Registro dei provvedimenti
n. 95 del 1° giugno 2020

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, alla quale hanno preso parte il dott. Antonello Soro, presidente, la dott.ssa Augusta Iannini, vicepresidente, la dott.ssa Giovanna Bianchi Clerici e la prof.ssa Licia Califano, componenti, e il dott. Giuseppe Busia, segretario generale;

Visto il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati, di seguito "Regolamento");

Visto il decreto legislativo 30 giugno 2003, n. 196, recante "*Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE*", così come modificato dal decreto legislativo 10 agosto 2018, n. 101 (di seguito "Codice");

Viste le "*Linee guida 04/2020 sull'utilizzo dei dati di localizzazione e degli strumenti per il tracciamento dei contatti nel contesto dell'emergenza legata al COVID-19"* del Comitato europeo per la protezione dei dati del 21 aprile 2020 (doc. *web* n. 9322516);

Vista la documentazione in atti;

Viste le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

Relatore il dott. Antonello Soro;

PREMESSO

Il Ministero della salute, con la nota del 28 maggio 2020, ha trasmesso al Garante, ai sensi dell'art. 36, § 5, del Regolamento e dell'art. 2-*quinquiesdecies* del Codice, la valutazione d'impatto sulla protezione dei dati, effettuata ai sensi dell'art. 35 del Regolamento, per essere autorizzato ad avviare il trattamento di dati personali relativo al "*Sistema di allerta Covid-19*", istituito dall'art. 6 del decreto legge 30 aprile 2020, n. 28 (sul quale l'Autorità ha espresso il proprio parere con il provvedimento n. 79 del 29 aprile 2020, doc. *web* n. 9328050), "*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 Ministero ha successivamente integrato la documentazione inviata, fornendo, in data 30 maggio 2020, il testo dell'informativa che si intende rendere agli interessati, ai sensi degli artt. 13 e 14 del Regolamento, in relazione al trattamento dei dati personali.

Nella predetta valutazione di impatto, corredata da ampia documentazione, sono state rappresentate le misure tecniche e organizzative adottate dal Ministero al fine di garantire, in particolare, un livello di sicurezza adeguato ai rischi elevati per i diritti e le libertà degli interessati.

1. La descrizione del Sistema di allerta Covid-19

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

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

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

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

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

Nella valutazione d'impatto il Ministero della salute ha rappresentato l'esigenza, condivisa con le Regioni, di una preliminare fase di sperimentazione del processo di c*ontact tracing* digitale in un numero limitato di Regioni o Province autonome.

1.1. Il rilevamento dell'esposizione a rischio di contagio

In sintesi, si rappresenta che il Sistema Immuni fa ricorso a un approccio c.d. "decentralizzato" di rilevamento dell'esposizione al contagio, di seguito descritto, in cui il contatto stretto con soggetti risultati positivi è notificato direttamente all'utente a seguito di una procedura svolta all'interno del dispositivo su cui è istallata l'app Immuni.

Tale procedura è possibile perché vengono memorizzati all'interno del dispositivo, in un'area crittograficamente protetta, i dati relativi alle interazioni, avvenute con tecnologia

bluetooth in modalità paritaria (*peer-to-peer*), con i dispositivi di altri utenti dell'app Immuni rilevati in sua prossimità.

A) *Installazione e configurazione dell'app*

Ogni utente, dopo aver scaricato l'app Immuni dagli *app store* ufficiali di Apple e Google, procede alla sua installazione e configurazione, ricevendo una sintetica descrizione del suo funzionamento e di alcune caratteristiche del trattamento dei dati personali effettuato attraverso delle infografiche, accompagnate dai *link* all'"*informativa privacy*" e ai "*termini di utilizzo*" del servizio.

L'app Immuni, per il suo funzionamento, non richiede l'identificazione dell'interessato attraverso la registrazione o la creazione di un *account* individuale dei propri utenti.

In tale fase preliminare (c.d. *onboarding*), all'utente viene richiesto di dichiarare di avere almeno 14 anni (età minima per accedere al servizio), di indicare la provincia di domicilio (che successivamente può essere modificata), nonché di concedere i permessi necessari al funzionamento dell'app (abilitazione delle notifiche di esposizione al Covid-19; visualizzazione, per i soli dispositivi iOS, delle notifiche locali generate dall'app; attivazione del *bluetooth* e, per i soli dispositivi Android, anche della geolocalizzazione che, pur non essendo utilizzata dall'app Immuni, è richiesta dal sistema operativo per poter rilevare i dispositivi *bluetooth* nelle vicinanze).

B) *Interazione tra i dispositivi mobili degli utenti*

Una volta compiute queste operazioni l'app inizia a funzionare e viene generata, in modo casuale, mediante algoritmi crittografici, una chiave temporanea (composta da 128 bit) denominata TEK (*Temporary Exposure Key*) che varia con frequenza giornaliera. A partire da ogni TEK, ogni 10 minuti, viene generato un identificativo di prossimità del dispositivo mobile (composto da 128 bit), denominato RPI (*Rolling Proximity Identifier*). Da ogni TEK possono essere generati 144 RPI a essa corrispondenti, mentre in presenza del solo RPI non è possibile risalire alla TEK da cui è stato generato.

Tali RPI vengono diffusi in modalità *broadcast* e sono ricevuti da altri dispositivi raggiungibili mediante interfaccia *bluetooth*, producendo di fatto, in caso di sufficiente prossimità, uno scambio reciproco di RPI tra i dispositivi su cui è installata l'app Immuni, registrandoli automaticamente nella loro memoria locale, unitamente ad altri dati accessori (metadati quali la data, la durata e la distanza del contatto). In tal modo, sul dispositivo di ogni utente sono memorizzate la lista delle proprie TEK (aggiornata quotidianamente) e la lista degli RPI dei dispositivi degli altri utenti con cui si è entrati in contatto. Le TEK e gli RPI sono automaticamente cancellati, dai dispositivi, trascorsi 14 giorni dalla loro memorizzazione.

C) *Raccolta delle TEK dal dispositivo di un utente accertato positivo al Covid-19*

In caso di esito positivo di un tampone, nell'ambito dell'indagine epidemiologica effettuata dall'operatore sanitario del Dipartimento di prevenzione della Azienda sanitaria locale competente, viene chiesto al paziente se abbia installato l'app Immuni. In tal caso, l'operatore chiederà allo stesso se voglia rendere disponibili le proprie TEK al fine di allertare

del rischio di contagio gli utenti con cui è entrato in contatto stretto nei giorni precedenti la diagnosi o la manifestazione dei sintomi. Qualora il paziente voglia procedere in tal senso, l'operatore sanitario richiede allo stesso di aprire l'app e di utilizzare la funzione di generazione del codice OTP (*One Time Password*), composto da 10 caratteri. Il paziente comunica tale codice OTP all'operatore sanitario e attende l'autorizzazione per effettuare il caricamento (c.d. *upload*) delle proprie TEK. L'operatore sanitario, utilizzando una specifica funzionalità resa disponibile sul Sistema TS, inserisce il codice OTP e la data di inizio dei sintomi forniti dal paziente, che vengono così trasmessi al *backend* di Immuni. Entro un limitato intervallo temporale (2 minuti e 30 secondi), il paziente dovrà completare la procedura di caricamento delle TEK generate sul proprio dispositivo negli ultimi 14 giorni, che sono trasmesse al *backend* di Immuni che, previa verifica dell'OTP, le elabora per individuare, sulla base della data di inizio dei sintomi, solo le TEK generate nei giorni in cui il paziente, sulla base della data di insorgenza dei sintomi dichiarata, deve essere considerato contagioso.

