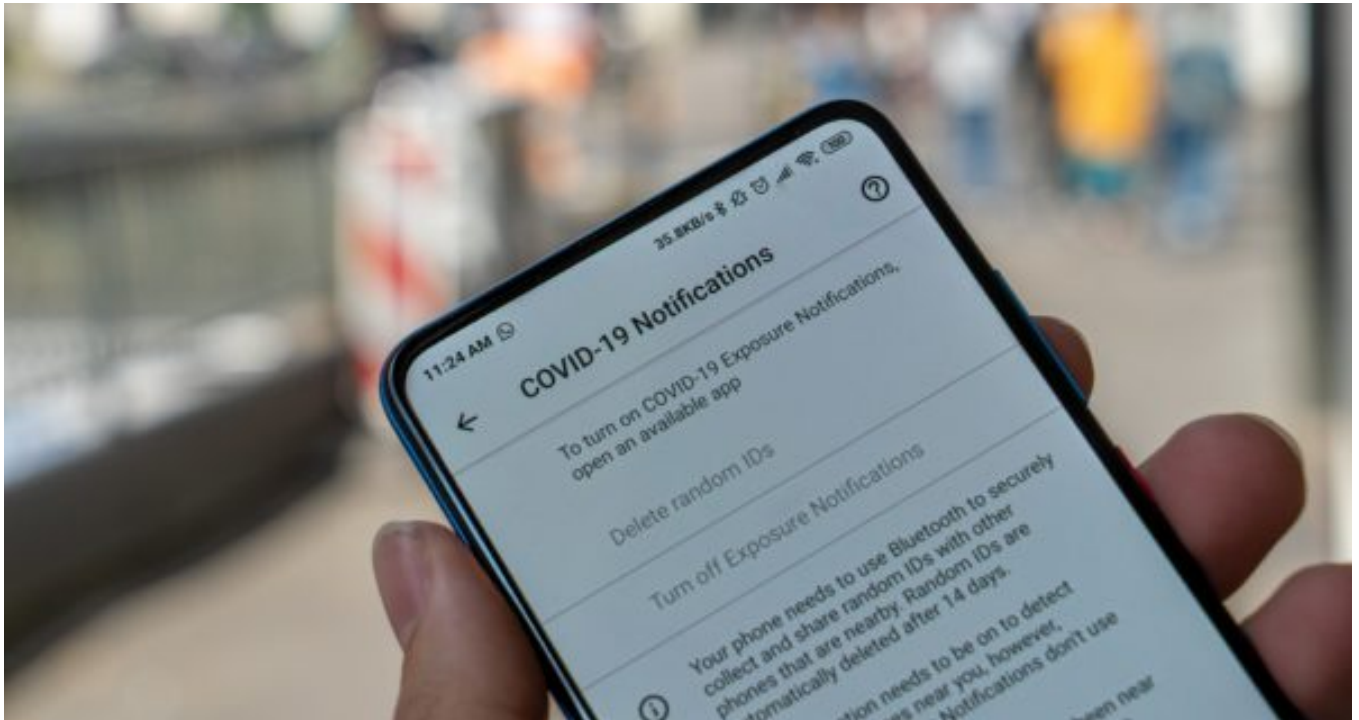
Tra gli elementi più importanti che sono stati previsti, vi è l'applicazione facoltativa che offre assistenza sanitaria ai turisti ed ai non residenti che si recano sull'isola e che, però, non si sovrappone all'app Immunì ma si limita a tenere in contatto i turisti con il sistema sanitario regionale.

Inoltre, anche in Sardegna, dove la registrazione digitale è diventata obbligatoria per i visitatori, è stata sviluppata l'app "**SardegnaSicura**", cui può registrarsi chiunque arrivi sull'isola mediante l'utilizzo dei sistemi operativi iOS e Android.

La Regione Lazio, invece, ha attivato l'applicazione "**DoctorCovid**", dedicata al personale sanitario per gestire le persone in quarantena presso il proprio domicilio nonché a monitorare i cittadini a casa con sintomi.