Il predetto meccanismo di autorizzazione è volto ad assicurare che siano caricate sul Sistema Immuni esclusivamente le TEK riferibili a utenti accertati positivi al Covid-19.

All'atto dell'*upload* delle TEK, l'app effettua anche il caricamento automatico sul *backend* di Immuni di alcune informazioni relative agli eventuali contatti stretti con soggetti positivi rilevati in precedenza (c.d. *analytics* di tipo *Epidemiological Information*, meglio descritti alla lett. A) del par. 1.2 del presente provvedimento), e della provincia di domicilio indicata dall'utente all'atto del primo utilizzo dell'app o successivamente modificata.

D) *Pubblicazione delle TEK degli utenti risultati positivi al Covid-19*

Le TEK degli utenti risultati positivi, acquisite con le modalità di cui sopra, sono pubblicate per la messa a disposizione dell'app immuni, affinché possano essere scaricate automaticamente e periodicamente dagli utenti dell'app per consentire alla stessa di rilevare la ricorrenza di un eventuale contatto mediante il confronto con gli RPI salvati all'interno di ciascun dispositivo mobile.

A tal fine, il *backend* di Immuni genera periodicamente, a un intervallo regolare di 30 minuti, un *file*, firmato digitalmente, contenente l'insieme delle TEK (c.d. TEK *Chunk*) dei nuovi soggetti risultati positivi. Tale *file* viene pubblicato e reso disponibile attraverso una *Content Delivery Network* (CDN), ossia un insieme di *server* distribuiti geograficamente che consente di garantire lo scaricamento (*download*) del *file* da parte di numerosi utenti, fornito da una società, designata, a sua volta, responsabile del trattamento da Sogei. Tali *file* vengono automaticamente cancellati trascorsi 14 giorni dalla sua generazione.

L'app installata sui singoli dispositivi degli utenti verifica periodicamente (ogni 4 ore circa, ma anche con frequenza maggiore qualora il dispositivo mobile sia connesso al proprio alimentatore elettrico) la presenza di aggiornamenti, memorizzando nel dispositivo gli eventuali nuovi *file* contenenti le TEK pubblicate.

E) *Raffronto con gli RPI salvati nei dispositivi degli utenti*

Una volta ricevute le TEK pubblicate dal sistema di *backend*, ciascun dispositivo su cui è installata l'app avvia il raffronto tra gli RPI ricavati dalle TEK scaricate e quelli, rilevati nei

14 giorni precedenti, memorizzati all'interno di ciascun dispositivo mobile, al fine di verificare la presenza di un contatto stretto con utenti accertati positivi al Covid-19 (*match*).

Tale raffronto viene effettuato a livello locale attraverso l'algoritmo messo a disposizione dal *Framework* A/G che sulla base di alcuni parametri quali la durata del contatto e la distanza tra i dispositivi su cui è installata l'app (rilevata mediante l'intensità del segnale *bluetooth*), calcola l'indice di rischio di contagio (*Total Risk Score*) per ogni eventuale contatto rilevato. Se tale indice di rischio supera una soglia predefinita, l'app mostra all'utente un messaggio di allerta sulla possibile esposizione al contagio (c.d. notifica di esposizione), per essere stato un contatto stretto di un soggetto accertato positivo al Covid-19 ("*Il giorno TOT sei stato vicino a un caso COVID-19 positivo*"). Il messaggio invita quindi l'utente ad adottare alcune regole di comportamento, nonché a contattare il proprio medico di medicina generale/pediatra di libera scelta, che a sua volta provvederà a contattare il Dipartimento di prevenzione della Azienda sanitaria locale territorialmente competente.

Successivamente all'operazione di raffronto con gli RPI memorizzati all'interno del dispositivo mobile, in presenza o meno di un contatto a rischio, l'app può trasmettere, in modo automatico e secondo un modello probabilistico, alcune informazioni al *backend* di Immuni che riguardano: la ricezione o meno di una notifica di esposizione al rischio, la data dell'eventuale ultimo contatto stretto con soggetto risultato positivo, la provincia di domicilio, nonché indicatori tecnici relativi al dispositivo dell'utente e all'utilizzo dell'app (c.d. *analytics* di tipo *Operational Info with/without Exposure*, meglio descritti alla lett. B) del par. 1.2 del presente provvedimento).

1.2. *La raccolta e l'utilizzo degli* analytics

Il Sistema di allerta Covid-19, oltre alle TEK degli utenti accertati positivi al Covid-19, raccoglie, attraverso l'app, le ulteriori informazioni di seguito descritte.

A) *Gli* analytics *di tipo* Epidemiological Info

Ogni qual volta un utente risultato positivo al Covid-19 decide, liberamente, al fine di "*avvisare altri utenti a rischio di contagio*", di effettuare il caricamento delle proprie TEK su sistema di *backend*, comunicando all'operatore sanitario la data di inizio dei sintomi, l'app trasmette automaticamente anche ulteriori informazioni c.d. *Epidemiological Info* al *backend* di Immuni. In tale circostanza, di per impostazione predefinita, vengono quindi raccolti sul Sistema di allerta Covid-19 anche i dati sotto specificati per "*consentire l'affinamento dell'algoritmo di calcolo del rischio derivante da un contatto e allertare solo le persone che sono effettivamente a rischio*", nonché per "*finalità di tutela della salute pubblica*" e "*di carattere epidemiologico*":

Le *Epidemiological Info* raccolte comprendono:

1) provincia di domicilio;
2) *Exposure Detection Summary*, ossia una serie di informazioni sintetiche relative a tutti gli eventuali contatti a rischio avvenuti negli ultimi 14 giorni (rilevati attraverso il raffronto delle TEK scaricate con gli RPI memorizzati all'interno del dispositivo), che comprende:
   a) numero di contatti a rischio rilevati;
   b) numero di giorni trascorsi dall'ultimo contatto a rischio;

c) durata aggregata dei contatti a rischio (misurata in multipli di 5 min. fino a un massimo di 30 min.), distinta per tre intervalli di intensità del segnale *bluetooth* (c.d. *attenuation)*;
d) indice di rischio più elevato tra quelli relativi ai contatti a rischio;

3) *Exposure Info*, ossia una serie di informazioni analitiche relative a ciascun eventuale contatto a rischio avvenuto negli ultimi 14 giorni (rilevato attraverso il raffronto delle TEK scaricate con gli RPI memorizzati all'interno del dispositivo), che comprende:
a) data in cui è avvenuto il contatto a rischio;
b) durata del contatto a rischio (misurata in multipli di 5 min fino a un massimo di 30 min);
c) intensità del segnale *bluetooth* durante il contatto a rischio (c.d. *attenuation*);
d) durata del contatto a rischio (misurata in multipli di 5 min fino a un massimo di 30 min), distinta per tre intervalli di intensità del segnale *bluetooth* (c.d. *attenuation)*;
e) rischio di contagiosità associato alla TEK relativa al contatto a rischio;
f) indice di rischio relativo al contatto a rischio.

La raccolta dei predetti dati (*Epidemiological Info*, TEK degli ultimi 14 giorni, *clock* del dispositivo e data di inizio dei sintomi, è subordinata al meccanismo di autorizzazione basato su un codice OTP descritto alla lett. C del par. 1.1 del presente provvedimento).

B) *Gli* analytics *di tipo* Operational Info

L'app trasmette, in maniera automatica e secondo un modello probabilistico, al *backend* di Immuni le c.d. *Operational Info without Exposure* e, se c'è stato un contatto a rischio le c.d. *Operational Info with Exposure*. In ogni caso, il numero di invii di analytics di tipo *Operational Info* che un singolo dispositivo può effettuare è limitato su base mensile.

Le *Operational Info* sono raccolte per "*capire statisticamente il livello di diffusione dell'app sul territorio e la correttezza del suo utilizzo*", nonché per "*monitorare su base statistica l'epidemia, allocare in modo più efficiente le risorse sanitarie e massimizzare quindi la prontezza e adeguatezza del supporto fornito agli utenti che risultano a rischio*".

Allo stato attuale, la trasmissione di tali *analytics* riguarda unicamente i dispositivi con sistema operativo iOS. Infatti, al fine di garantire la validità delle *Operational Info* e di imporre un limite mensile al loro invio da parte dei dispositivi mobili, evitando nel contempo l'eventuale inquinamento dei dati raccolti dal *backend*, il Sistema di allerta Covid-19 fa ricorso a tecniche di *device attestation* che consentono di verificare l'autenticità del dispositivo dal quale provengono i dati, allo stato possibili solo per dispositivi con sistema operativo iOS (API *DeviceCheck* di Apple) con le modalità di seguito descritte.

Le *Operational Info* comprendono:

1) *analytics token* (il cui significato è descritto nel par. 1.3, raccolto per una finalità meramente tecnica strumentale a garantire sicurezza e maggior affidabilità dei dati trattati nell'ambito del meccanismo di *device attestation* dei dispositivi iOS);
2) provincia di domicilio;
3) stato di attivazione dell'interfaccia *bluetooth*;
4) stato del permesso all'utilizzo del *Framework* A/G per la notifica di esposizione;

5) stato del permesso alla visualizzazione di notifiche locali generate dall'app;
6) sistema operativo del dispositivo mobile (iOS o Android);
7) avvenuta ricezione o meno di notifiche di esposizione al rischio;
8) data in cui è eventualmente avvenuta l'ultima esposizione al rischio (contatto stretto con un soggetto risultato positivo).

C) *La conservazione e l'utilizzo degli* analytics *da parte del Ministero*

In relazione alle modalità di conservazione e al successivo trattamento di entrambe le categorie di analytics per le finalità sopra descritte, viene rappresentato che "l*a fornitura dei dati da parte di Sogei sarà effettuata giornalmente, in forma anonima e aggregata via PEC, agli uffici competenti del Ministero della salute.*", senza fornire ulteriori elementi (es. tecniche di anonimizzazione applicate ai dati dopo la loro raccolta, tempi di conservazione).

D) Device attestation: *generazione e utilizzo dell'*analytics token

Al fine di consentire al *backend* di Immuni di verificare l'autenticità dei dispositivi dai quali provengono gli *analytics* di tipo *Operational Info*, per i soli dispositivi con sistema operativo iOS, vengono effettuate le seguenti operazioni:

- l'app Immuni richiede ad Apple ("*DeviceCheck* iOS API") l'attribuzione di un identificativo temporaneo del dispositivo, denominato *device token*, che consentirà al *backend* di Immuni di verificarne l'autenticità;
- successivamente, l'app Immuni genera, in modo casuale, un altro identificativo del dispositivo, denominato *analytics token*, salvandolo in locale e inviandolo al *backend* di Immuni unitamente al *device token* attribuito da Apple;
- alla ricezione di tali dati, il *backend* di Immuni verifica con Apple ("*DeviceCheck server* API") la validità del *device token* relativo al dispositivo dell'utente; in tale circostanza, il *backend* di Immuni si avvale anche di alcune funzionalità rese disponibili da Apple (c.d. "*DeviceCheck per-device bits*") che consentono di tenere traccia di quei dispositivi mobili che, avendo assunto un comportamento anomalo nella generazione dell'*analytics token*, non sono autorizzati a inviare *Operational Info*;
- in caso di riscontro positivo da parte del servizio di Apple, il *backend* di Immuni memorizza l'*analytics token* in un *database*, associandolo a un contatore di invii;
- ogni qual volta l'app Immuni deve inviare gli *analytics* di tipo *Operational Info*, assieme a tali dati viene trasmesso l'*analytics token* generato in precedenza;
- alla ricezione di tali *analytics*, il *backend* di Immuni controlla se l'*analytics token* esiste, se è stato generato e se non è già stato utilizzato per effettuare due invii; solo se tutte queste condizioni sono soddisfatte, le *Operational Info* vengono accettate e salvate nel *backend* di Immuni; in caso contrario, i dati vengono scartati.

L'*analytics token* cambia con cadenza mensile e viene inviato al *backend* di Immuni al massimo tre volte al mese (all'atto della generazione, dell'invio delle *Operational Info with Exposure* e dell'invio delle *Operational Info without Exposure*), in modo da limitare "*la capacità del server di reidentificare lo stesso dispositivo a cavallo di più chiamate al server*".

Su base mensile i dispositivi su cui è istallata l'app Immuni generano, in modo casuale, un identificativo denominato *analytics token* necessario a verificare la validità degli *analytics* di tipo *Operational Info* inviati al Sistema di allerta Covid-10.

OSSERVA

Il trattamento di dati personali effettuato nell'ambito del Sistema di allerta risulta legittimo e proporzionato in quanto siano rispettati i diritti e le libertà degli interessati e sia accompagnato anche da adeguate misure di prevenzione e diagnosi volte ad agevolare la presa in carico delle persone contagiate da parte del Sistema sanitario nazionale e la precoce individuazione di nuovi focolai di infezione. Ciò, assicurando, in particolare la trasparenza, la correttezza e la sicurezza in ogni fase del trattamento, in relazione ai rischi elevati che presenta per i diritti e le libertà degli interessati.

1. Base giuridica del trattamento, volontarietà e finalità perseguite

Come detto, la realizzazione dell'app Immuni si colloca nel contesto normativo stabilito dall'art. 6 del d.l. n. 28/2020 con il quale è stata istituita la piattaforma unica nazionale per la gestione Sistema di allerta Covid-19.

La predetta disposizione, fra l'altro, prevede alcuni requisiti fra loro strettamente connessi quali: 1.1) la volontarietà dell'istallazione dell'app; 1.2) il perseguimento di alcune specifiche finalità; 1.3) l'utilizzo di dati pseudonimizzati.

1.1) *Sulla volontarietà dell'utilizzo dell'app*

Quanto alla prima, occorre sottolineare che un'applicazione fondata sulla volontarietà degli utenti implica che la volontà si manifesti in tutte parti del suo funzionamento: il *download*, l'istallazione, la configurazione, l'attivazione della tecnologia Bluetooth, il caricamento delle TEK sul *backend* di Immuni in caso di risultato positivo del tampone, la raccolta delle diverse categorie di *analytics* nelle fasi in cui si articola il trattamento, la consultazione del medico di fiducia dopo aver ricevuto un messaggio di allerta sul rischio di essere entrato in contatto stretto con soggetti risultati positivi, la disinstallazione dell'applicazione, ecc. (cfr. punti 24 e 31 delle "*Linee guida 04/2020 sull'utilizzo dei dati di localizzazione e degli strumenti per il tracciamento dei contatti nel contesto dell'emergenza legata al COVID-19*" del Comitato europeo per la protezione dei dati del 21 aprile 2020).

Corollario della volontarietà è, come previsto anche dal legislatore, che le persone che non intendono o non possono utilizzare l'applicazione, intesa nella sua interezza o solamente in una sua fase, non possono subire alcun pregiudizio, e deve, in ogni caso, essere assicurato il rispetto del principio di parità di trattamento (art. 6, comma 3, d.l. n. 28/2020).

L'utilizzo volontario dell'app deve essere chiaramente specificato agli utenti, in aderenza al principio di trasparenza ed eventuali innovazioni nelle caratteristiche del trattamento devono essere riscontrate in corrispondenti modifiche dell'informativa stessa (artt. 5, par. 1, lett. a; 12; cons. nn. 39 e 60, del Regolamento).