Non mancano, poi, app di tracciamento dei contatti che vengono utilizzate a titolo volontario in ambito aziendale, dietro accordo con i sindacati, come ad esempio nel caso del gruppo hi-tech del settore militare. A Siena, ad esempio, tra le misure adottate per le visite alla Cattedrale ed al Museo, oltre alla rilevazione della temperatura all'ingresso, è stata introdotta l'app per smartphone "**The Right Distance**" che, però, non richiede informazioni personali lesive della tutela dei dati personali ma serve esclusivamente a mantenere la giusta distanza tra le persone.

Qui sotto un approfondimento sulle app aziendali.



I dispositivi indossabili

Altro strumento tecnologico il cui utilizzo è ancora fortemente auspicato per contrastare la pandemia legata al diffondersi del Coronavirus è il wristband (braccialetti).

I wristband sono dei dispositivi indossabili, che avvisano l'utente se questo si avvicina troppo a un'altra persona. Entrambi i soggetti devono ovviamente indossare il *device* perché il sistema funzioni.

Per questo è consigliabile adottare il sistema in luoghi "controllabili", come aziende, stabilimenti balneari, biblioteche e così via: il wristband sarà di conseguenza fornito a ogni singola persona che vorrà entrarci.

Per quanto riguarda il funzionamento, per poter dare l'allarme tali dispositivi necessitano di un sistema Bluetooth a bassa potenza, come quello adottato dall'app [Immun](#)i. Attraverso tale sistema si consentono misurazioni precise e un basso consumo energetico.

La posizione del dispositivo nello spazio non viene memorizzata, tant'è che nessuno dei provider sul mercato utilizza il GPS.

Alcuni wristband hanno bisogno di un'app nativa per funzionare, attraverso la stessa i wristband memorizzano i dati dei contatti avvenuti tra i vari utenti.

Altri, invece, non necessitano di alcuna piattaforma a supporto, anche perché non salvano tali informazioni.

La differenza sta nell'utilizzo che ne viene fatto. Alcuni sistemi memorizzano i contatti che gli utenti hanno fra loro. Tale soluzione è specifica per **situazioni più "istituzionali"**, come nel caso in cui in azienda si scopre che un dipendente è positivo al Covid-19, il sistema potrà mandare una notifica ai suoi contatti più frequenti, invitandoli a fare attenzione e a contattare un medico. In definitiva è, nel piccolo, ciò che fa anche Immuni.

Questo sistema, invece, difficilmente potrebbe trovare applicazioni in ambienti più informali, come stabilimenti balneari o bar e ristoranti. Infatti, in questo caso l'utente non accetterebbe di condividere i propri dati con il gestore. Anche l'utilità stessa di questa funzione sarebbe limitata, dato che i contatti sarebbero molto limitati nel tempo e nello spazio. Per questo motivo il wristband, in tali situazioni, lavorerebbe solo come deterrente per evitare i comportamenti scorretti degli avventori.

Quindi al momento esistono strumenti che lavorano in maniera diversa, specificamente pensati per venire incontro alle necessità di grandi aziende o piccole attività.

Alcune società, quali la società **Neosperience**, stanno sviluppando un wristband bluetooth, denominato **Disband**, che possa assolvere entrambe le funzioni, personalizzando il suo funzionamento in base alle necessità.

Infatti, se il wristband viene impiegato in azienda, metterà a disposizione del management una piattaforma backend dove poter controllare le informazioni raccolte anonimizzate.

Invece, se dovesse essere adottato da una piccola realtà, come un ristorante, questa funzione sarebbe oscurata, e funzionerebbe solo come allarme di prossimità.

Garante Privacy e app aziendali: le faq

Si legge nelle faq 9 e 10 del Garante sul coronavirus:

“Sono utilizzabili applicativi con funzionalità di “contact tracing” in ambito aziendale?

La funzionalità di “contact tracing”, prevista da alcuni applicativi al dichiarato fine di poter ricostruire, in caso di contagio, i contatti significativi avuti in un periodo di tempo commisurato con quello individuato dalle autorità sanitarie in ordine alla ricostruzione della catena dei contagi ed allertare le persone che siano entrate in contatto stretto con soggetti risultati positivi, è – allo stato – disciplinata unicamente dall’art. 6, d.l. 30.4.2020, n. 28.

Al fine di contenere il rischio di contagio sul luogo di lavoro sono disponibili applicativi che non trattano dati personali?