1.2) *Sulle finalità dell'app*

La normativa di riferimento stabilisce che il Sistema di allerta Covid-19 debba perseguire esclusivamente la finalità, da un lato, di "*allertare le persone che siano entrate in contatto stretto con soggetti risultati positivi*" e, dall'altro, di "*tutelarne la salute attraverso le previste misure di prevenzione nell'ambito delle misure di sanità pubblica legata all'emergenza Covid*

19". È, inoltre, conferito al Ministero, in qualità di titolare del trattamento dei dati personali effettuato attraverso il predetto Sistema, il compito di porre in essere gli ulteriori adempimenti necessari alla gestione del sistema di allerta per l'adozione di correlate misure di sanità pubblica e di cura, in coordinamento con i soggetti previsti dalla legge, anche per il tramite del Sistema TS e nel rispetto delle relative competenze istituzionali in materia sanitaria connessa all'emergenza epidemiologica (art. 6, comma 1, d.l. n. 28/2020).

Le predette finalità possono essere perseguite attraverso il trattamento dei dati personali raccolti dall'app che, "*per impostazione predefinita, siano esclusivamente quelli necessari ad avvisare gli utenti dell'applicazione di rientrare tra i contatti stretti di altri utenti accertati positivi al COVID-19, individuati secondo criteri stabiliti dal Ministero della salute e specificati nell'ambito delle misure di cui al presente comma, nonché ad agevolare l'eventuale adozione di misure di assistenza sanitaria in favore degli stessi soggetti*" (art. 6, comma 2, lett. b, *ivi*).

A ciò si aggiunge che il funzionamento dell'app Immuni implica anche il trattamento di "*categorie particolari dati*, in quanto relativi alla salute degli utenti. Questi ultimi possono essere trattati ai sensi dell'art. 9, par. 1, lett. g, del Regolamento, nel rispetto delle ulteriori garanzie previste dall'art. 2-*sexies* del Codice, che prevede la specificazione dei "*tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato*".

Al riguardo, tale livello di dettaglio è riportato nella valutazione di impatto in esame, con la quale – ai sensi dell'art. 6, comma 2, del d.l. n. 28/2020 – il Ministero della Salute è stato chiamato ad adottare "*misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato ai rischi elevati per i diritti e le libertà degli interessati*". Tale documento contiene una descrizione generale dei dati trattati, delle operazioni eseguite, dei flussi di dati e delle specifiche finalità perseguite.

In particolare, il Sistema comporta il trattamento dei dati necessari, come previsto dal legislatore, da un lato, per il tracciamento dei contratti al fine di allertare le persone che siano entrate in contatto stretto con soggetti risultati positivi (es: TEK, RPI, la data di inizio dei sintomi per persone positive al tampone, la avvenuta ricezione della notifica di esposizione) e, dall'altro, per fini di sanità pubblica, contribuendo, nel contempo, a migliorare il funzionamento del Sistema di allerta Covid-19 (es: analytics Operational Info ed Epidemiological Info, descritti sopra, che comprendono, tra l'altro, la provincia di domicilio, la data in cui è avvenuto l'ultimo contatto a rischio, il grado di rischio di contagio, l'aver ricevuto un messaggio di allerta, lo stato di attivazione del bluetooth, il permesso per l'utilizzo del Framework A/G che rende possibile il tracciamento dei contatti, il permesso per le notifiche, il sistema operativo del dispositivo, il clock del dispositivo, gli analytics token, i device token).

1.3) Sull'utilizzo di dati pseudonimizzati

L'art. 6 comma 2, lett. c) del d.l. n. 28/2020 stabilisce che il trattamento effettuato per allertare i contatti sia basato sul trattamento di dati di prossimità dei dispositivi pseudonimizzati.

La pseudonimizzazione, ai sensi dell'art 25 del regolamento costituisce una misura di privacy by design, volta primariamente ad assicurare l'applicazione efficace dei principi

della protezione dei dati personali, integrando nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati. Si tratta dunque di un adempimento e non di una tecnica di anonimizzazione dei dati.

Lo scopo della tutela è rappresentato dalla definizione di pseudonimizzazione, introdotta dall'art 4 comma 1 del Regolamento come il risultato di un trattamento di dati personali che non ne consente l'attribuzione a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a specifiche misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.

Per dare compiuta applicazione al dettato normativo devono dunque essere chiaramente individuate le due componenti di un trattamento di pseudonimizzazione, il dato pseudonimizzato e l'informazione aggiuntiva, e deve inoltre essere garantita la separazione tra queste due componenti in assenza della quale sarebbe possibile l'identificazione di un interessato.

Nel contesto del contact tracing lo scopo della pseudonimizzazione, in tal modo realizzata, è di consentire la distribuzione delle chiavi TEK (vale a dire il risultato della pseudonimizzazione) ai partecipanti al sistema ma non delle chiavi di co-decodifica (vale a dire l'informazione aggiuntiva) venendo a mancare la quale sarebbe impedita in radice ai partecipanti la possibilità di risalire all'identità di qualsiasi altro partecipante.

A tal riguardo, l'applicazione di tecniche di cifratura asimmetriche a stato dell'arte (ad esempio, basate su algoritmi di *hash*), con una adeguata custodia delle chiavi da parte del soggetto centrale, che sarebbe l'unico in grado di consentire la re-identificazione per ragioni meramente funzionali all'operatività del sistema, si configurerebbe come una schema di pseudonimizzazione idoneo a realizzare il disaccoppiamento tra TEK e le loro chiavi di decodifica, consentendo così la corretta applicazione dell'art. 6 comma 2, lett. C) del d.l. n. 28/2020, nonchè, su tale base, la pubblicazione delle TEK dei soggetti risultati positivi.

2. Le caratteristiche dell'algoritmo di esposizione al contagio

In via preliminare si rappresenta che, nella valutazione d'impatto non sono ancora individuati puntualmente i criteri epidemiologici di rischio e i modelli probabilistici su cui si basa l'algoritmo, né i parametri di configurazione impiegati corredati dalle assunzioni effettuate, in conformità con quanto disposto dall'art. 6, comma 2, lett. B), del d.l. n. 28/2020, il quale prevede che l'individuazione del contatto stretto avvenga "*secondo criteri stabiliti dal Ministero della salute e specificati nell'ambito delle misure*" tecniche e organizzative contenute nella valutazione d'impatto.

Al riguardo, si sottolinea l'importanza che sia assicurata la massima trasparenza pubblica di tali criteri, anche al fine di garantire un idoneo scrutinio da parte della comunità scientifica.

Sotto questo profilo, si rappresenta che la valutazione del rischio di esposizione al contagio effettuata dall'app è calcolata mediante un algoritmo, solo genericamente rappresentato nella valutazione di impatto, che tiene conto della durata del contatto e della distanza dei dispositivi mobili desunta dall'intensità del segnale *bluetooth* ricevuto dal

dispositivo (c.d. *attenuation*). Il modello di rischio può evolvere con il tempo, in funzione delle informazioni sul virus che risulteranno disponibili.

Occorre considerare che la valutazione della distanza fra dispositivi è intrinsecamente suscettibile di errori in quanto l'intensità del segnale *bluetooth* dipende da fattori diversi come l'orientamento reciproco di due dispositivi o la presenza di ostacoli fra essi (compresa la presenza di corpi umani), potendo così rilevare "falsi positivi" e "falsi negativi".

Peraltro, la mancata conoscenza del contesto in cui è avvenuto il contatto stretto con un caso accertato Covid-19 (dato certamente rilevante, invece, ai fini epidemiologici, anche in ragione dell'eventuale utilizzo di sistemi di protezione) è suscettibile di creare potenzialmente numerosi "falsi positivi".