Sì, il datore di lavoro può ricorrere all'utilizzo di applicativi, allo stato disponibili sul mercato, che non comportano il trattamento di dati personali riferiti a soggetti identificati o identificabili. Ciò nel caso in cui il dispositivo utilizzato non sia associato o associabile, anche indirettamente (es. attraverso un codice o altra informazione), all'interessato né preveda la registrazione dei dati trattati.

Si pensi alle applicazioni che effettuano il conteggio del numero delle persone che entrano ed escono da un determinato luogo, attivando un “semaforo rosso” al superamento di un prestabilito numero di persone contemporaneamente presenti; oppure alle funzioni di taluni dispositivi indossabili che emettono un avviso sonoro o una vibrazione in caso di superamento della soglia di distanziamento fisico prestabilita (dunque senza tracciare chi indossa il dispositivo e senza registrare alcuna informazione). Si pensi, altresì, ad applicativi collegati ai tornelli di ingresso che, attraverso un rilevatore di immagini, consentono l'accesso solo a persone che indossano una mascherina (senza registrare alcuna immagine o altra informazione). In questi casi spetta comunque al titolare verificare il grado di affidabilità dei sistemi scelti, predisponendo misure da adottare in caso di malfunzionamento dei dispositivi o di falsi positivi o negativi”.

WHITEPAPER

Sicurezza: perchè puntare su un approccio zero trust?

 Sicurezza  Sicurezza dei dati

E-mail

E-mail aziendale

☐ Consente all'invio di comunicazioni promozionali inerenti i prodotti e servizi di soggetti terzi rispetto ai Titolari con modalità di contatto automatizzate e tradizionali da parte dei terzi medesimi, a cui vengono comunicati i dati.

ISCRIVITI

L'app AllertaLOM

Tra le applicazioni che sono state elaborate al fine di contrastare il diffondersi del Coronavirus, merita una particolare analisi l'App "**AllertaLOM**", introdotta dalla Regione Lombardia e definita un importante strumento per il monitoraggio e la mappatura della diffusione del Covid-19.

Con riguardo al suo funzionamento, è necessario scaricare l'applicazione tramite apple Store o Google Play Store, compilando – in forma anonima e su base volontaria – un questionario integrato all'interno dell'App. stessa denominato "Cercacovid", la cui finalità è quella di raccogliere dati attraverso i quali viene calcolata la densità di rischio e viene prevista la possibilità di focolai non conosciuti ed individuati trend nel tempo, consentendo in tal modo una campionatura efficace e mettendo a disposizione dell'Unità di Crisi regionale e degli specialisti, informazioni complete e strutturate sulla diffusione del contagio sul territorio lombardo.

La **sezione Coronavirus** e il **questionario** permettono una sorta di "**triage**" a distanza.

Come anticipato, il questionario sopra descritto viene compilato dagli utenti in via del tutto anonima e non si rivolge solo a chi manifesta sintomi ricollegabili al Covid-19, ma a **tutti i cittadini**.

Gli utenti sono infatti invitati a ripetere ogni giorno (non più di una volta al giorno) la compilazione del questionario, aggiornando il loro stato di salute.

Le informazioni raccolte contribuiscono ad alimentare una "**mappa del rischio contagio**", che viene continuamente aggiornata e che permette agli esperti di sviluppare modelli previsionali sul contagio. L'obiettivo ultimo è quello di incrociare l'analisi dei dati raccolti con altri dati a disposizione della Regione Lombardia e, partendo dalle evidenze cliniche fornite dalle strutture sanitarie e dai presidi sul territorio regionale, calcolare il grado di rischio di contagio, rafforzando in tal modo le tutele per tutti i cittadini, sintomatici e asintomatici. Mediante l'utilizzo dell'App, quindi, si fornisce all'Unità Regionale di gestione della crisi elementi utili a localizzare le zone con maggior probabilità di ospitare un focolaio attivo, o ad individuare la ripresa del contagio in zone considerate meno a rischio, nonché sviluppare analisi statistiche ed epidemiologiche indispensabili sia per il presente che per il futuro.^[1]

L'App AllertaLOM era già utilizzata per le allerte della Protezione Civile, ovvero per i documenti ufficiali che la Regione Lombardia emette in previsione dell'arrivo di fenomeni potenzialmente critici per il territorio e, sin dall'inizio dell'emergenza Coronavirus, il suo utilizzo è stato fortemente caldeggiato dalla Regione stessa, come evidenziato con l'ordinanza n. 525 del 09 aprile 2020 con cui la

Regione Lombardia ha disposto che “ai fini del contenimento e della gestione dell’emergenza epidemiologica da COVID-19 si è resa necessaria la valorizzazione dell’App. denominata “AllertaLOM” in uso presso la Regione”.^[2]

Inoltre, proprio quando la Presidenza del Consiglio dei Ministri ha annunciato nell’ultima conferenza stampa il possibile avvio della sperimentazione dell’app Immuni, la Regione Lombardia ha emesso l’ordinanza n. 546 del 13 maggio 2020 in cui ha disposto che “è fortemente raccomandato l’**utilizzo della app. “AllertaLom”** da parte del datore di lavoro e di tutto il personale, compilando quotidianamente il **questionario “CercaCovid”**”.^[3]

In relazione a tale disposizione sono sorti numerosi **dubbi** e **criticità**. Infatti, l’utilizzo dell’espressione “forte raccomandazione all’utilizzo della app ‘AllertaLom’ da parte del datore di lavoro e di tutto il personale, compilando quotidianamente il questionario “CercaCovid”, sta ad indicare un “quasi” obbligo all’installazione ed uso dell’applicazione, vietato sia dal Garante sia dalle raccomandazioni della Commissione Ue e da EDPB ed EDPS. Infatti, il Garante nell’audizione in Parlamento dell’8 aprile ha dichiarato di “...**preferire il ricorso a sistemi fondati sulla volontaria adesione dei singoli che consentano il tracciamento della propria posizione. Tuttavia, per garantire la reale libertà (e quindi la validità) del consenso al trattamento dei dati, esso non dovrebbe risultare in alcun modo condizionato**”.^[4]

Inoltre, sul sito della **Regione Lombardia** viene indicato *che* “gli utenti possono compilare un questionario integrato all’interno dell’app che rende possibile raccogliere dati, in forma anonimizzata, e mettere a disposizione dell’Unità di Crisi regionale e degli specialisti informazioni complete e strutturate sulla diffusione del contagio sul territorio lombardo”. Il termine “**anonimizzata**” è ambiguo, in quanto con esso potrebbe intendersi che i dati raccolti possano qualificarsi inizialmente come dati personali, ma poi ci sia ad esempio un processo di aggregazione dei dati che porta alla loro anonimizzazione. Il processo di anonimizzazione, infatti, è un trattamento di dati personali perché comporta l’utilizzo di dati personali al fine di privarli delle informazioni che consentono di rendere una persona “identificata o identificabile”.

Tale interpretazione è stata smentita dalla stessa Regione Lombardia, che nella Guida per l’utente all’utilizzo, pubblicata sul sito della Regione stessa, ha disposto che il questionario è anonimo, comportando, quindi, che una persona non possa essere “identificata, direttamente o indirettamente”.

Tuttavia, nell’informativa sul trattamento dei dati personali ex art. 13 GDPR mediante l’App. AllertaLom, che viene fornita dalla Regione Lombardia agli interessati viene chiesto un consenso al trattamento dei dati che non sarebbe necessario in caso di trattamento di dati del tutto anonimi.

Inoltre, la stessa informativa prevede che vengono trattati i seguenti dati personali “Il sesso, l’età, il domicilio, il luogo di lavoro, l’eventuale necessità di spostamenti rispetto al domicilio, l’eventuale frequentazione di luoghi pubblici poi chiusi a seguito dell’emergenza Covid-19, gli eventuali contatti recenti con persone positive a Covid-19, una eventuale positività riscontrata, gli eventuali sintomi connessi alla manifestazione dell’infezione dal virus” e questi dati sono collegati a “un codice identificativo del suo dispositivo mobile”.