È importante infatti sottolineare che l'individuazione dei contatti a rischio è effettuata in modo probabilistico, al fine di allertare gli utenti di un possibile rischio di contagio; per cui deve essere chiaro che in nessun caso la ricezione di un messaggio di allerta proveniente dall'app significa automaticamente che l'utente è stato sicuramente contagiato.

Quanto detto è rilevante anche considerando la fase di sperimentazione e la successiva fase iniziale di utilizzo dell'app in tutto il territorio nazionale, anche per ottenere (e mantenere) la fiducia degli utenti circa l'esattezza e la precisione dell'app nel generare messaggi di allerta solo nei confronti degli utenti che abbiano avuto un reale rischio di aver contratto il virus. In caso contrario, infatti, nel caso in cui ove i falsi contatti stretti o non effettivamente ad alto rischio di contagio fossero numerosi, si rischierebbe invece di compromettere la fiducia degli utenti nell'affidabilità della app con conseguente interruzione del suo utilizzo.

******

Su tali basi, si raccomanda, pertanto, che:

- l'algoritmo, basato su criteri epidemiologici di rischio e modelli probabilistici (specificando i parametri di configurazione impiegati e le assunzioni effettuate), sia puntualmente indicato e costantemente aggiornato nella valutazione d'impatto, in osservanza del principio di responsabilizzazione, come del resto previsto dall'art. 6, comma 2, lett. b), del d.l. n. 28/2020, rendendolo disponibile allo scrutinio da parte della comunità scientifica;
- gli utenti siano adeguatamente informati in ordine alla possibilità che l'app generi notifiche di esposizione che non sempre riflettono un'effettiva condizione di rischio (stante la possibilità, ad esempio, che alcuni soggetti entrino in contatto con persone positive al Covid-19 in ragione della propria attività lavorativa, ma adottando dispositivi di protezione individuale o altri accorgimenti), e fornisca agli utenti informazioni semplici e chiare sul funzionamento dell'algoritmo (anche attraverso una c.d. infografica);
- gli utenti dell'app possano temporaneamente disattivare la stessa attraverso una funzione facilmente accessibile nella schermata principale e che di tale funzione di disattivazione temporanea siano informati gli utenti in modo chiaro attraverso le infografiche visualizzate all'atto dell'installazione dell'app.

3. Analytics

Per raggiungere le finalità di "*allertare le persone che siano entrate in contatto stretto con soggetti risultati positivi*" e di "*tutelarne la salute attraverso le previste misure di prevenzione nell'ambito delle misure di sanità pubblica legata all'emergenza Covid 19*", il Ministero della salute ha ritenuto necessario prevedere che il Sistema Immuni raccolga attraverso l'app le diverse tipologie di *analytics* sopra descritte. Ciò, per consentire, in primo luogo, di predisporre le adeguate misure di presa in carico, da parte del Servizio sanitario nazionale, dei soggetti risultati a rischio di contagio - individuando tempestivamente nuovi focolai di infezione e monitorando il grado di adesione all'utilizzo dell'app da parte degli utenti - e, dall'altro, di permettere, attraverso l'analisi di dati epidemiologici, un costante miglioramento della capacità dell'algoritmo di individuare i contatti stretti tra gli utenti, assicurando al contempo il complessivo funzionamento del Sistema di allerta Covid-19 attraverso una migliore calibrazione delle configurazioni dell'app.

Al riguardo, si ritiene opportuno che, come già rappresentato, venga assicurata la massima trasparenza nei confronti degli utenti, garantendo la volontarietà del conferimento delle informazioni da parte degli utenti verso il backend di Immuni. Le informazioni che il Ministero intende acquisire sono, infatti, archiviate sul dispositivo dell'utente cui deve essere garantita la massima consapevolezza delle operazioni eseguite, favorendo, in tal modo, una fiduciosa e ampia adesione al Sistema di allerta Covid-19 (cfr. punto 28 delle Linee guida n. 04/2020 cit. del Comitato europeo per la protezione dei dati).

Occorre, infatti, rappresentare che tali informazioni non possono essere considerate dati anonimi (queste sono, infatti, acquisite dal Sistema di allerta Covid-19 in forma individuale dai singoli dispositivi) e consentono, in diversi contesti, concrete possibilità di re-identificazione degli interessati, soprattutto se associate ad altre informazioni ovvero in caso di morbilità non elevata o di ambiti territoriali con bassa densità di popolazione.

Al riguardo, si evidenzia che nella valutazione d'impatto non sono adeguatamente precisate le modalità con cui il Ministero della salute intende trattare e conservare le diverse tipologie di *analytics* raccolti, le tecniche di anonimizzazione eventualmente adottate, i tempi di cancellazione, nonché le specifiche misure di sicurezza poste in essere anche in relazione ai prospettati flussi di dati via PEC tra Sogei e il medesimo Ministero.

Infine, con riferimento al fatto che le *Operational Info* vengono attualmente raccolte solo da dispostivi iOS, si rappresenta che il Ministero ha ritenuto che i dati acquisiti in tal modo siano sufficienti per ottenere elaborazioni rappresentative, essendo conosciuta la distribuzione di dispositivi iOS e Android nelle diverse province italiane, precisando, altresì, che è in fase di sviluppo un meccanismo di *device attestation* anche per dispositivi Android. In particolare, la necessità di coinvolgere Apple e, successivamente, Google nel predetto meccanismo deriverebbe da esigenze di natura meramente tecnica, strumentale a garantire la sicurezza e una maggiore affidabilità dei dati raccolti.

È opportuno, a tal proposito, osservare come il ricorso iniziale agli *analytics* prodotti dai soli dispositivi iOS introduca una possibile distorsione (*bias*) nel campione su cui saranno calcolati gli indicatori di efficacia nell'uso del sistema e a partire dai quali sarà eventualmente effettuata la calibrazione del funzionamento dell'app. Ciò anche in ragione delle

caratteristiche socio-demografiche proprie degli utilizzatori di dispositivi iOS che possono essere significativamente diverse da quelle degli utilizzatori dei dispositivi Android.

Si rileva peraltro che la comunicazione dei dati, diversi da quelli appartenenti a categorie particolari, nei confronti di Apple può trovare legittimazione nell'art. 17-*bis* del d.l. 9 marzo 2020, n. 14, che disciplina il trattamento dei dati personali nel contesto emergenziale, purché gli utenti siano adeguatamente informati del ruolo svolto da Apple in tale circostanza.

******

In relazione a quanto sopra rappresentato, si ritiene necessario che gli *analytics* siano accuratamente protetti nel *backend* di Immuni, evitando ogni forma di riassociazione degli stessi a interessati identificabili e assicurando l'adozione di adeguate misure di sicurezza e tecniche di anonimizzazione, da individuarsi in ragione delle specifiche finalità in concreto perseguite, nel rispetto dei principi di *privacy by design* e *by default* (art. 25 del Regolamento).

Con riferimento al prospettato meccanismo di *device attestation* messo a disposizione da Apple, si invita a ponderare la possibilità di introdurre analoghi strumenti che non comportino il coinvolgimento di soggetti terzi nel trattamento. Laddove, invece, ciò, nel rispetto del principio di *accountability*, fosse ritenuto indispensabile, si raccomanda di rappresentare chiaramente agli utenti tale circostanza, specificando che saranno comunicati ad Apple esclusivamente i dati tecnici necessari a garantire la sicurezza e una maggior affidabilità dei dati raccolti, ferma restando la necessità di esaminare la soluzione di *device attestation* che verrà individuata per i dispositivi Android.