Non viene, quindi, raccolto il nome e cognome della persona, ma come ben sappiamo questi sono solo una categoria di dati personali, in quanto i *cookies* per esempio non ci dicono il nome della persona ma, come nel caso dell’App. AllertaLom, **identificano il suo dispositivo e le caratteristiche** del suo utente ed è logico che comportino il trattamento di dati personali, al punto che sono stati oggetto della Direttiva ePrivacy 2002/58/CE e proprio il limite relativo all’utilizzo dei dati che indirettamente consentono di risalire a un individuo è ancora oggetto dei lunghi dibattiti. L’informativa sul trattamento dei dati personali AllertaLom fa riferimento al trattamento dei dati personali per la fruizione del “Servizio”, che tuttavia non viene definito nell’informativa. I termini e condizioni dell’app lo definiscono invece come “il servizio come attraverso il quale gli utenti possono prendere visione di talune informazioni relative alle allerte di protezione civile emesse dal Centro Funzionale Monitoraggio Rischi Naturali di Regione Lombardia e/o ulteriori informazioni di pubblico interesse emesse dall’Ente Regione Lombardia”, ma per accedere a informazioni non è necessario trattare i dati del questionario che possono qualificarsi anche come **dati sulla salute**. Se la finalità del trattamento fosse stata unicamente la ricezione di informazioni non sarebbe stato necessario richiedere il **consenso dell’utente** al trattamento dei dati personali perché il

trattamento sarebbe stato necessario per l'utilizzo dell'app. In realtà l'informativa di AllertaLom menziona che "detti dati potranno altresì essere trattati per elaborare **informazioni statistiche anonime sull'uso dell'app e del servizio**, anche per verificarne il funzionamento, nonché in assolvimento di obblighi di legge", ma poi indica come base giuridica di tutti i trattamenti sopra indicati un unico consenso e non menziona in ogni caso il processo di anonimizzazione per "raccolgere dati, in forma anonimizzata, e mettere a disposizione dell'Unità di Crisi regionale e degli specialisti informazioni complete e strutturate sulla diffusione del contagio sul territorio lombardo" citato sul sito della Regione Lombardia.

Immuni, come funziona e la privacy

Infine, per un confronto: Immuni. Dal primo giugno l'app Immuni, sviluppata dalla società Bending Spoons Spa su iOS e Android, è scelta dal Governo italiano per il **contact tracing** dei soggetti risultati positivi al Covid-19, è disponibile negli store Apple (iOS) e Google (Android).

Dopo una prima fase di sperimentazione, partita l'8 giugno nelle Regioni Abruzzo, Liguria, Marche e Puglia, dal 15 giugno è operativa su tutto il territorio nazionale.

L'app rappresenta un supporto tecnologico per limitare la diffusione del Covid-19 ed aumentare la sicurezza nella fase di ripresa delle attività. Il progetto è nato dalla collaborazione tra Presidenza del Consiglio dei ministri, Ministro della Salute, Ministro per l'Innovazione Tecnologica e la Digitalizzazione, Regioni, Commissario straordinario per l'emergenza Covid-19 e le società pubbliche Sogei e **PagoPa**. Inoltre, tale progetto è stato sviluppato grazie ad un'approfondita interlocuzione con l'Autorità Garante per la protezione dei dati personali (il "Garante"), riservando, quindi, massima attenzione alla tutela dei dati personali.

Con riguardo al fondamento normativo dell'app, con l'art. 6 del **D.L. n. 28 del 30 aprile 2020** che sono state fissate le regole per l'introduzione della app. di allerta del Covid-19, con utilizzo esclusivamente su base volontaria. La scelta di non utilizzare tale app. è quindi libera e non deve comportare discriminazioni di alcun genere, né restrizioni alla libertà di circolazione dei cittadini interessati.

L'app è basata su un sistema cosiddetto di "contact tracing", finalizzato ad informare ed allertare gli utilizzatori di essere entrati in contatto con una persona affetta da Covid-19. Il trattamento dei dati potrà avvenire esclusivamente per le finalità indicate dalla legge, garantendo l'assoluto anonimato degli utenti utilizzatori dell'applicazione.

L'applicazione utilizza la tecnologia Bluetooth per rilevare i contatti tra i diversi dispositivi degli utilizzatori e si appoggia su un sistema di notifica dell'esposizione al contagio realizzato da Apple e da Google.

L'utente può scaricare l'applicazione senza la necessità di effettuare alcuna registrazione che richieda l'inserimento dei propri dati, e senza dover creare un account personale di identificazione. **Gli unici dati che devono essere indicati per l'utilizzo dell'App sono quelli relativi all'età, superiore ad anni 14, ed alla provincia di domicilio**, modificabile in qualsiasi momento in caso di mutamento. Successivamente, l'utente deve autorizzare l'applicazione ad inviare le notifiche di esposizione al Covid-19 ed attivare il Bluetooth.

Solo per i sistemi operativi Android è richiesta **l'autorizzazione alla geolocalizzazione**, che, pur non essendo utilizzata dall'App. Immuni, è comunque richiesta dal sistema operativo, al fine di rilevare i dispositivi Bluetooth, che si trovino nelle vicinanze.

L'App. Immuni genera degli algoritmi protetti dalla crittografia, che danno luogo ad una temporary exposure key **"TEK"**, che cambia giornalmente. La chiave dell'utente genera, ogni 10 minuti, un Rolling Proximity Identifier **"RPI"** con altri utenti.

Nel caso in cui un soggetto positivo al Covid-19 abbia installato la app. potrà acconsentire, rendendo disponibile l'elenco delle proprie TEK degli ultimi 14 giorni ed attivare l'allerta su tutti i dispositivi che siano entrati in contatto con il proprio. Con tale autorizzazione, fornita all'operatore sanitario mediante la generazione di una password temporanea "OTP", la app. trasmette al sistema l'informazione sanitaria del contagio ed ulteriori informazioni ritenute di interesse per l'indagine epidemiologica, quali la provincia di domicilio dell'utilizzatore, il numero di contatti che ha avuto, la durata dei contatti a rischio.

Per ciascun contatto la app elabora la data in cui lo stesso si è verificato, la durata del contatto, l'intensità del segnale Bluetooth registrato durante il tempo del contatto, il rischio di contagiosità dell'utente e l'indice di rischio di contagio.

Quest'ultimo dato viene elaborato attraverso l'algoritmo messo a disposizione da apple e da Google, il quale esamina due parametri, ovvero l'intensità del segnale Bluetooth, che attesterebbe la **vicinanza** del contatto, e la **durata** del contatto.

La app, inoltre, raccoglie quotidianamente ulteriori informazioni, che trasmette automaticamente al sistema. Tali informazioni sono finalizzate a comprendere la diffusione dell'utilizzo della app Immuni sul territorio nazionale. A tal fine sono raccolti dati relativi: alla provincia di domicilio, al sistema operativo utilizzato (iOS o Android), all'attivazione o meno del Bluetooth, alla concessione delle autorizzazioni di notifica del rischio di contagio, all'avvenuta ricezione o meno e, quando esistenti, di notifiche relative ad un sospetto contagio.^[5]

Queste ulteriori informazioni vengono raccolte esclusivamente dai dispositivi apple, in quanto le stesse, per la loro attendibilità, necessitano di un meccanismo di verifica dell'autenticità del dispositivo mobile che raccoglie le informazioni. Analogo meccanismo sarà sviluppato anche per i sistemi Android.^[6]

In base a quanto disposto nel D.L. 28/2020 e nel Regolamento UE 679/2016 ("**GDPR**"), il Ministero della Salute, in qualità di titolare del trattamento dei dati, con nota del 28 maggio 2020 ha trasmesso al Garante la valutazione di impatto, descrivendo il meccanismo di funzionamento della app immuni.

In particolare, il Garante ha esaminato il rispetto del meccanismo di funzionamento dell'app in relazione ai requisiti normativi previsti dall'art. 6 del D.L. 28/2020 e con il provvedimento n. 95 del 1 giugno 2020, ha autorizzato il Ministero della salute ad avviare il trattamento relativo al Sistema di allerta Covid-19 ("App Immuni").

Infatti, sulla base della valutazione d'impatto ex art. 35 del GDPR, trasmessa dal Ministero della salute per essere autorizzato ad avviare il trattamento di dati personali relativo al "Sistema di allerta Covid-19", "al solo fine di allertare le persone che siano entrate in contatto stretto con soggetti risultati positivi e tutelarne la salute attraverso le previste misure di prevenzione nell'ambito delle misure di sanità pubblica legate all'emergenza Covid-19, mediante una piattaforma unica nazionale "per la gestione del sistema di allerta dei soggetti che hanno installato, su base volontaria, un'apposita applicazione sui dispositivi di telefonia mobile", il Garante ha ritenuto che il trattamento di dati personali effettuato nell'ambito del Sistema può essere considerato **legittimo e proporzionato**, essendo state previste misure volte a garantire in misura sufficiente il rispetto dei diritti e delle libertà degli interessati, attenuando i rischi che potrebbero derivare da trattamento dei dati personali degli stessi.