4. Trasparenza del trattamento e diritti degli interessati

4.1. Principio di trasparenza

In virtù del principio di trasparenza, il titolare deve informare l'interessato dell'esistenza del trattamento effettuato nell'ambito del Sistema di allerta Covid-19 e delle sue finalità, fornendogli le informazioni necessarie ad assicurare un trattamento corretto e trasparente, pur in considerazione le circostanze emergenziali in cui è effettuato e il contesto specifico in cui i dati personali sono trattati (artt. 5, par. 1, lett. a), 13 e 14 del Regolamento e considerando n. 60).

Le informazioni devono essere rese disponibili all'interessato prima della raccolta dei dati, anche con una modalità progressiva, fornendo in primo luogo quelle relative alle principali caratteristiche del trattamento. Al riguardo, il legislatore ha previsto che gli utenti ricevano, prima dell'attivazione dell'applicazione, informazioni chiare e trasparenti, al fine di raggiungere una piena consapevolezza, in particolare, sulle finalità e sulle operazioni di trattamento, sulle tecniche di pseudonimizzazione utilizzate per proteggere la sua identità e sui tempi di conservazione dei dati (art. 6, comma 2, lett. a), d.l. n. 28/2020). Particolare attenzione deve essere poi prestata alla volontarietà dell'uso dell'app, alla tipologia dei dati trattati e ai soggetti coinvolti nel trattamento.

Oltre a quanto già indicato nei precedenti paragrafi in relazione al rispetto del principio di trasparenza, al fine di facilitare la comprensione degli elementi informativi previsti dal Regolamento, si conviene che, come rappresentato nella valutazione d'impatto, gli stessi possano essere forniti in combinazione con icone standardizzate – leggibili da

dispositivo automatico – per dare, in modo facilmente visibile, intelligibile e chiaramente leggibile, un quadro d'insieme del trattamento previsto (cfr. considerando n. 61 al Regolamento).

Il linguaggio con cui devono essere rese le informazioni previste dal Regolamento deve essere formulato con modalità tali da essere comprensibile al maggior numero possibile di persone, in quanto una parte significativa della popolazione sarà probabilmente interessata dall'app.

Si esorta inoltre anche a individuare adeguate modalità di fruizione delle predette informazioni anche da parte delle persone con disabilità.

******

Ciò premesso, oltre all'esigenza rappresentata nel paragrafo 3 relativa alla trasparenza nella raccolta e nell'elaborazione degli *analytics*, in relazione al modello di informativa trasmesso a questa Autorità successivamente alla ricezione della valutazione d'impatto, si raccomanda di descrivere – nella parte relativa alla "Trasmissione/flusso dei dati" – le operazioni effettuate con riferimento ai dati *analytics* di tipo *Epidemiological Info*, nonché di specificare con maggiore chiarezza che i dati personali raccolti "*Per i soli utenti esposti al rischio di contagio*" e "*Per i soli utenti risultati positivi al SARS-CoV-2*" si aggiungono a quelli acquisiti per "*Tutti gli utenti dell'app*" (punti 5 e 4 del modello di "Informativa resa ai sensi degli articoli 13-14 del Regolamento (UE) 2016/679 ("General Data Protection Regulation – GDPR" in atti).

Con specifico riferimento all'utilizzo dell'app anche da parti di minori ultra quattordicenni, si raccomanda di prestare particolare attenzione alle informazioni da fornire e al contenuto dei messaggi di avvenuta esposizione a rischio di contagio.

Per quanto riguarda la fase di sperimentazione del Sistema di allerta Covid-19 indicata nella valutazione di impatto (par. 3), si raccomanda di informare gli utenti, tempestivamente e con modalità efficaci, che -in tale fase- sebbene possano installare l'app, l'avviso di esposizione al rischio di contagio potrà pervenire soltanto se il contatto è avvenuto con soggetti risultati positivi al Covid-19 assistiti dalle Regioni o Province autonome deputate alla sperimentazione.

4.2. Diritti dell'interessato

Il Regolamento, nel riconoscere all'interessato specifici diritti rispetto al trattamento dei suoi dati personali, individua anche alcuni ambiti in cui l'esercizio degli stessi può essere limitato (cfr. considerando nn. 63 e 68 e artt. 15 e ss. del Regolamento).

In primo luogo, si evidenzia che, per le caratteristiche del trattamento effettuato attraverso il Sistema di allerta Covid-19 e le tecniche di pseudonimizzazione utilizzate, come indicato nella valutazione d'impatto, il titolare potrebbe non essere in grado di identificare l'interessato in funzione dell'esercizio da parte dello stesso dei diritti riconosciuti dal Regolamento. Di tale circostanza il titolare deve compiutamente informare l'interessato (art. 11, par. 2, del Regolamento).

Ciò premesso, con specifico riferimento alle valutazioni effettuate dal Ministero in merito all'esercizio dei diritti da parte degli interessati e a quanto indicato nel modello di informativa trasmesso a questa Autorità, si evidenzia che:

- i diritti di accesso (art. 15 del Regolamento), rettifica (art. 16 del Regolamento), limitazione del trattamento (art. 18 del Regolamento) e portabilità dei dati (art. 20 del Regolamento) non sono esercitabili da parte dell'interessato con riferimento al trattamento dei dati personali effettuati attraverso il Sistema di allerta Covid-19 in considerazione delle caratteristiche del trattamento;
- il diritto di opposizione (art. 21 del Regolamento), analogamente a quanto indicato per il diritto alla cancellazione, può essere esercitato dall'interessato. Come correttamente rappresentato nella valutazione di impatto e nell'informativa, il diritto di opposizione si concretizza nella possibilità per l'interessato di disinstallare l'app. Al riguardo, si rappresenta l'opportunità che l'interessato sia edotto della circostanza che le chiavi saranno via via cancellate, al termine del quattordicesimo giorno di vita, anche sull'infrastruttura centrale.

******

Il diritto di cancellazione è invece esercitabile direttamente tramite l'app per tutte le chiavi temporanee (TEK) e gli identificativi di prossimità (RPI) mediante una funzione appositamente messa a disposizione dal *Framework* A/G volta a interrompere l'utilizzo dell'app in qualsiasi momento. L'interessato dovrebbe essere reso edotto della modalità di esercizio di tale diritto indicata nella valutazione di impatto e delle relative conseguenze.

Inoltre, si rappresenta l'opportunità che la funzionalità necessaria ad adattare l'utilizzo dell'app in contesti in cui sarebbero prodotti falsi positivi, sopra descritta, possa utilmente essere impiegata per garantire l'esercizio del diritto di opposizione qualora l'utente su base temporanea, ne ravvisi l'esigenza, evitando di ricorrere alla soluzione più radicale della disinstallazione dell'app.

5. Temporaneità della misura e tempi di cancellazione dei dati

Il trattamento dei dati personali deve essere conforme ai principi di minimizzazione dei dati e di limitazione della conservazione, in base ai quali – rispettivamente – i dati personali devono essere "*adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati*", nonché "*conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati*" (art. 5, par. 1, lett. c) ed e), del Regolamento).

Al riguardo l'art. 6, comma 6, del d.l. n. 28/2020 prevede che l'utilizzo dell'app e della piattaforma, nonché ogni trattamento di dati personali effettuato tramite di essi devono essere interrotti alla data di cessazione dello stato di emergenza disposto con delibera del Consiglio dei ministri del 31 gennaio 2020, e comunque non oltre il 31 dicembre 2020. Entro tale data tutti i dati personali trattati devono essere cancellati o resi definitivamente anonimi.