Tuttavia, il parere è accompagnato dal rilievo di alcune **criticità e vulnerabilità** del sistema e dall'indicazione delle necessarie prescrizioni che il Ministero della Salute dovrà soddisfare nei prossimi 30 giorni.

Infatti, tenuto conto della complessità del sistema di allerta e del numero dei soggetti potenzialmente coinvolti, il Garante ha comunque ritenuto di fornire una serie di misure volte a rafforzare la sicurezza dei dati delle persone che scaricheranno la app.

In particolare, l'Autorità ha 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 e dovranno, altresì, essere portati a conoscenza del fatto che il sistema potrebbe generare notifiche di esposizione che non sempre riflettono un'effettiva condizione di rischio.^[7]

Gli utenti dovranno avere, inoltre, la possibilità di **disattivare temporaneamente l'app Immuni** attraverso una funzione facilmente accessibile nella schermata principale della stessa.

I dati raccolti attraverso il sistema di allerta non potranno essere trattati per finalità non previste dalla norma che istituisce l'App.

Dovrà necessariamente essere garantita anche la **trasparenza del trattamento a fini statistico-epidemiologici** dei dati raccolti mediante l'individuazione di modalità adeguate a proteggerli, evitando ogni forma di riassociazione a soggetti identificabili ed adottando idonee misure di sicurezza e tecniche di "anonimizzazione".^[8]

Dovranno, inoltre, essere introdotte misure volte ad assicurare il **tracciamento delle operazioni compiute dagli amministratori di sistema** sui sistemi operativi, sulla rete e sulle basi dati.

La conservazione degli indirizzi IP dei cellulari dovrà essere commisurata ai tempi strettamente necessari per il rilevamento di anomalie e di attacchi e dovranno essere adottate misure tecniche ed organizzative finalizzate a mitigare i rischi derivanti da eventuali falsi positivi.

Particolare attenzione dovrà, poi, essere dedicata all’informativa ed al messaggio di allerta, tenendo altresì conto del fatto che è previsto l’uso del Sistema anche da parte di minori ultraquattordicenni.^[9]

Il Garante ha sottolineato infine che il trattamento di dati personali raccolti attraverso la app Immuni da parte di soggetti non autorizzati, può determinare un trattamento di dati personali **illecito**, che potrà eventualmente assumere rilievo anche sotto il profilo penale.

Tuttavia, nonostante il complessivo giudizio positivo di accompagnamento al provvedimento di autorizzazione trasmesso nella nota del Garante in ordine alla sufficiente tutela dei diritti e delle libertà degli interessati, nonché alla proporzionalità delle misure previste in relazione ai rischi connessi al trattamento dei dati personali, “Sparuti ma aggressivi drappelli di critici dell’app di tracciamento nazionale continuano a puntare il dito contro il lavoro di Bending Spoons e dei 74 esperti”. Inoltre, **“quasi nessuno discute dell’uso di decine di app regionali e comunali usate per la sorveglianza sanitaria”**^[10]; è quanto affermato da Antonello Soro, Presidente del Garante per la protezione dei dati personali, in un’intervista rilasciata al quotidiano “La Repubblica” il 5 giugno 2020.

Conclusioni

Alla luce della panoramica sopra esposta, ci si chiede se sia corretto l’utilizzo delle app regionali, stante la sperimentazione dell’app Immuni, quale piattaforma software nazionale scelta per il contrasto all’epidemia Covid-19, nonché **l’assenza di un parere ed una valutazione del Garante in merito al funzionamento di tali app. ed alla loro idoneità a non ledere dati personali degli utenti.**

Sul tema dell’utilizzo delle **app regionali**, anche a seguito del lancio dell’app. Immuni, si è espresso anche il Garante nella già richiamata intervista a “La Repubblica”, il quale sottolinea che “se le altre app non hanno valutato i rischi, interverremo”.

Infatti, nella suddetta intervista il Garante, rassicurando sul fatto che Immuni non mandi i dati all’esterno e non geolocalizzi, ha ribadito che “nelle prime settimane sotto la spinta emotiva, regioni, comuni e imprese hanno promesso il ricorso a un app salvifica usando come base giuridica l’ordinanza della Protezione civile recepita poi con decreto legge. Per alcuni è rimasto un progetto, **altri ne hanno fatto uno strumento. Ma il ricorso a sistemi autogestiti e autoprodotti anche da società non italiane che hanno offerto tecnologie e servizi è avvenuto con poche garanzie**”.

Il Garante prosegue poi sostenendo che “Molte delle app sono rimaste a livello progettuale, nate sull’onda emergenziale e con interpretazioni troppo estese anche in base al Dpcm citato. Oggi che esiste una norma che definisce le modalità di tracciamento voglio ribadire che parliamo di tracciamento dei contatti e non di tracciamento delle persone e che non possono raccogliere dati sulla salute se non si rispetta la norma primaria invocata in coro in parlamento”.

Infine, al fine di escludere che il loro utilizzo comporti dei rischi per la privacy, il Garante ha ribadito come **“nel nostro ordinamento ora esiste un principio di “accountability”, di responsabilità, per cui chi mette in piedi sistemi di tracciamento deve fare una valutazione di impatto che il Garante valuterà, anche nel prossimo futuro. Se la valutazione non è stata fatta su misura dei rischi, interverremo**”.

Alla luce delle considerazioni sopra esposte, e stante l’operatività dell’app Immuni sull’intero territorio nazionale, non appare condivisibile l’utilizzo, caldeggiato da alcune Regioni, di app “concorrenti” alla stessa, soprattutto in considerazione del fatto che Immuni è definita quale piattaforma nazionale utilizzata per il contrasto al Coronavirus da una norma primaria attualmente all’esame del Parlamento ed ha ottenuto il via libera del Garante, sulla base dell’effettuazione di una valutazione d’impatto ex art. 35 GDPR.

Infatti, e come ben sottolineato dal Garante, è soltanto a seguito di una valutazione d'impatto effettuata sul funzionamento dell'app, e, quindi, dell'esecuzione di tutte verifiche *compliance privacy* che si potrà essere autorizzati ad avviare il trattamento di dati personali.

★ DIGITAL EVENT 9 SETTEMBRE

Cyber Security: tra tecnologia e cultura del dato. Ecco cosa fanno i Security People

Legal # Sicurezza

Scopri di più

Iscriviti subito

-
1. www.regione.lombardia.it ↑
 2. Regione Lombardia, Ordinanza n. 525 del 09 aprile 2020, www.regione.lombardia.it. ↑
 3. Regione Lombardia, ordinanza n. 546 del 13 maggio 2020, www.regione.lombardia.it ↑
 4. Autorità Garante per la protezione dei dati personali, "Audizione informale, in videoconferenza, del Presidente del Garante per la protezione dei dati personali sull'uso delle nuove tecnologie e della rete per contrastare l'emergenza epidemologica da Coronavirus – Commissione IX (Trasporti, Poste e Telecomunicazioni) della Camera dei Deputati" del 08 aprile 2020, www.garanteprivacy.it. ↑
 5. S. Occhipinti, "App Immuni, via libera dal Garante della privacy", www.altalex.com. ↑
 6. Autorità Garante per la protezione dei dati personali, Provvedimento n. 95 del 1 giugno 2020, www.garanteprivacy.it. ↑
 7. Autorità Garante per la protezione dei dati personali, "App "Immuni": via libera del Garante privacy", Comunicato del 1 giugno 2020, www.garanteprivacy.it ↑
 8. Autorità Garante per la protezione dei dati personali, "App "Immuni": via libera del Garante privacy", Comunicato del 1 giugno 2020, www.garanteprivacy.it ↑

9. Autorità Garante per la protezione dei dati personali, "App "Immuni": via libera del Garante privacy", Comunicato del 1 giugno 2020, www.garanteprivacy.it; ↑
10. Intervista ad Antonello Soro, Presidente del Garante per la protezione dei dati personali (*Di Arturo Di Corinto, La Repubblica, 5 giugno 2020*) ↑

@RIPRODUZIONE RISERVATA

WEBINAR

Deep e Dark Web: nulla sfugge agli specialisti (in outsourcing) della Cyber Security



Il webcast è disponibile

[GUARDA](#)

WHITE PAPER

Impatti del GDPR nelle clausole contrattuali dei fornitori: linee guida per la valutazione
22 Gen 2020