È inoltre previsto che "*i dati relativi ai contatti stretti siano conservati, anche nei dispositivi mobili degli utenti, per il periodo strettamente necessario al trattamento, la cui durata è stabilita dal Ministero della salute e specificata nell'ambito delle misure di cui al presente comma; i dati sono*

cancellati in modo automatico alla scadenza del termine" (art. 6, comma 2, lett. e), del d.l. n. 28/2020)

Nella valutazione d'impatto il Ministero ha puntualmente individuato i tempi di conservazione dei dati in relazione alle specifiche finalità, prevedendo la cancellazione delle singole tipologie dei dati personali trattati una volta esaurita la finalità per i quali sono stati raccolti e comunque non oltre il 31/12/2020.

In proposito, al fine di valutare la proporzionalità del trattamento effettuato, è rilevante, fra l'altro, che:

- le TEK e gli RPI memorizzati sui dispositivi mobili degli utenti siano cancellati automaticamente dopo 14 giorni;
- le TEK dei soggetti risultati positivi Covid-19 che hanno effettuato l'*upload* sul *backend* di Immuni siano analogamente cancellate dopo 14 giorni.

Restano in ogni caso ferme le osservazioni formulate in ordine ai tempi di conservazione degli *Analytics* di cui al par. 3 dell'indirizzo IP di cui al par. 7 al cui contenuto si rinvia integralmente.

6. Soggetti coinvolti nel trattamento

L'art. 6, commi 1 e 5, del d.l. n. 28/2020 prevede quali sono i soggetti istituzionali coinvolti nel trattamento dei dati personali.

Il titolare del trattamento è il Ministero della salute che si avvale dei soggetti indicati nelle predette disposizioni, fra cui Sogei S.p.a. e il Ministero dell'economia e delle finanze, limitatamente all'utilizzo del Sistema TS, che operano in qualità di responsabili del trattamento (art. 28 del Regolamento).

In tale quadro, nella valutazione d'impatto è inoltre indicato il coinvolgimento di fornitori di servizi di *Content Delivery Network* (CDN), designati sub-responsabili da parte Sogei, a seguito di specifica autorizzazione del Ministero della Salute ai sensi dell'art. 28 del Regolamento. Ciò, al fine di garantire – come riportato nella predetta valutazione d'impatto – la disponibilità e resilienza del sistema, l'esposizione delle chiavi temporanee relative agli utenti risultati positivi al tampone Covid-19.

Nella valutazione d'impatto non è invece sufficientemente chiarito il ruolo di altri soggetti *ivi* nominati o che potrebbero essere coinvolti nel Sistema Immuni, quali la società che ha sviluppato l'applicazione (Bending Spoons S.p.a.), o le società Apple e Google. Relativamente a queste ultime, l'utilizzo del *Framework* A/G attribuisce loro un mero ruolo di fornitori di tecnologia (*technology provider*) senza implicare di per sé alcun trattamento di dati personali

Tale aspetto andrebbe precisato, in ossequio ai principi di trasparenza e responsabilizzazione.

7. Sicurezza del trattamento

Ai diversi pregi del modello decentralizzato su cui si basa il Sistema Immuni, si affiancano alcune vulnerabilità di cui occorre essere consapevoli anche al fine di adottare le opportune misure di mitigazione dei rischi di sicurezza del Sistema, relativi anche alla possibile re-identificazione degli utenti con riferimento sia a coloro che ricevono il messaggio di allerta che a coloro che sono risultati positivi al Covid-19.

7.1. Sicurezza del dispositivo e rischi di re-identificazione

La riservatezza dei dati relativi ai soggetti risultati positivi al Covid-19 è affidata in parte alle misure tecniche e organizzative che devono essere individuate dal titolare del trattamento ma, in parte, anche alla capacità di evitare le occasioni in cui gli RPI di un utente (identificativi di prossimità, pseudonimi di breve periodo), inviati in *broadcast* con tecnologia *bluetooth*, possano essere rilevati da terzi, anche in abbinamento ad altre informazioni identificative, per essere, successivamente, raffrontati con le TEK dei soggetti risultati positivi, pubblicate dal Sistema di allerta Covid-19.

L'utente deve essere adeguatamente avvisato della particolare cura da riservare alla sicurezza del proprio dispositivo mobile, per prevenire l'azione di *malware* anche in forma di app apparentemente innocue ma che potrebbero avere un comportamento malizioso al fine di acquisire informazioni utili a ricostruire le relazioni tra gli utenti o le catene di contagio, ovvero individuare i soggetti esposti al rischio di contagio o quelli risultati positivi al Covid-19.

Occorre inoltre considerare che, all'esterno del dispositivo mobile possono essere attivati degli apparati di scansione (*sniffer*) in grado di intercettare la trasmissione *broadcast* degli RPI per usi impropri o, comunque, non autorizzati, determinando conseguenze pregiudizievoli in capo agli interessati.

Accanto ai predetti scenari, si aggiungono i rischi di re-identificazione inferenziale dei soggetti risultati positivi al Covid-19, con la compromissione della riservatezza delle informazioni, sia da parte di soggetti coinvolti nel trattamento, anche attraverso la disponibilità di analytics, sia da parte di altri utenti con tentativi di ricostruire contatti senza che siano necessari sofisticati strumenti tecnologici.

Al riguardo, si rappresenta che la pubblicazione delle TEK relative ai soggetti risultati positivi al Covid-19, comportando la diffusione degli pseudonimi dei loro dispositivi, li espone a una particolare tecnica di attacco denominata "paparazzi attack", che si realizza quando sia possibile acquisire agevolmente lo pseudonimo di un soggetto la cui identità sia nota, per esempio in prossimità del suo luogo di dimora oppure in ogni altro luogo in cui alla trasmissione via *bluetooth* dello pseudonimo siano associabili informazioni aggiuntive, come avviene in esercizi commerciali all'atto del pagamento con carta di credito, al passaggio attraverso varchi di imbarco controllati negli aeroporti, oppure nei luoghi di lavoro con i sistemi di rilevamento delle presenze.

Si tratta di contesti in cui potrebbero essere acquisiti gli RPI generati dal dispositivo di un utente ignaro associandovi altre informazioni identificative e consentendo la ricerca degli RPI così acquisiti tra quelli ottenibili dalla pubblicazione delle chiavi TEK dei soggetti

positivi, con un effetto finale di re-identificazione associato a una caratterizzazione dello stato di salute.

In particolare, nel caso dell'app Immuni, la pubblicazione del codice del programma come *open source* e la pubblicità data agli algoritmi crittografici adoperati nel *Framework* A/G potrebbero consentire a chiunque conosca, avendole scaricate, le TEK dei soggetti risultati positivi, di ricavare da ciascuna di esse i 144 RPI da raffrontare con la base dati di RPI "etichettati".

7.2. Le misure adottate nell'ambito del Sistema di allerta Covid-19

Con riferimento alla sicurezza complessiva del trattamento, si rappresenta che nella valutazione d'impatto sono descritte accuratamente le misure tecniche e organizzative adottate dal Ministero della salute nell'ambito del Sistema di allerta Covid-19, nonché quelle condivise dal Ministero dell'economia e delle finanze in relazione alle funzionalità appositamente introdotte nel Sistema TS, di seguito sinteticamente descritte:

- le TEK, gli RPI e gli altri dati presenti sul dispositivo dell'utente sono memorizzati in aree crittograficamente protette, in modo da renderli illeggibili a soggetti non autorizzati;
- il colloquio tra l'app e i servizi del *backend* di Immuni avviene mediante canali di comunicazione sicuri basati sul protocollo HTTPS (*Hypertext Transfer Protocol Secure*) e sull'utilizzo del meccanismo di *certificate pinning*;
- la generazione di traffico *dummy* (dati fittizi), in modo automatico e secondo un modello probabilistico, consente di limitare, in modo efficace, la possibilità di inferire – attraverso l'analisi del traffico crittografato tra l'app e il *backend* di Immuni all'atto dell'*upload* delle TEK o della trasmissione delle *Operational Info* – informazioni relative a particolari categorie di utenti (soggetti risultati positivi o esposti al rischio di contagio);
- i *file* contenenti i *TEK Chunck* sono firmati digitalmente, in modo da consentire all'app di verificarne l'integrità e l'autenticità;
- la pubblicazione del codice sorgente dell'app e delle principali componenti del *backend* di Immuni che consente lo scrutinio da parte della comunità di sviluppatori;
- il tracciamento degli accessi compiuti ai sistemi e alle basi dati dagli amministratori di sistema, con un congruo periodo di conservazione dei *log*;
- l'utilizzo di apparati di sicurezza perimetrale per bloccare attacchi volti a sfruttare vulnerabilità note, associate sia al *software* di base che al codice sviluppato per il Sistema Immuni;
- l'utilizzo di un codice OTP, con una validità temporale limitata (2 minuti e 30 secondi), per autorizzare – nel corso dell'indagine epidemiologica condotta da un operatore sanitario del Dipartimento di prevenzione della Azienda sanitaria locale competente – l'operazione di *upload* delle TEK di un soggetto risultato positivo;
- l'adozione di procedure di autenticazione informatica degli operatori sanitari per l'accesso al servizio di autenticazione OTP, reso disponibile sul Sistema TS;

- il tracciamento degli accessi e delle operazioni compiute sul Sistema TS dai predetti operatori sanitari e dagli amministratori di sistema, con un congruo periodo di conservazione dei *log*.

7.3. Ulteriori misure suggerite

In relazione ai rischi elevati presentati dal trattamento, individuati anche nella valutazione d'impatto, si ravvisa la opportunità di apportare ulteriori miglioramenti alla sicurezza complessiva intervenendo sui seguenti aspetti.

A) *Conservazione degli indirizzi IP dei dispositivi mobili*

Dall'esame della documentazione, non è chiaro se vengano conservati gli indirizzi IP dei dispositivi mobili che interagiscono con il *backend*, sia direttamente (all'atto *dell'upload* delle TEK e delle *Epidemiological Info*) sia mediante l'intervento della CDN (al momento per il *download* delle TEK e la trasmissione delle *Operational Info*).

In particolare, nella valutazione d'impatto si afferma che "*l'indirizzo IP del dispositivo che invia i dati viene trasformato in un indirizzo fittizio attraverso tecniche di Network Address Translation (NAT) dall'infrastruttura di backend all'atto dell'upload dei dati e non viene memorizzato né nel database né nei file di log. L'indirizzo IP viene esclusivamente tracciato temporaneamente sui sistemi perimetrali di accesso degli upload*", mentre nel suo allegato n. 15 è riportato che "*non è prevista la memorizzazione degli indirizzi IP dei client da parte del server di backend centrale. L'indirizzo IP viene conservato dall'infrastruttura perimetrale ai soli fini di garantirne la sicurezza informatica*".

******

Occorre quindi commisurare i tempi di conservazione nella misura strettamente necessaria al rilevamento di anomalie e di attacchi. Ciò, in quanto gli indirizzi IP sono dati personali e possono costituire quell'informazione aggiuntiva che, collegata ai dati raccolti, in determinate circostanze consente l'identificazione degli utenti.

B) *Tracciamento delle operazioni compiute dagli amministratori di sistema*

Dall'esame della documentazione emerge che il tracciamento degli accessi dagli amministratori di sistema è limitato alle operazioni di login e logoff, non consentendo così un efficace controllo, a posteriori, delle operazioni eseguite sui dati.

******

Occorre, pertanto, introdurre misure volte ad assicurare il tracciamento delle operazioni compiute dagli amministratori di sistema sui sistemi operativi, sulla rete e sulle basi dati.

C) *Caricamento erroneo di Diagnosis Keys (TEK) non riferite a soggetti positivi a seguito di errori materiali o diagnostici*

Con riferimento alla valutazione dei rischi individuati nella valutazione d'impatto, occorre considerare l'ulteriore scenario di compromissione dell'integrità dei dati derivante dall'ipotesi in cui, una volta pubblicate le TEK di un soggetto ritenuto positivo, per varie

ragioni (ad esempio, casi di omonimia, scambio di referti, errori materiali), si renda necessario un intervento di rettifica dei dati inseriti al fine di ripristinarne l'accuratezza.

Andrebbero dunque individuate, nel rispetto del principio di responsabilizzazione, le misure tecniche e organizzative adeguate a tal fine.

8. Sperimentazione

Nella valutazione d'impatto il Ministero della salute ha rappresentato l'esigenza, condivisa con le Regioni, di una preliminare fase di sperimentazione del processo di *contact tracing* digitale in un numero limitato di Regioni o Province autonome.

Ciò al fine di verificare il corretto funzionamento dal punto di vista tecnico e dell'impatto sui servizi territoriali dell'app, in considerazione del possibile ulteriore carico di lavoro (*contact tracing*, individuazione, isolamento/quarantena, diagnostica, sorveglianza) derivante dalla diffusione del nuovo strumento digitale, che dovrebbe presumibilmente rivelare anche contatti non rilevabili con le modalità tradizionali di *contact tracing*.

Al riguardo, è stata ritenuta congrua la durata di almeno una settimana della fase di sperimentazione, da svolgersi nelle Regioni o Province autonome che saranno individuate dai decisori politici nazionali e regionali.

In tale quadro, poiché l'app non può essere rilasciata soltanto in zone limitate del Paese, per realizzare la sperimentazione, sarà inizialmente consentito l'utilizzo codice di sblocco OTP esclusivamente nelle Regioni o Province autonome scelte per la sperimentazione. Di conseguenza, in tale fase, tutti i cittadini pur potendo scaricare l'app dagli store ufficiali, saranno preventivamente avvertiti che l'avviso di esposizione al rischio di contagio potrà pervenire soltanto se il contatto è avvenuto con soggetti risultati positivi al Covid-19 assistiti dalle Regioni o Province autonome in cui è stata avviata la sperimentazione. Nella valutazione d'impatto è comunque indicato che di tale circostanza sarà fornito apposito avviso nell'app store.

In relazione alla fase iniziale di utilizzo della app, nella valutazione d'impatto è richiamato l'art. 35, par. 9, del Regolamento, ai sensi del quale il titolare del trattamento raccoglie, se del caso, le opinioni sul trattamento previsto da parte degli interessati che saranno coinvolti nel trattamento stesso, o dei loro rappresentanti, fatta salva la tutela degli interessi commerciali o pubblici o la sicurezza dei trattamenti.

Al riguardo, il Ministero ha evidenziato che è stato privilegiato "*il pieno rispetto degli obblighi di trasparenza attraverso, tra le altre cose, il carattere libero e aperto del software utilizzando lo strumento della piattaforma GitHub per la condivisione e la cooperazione sulle questioni tecniche legate all'applicazione, lasciando ad un momento successivo, e segnatamente al termine della fase di sperimentazione, la raccolta di opinioni sull'uso vero e proprio dell'applicazione da parte dei diretti interessati*", che dovrebbe consentire "*un primo momento di confronto con le opinioni esperte sulla parte più strettamente tecnica dell'applicazione e sulle misure di sicurezza volta a rafforzare quel vincolo di fiducia che è un elemento fondamentale per il buon esito del progetto*".

In relazione, invece alla raccolta delle opinioni degli utenti è stato deciso di "r*imandare alla fase di sperimentazione la raccolta di dette opinioni*", considerando, fra l'altro, l'ampio dibattito su tutti gli organi di stampa sull'app Immuni e il particolare "*contesto emergenziale*

in cui il trattamento si inserisce e quindi con la necessità di adottare misure di contenimento del Covid-19 nel più breve tempo possibile".

Si auspica che le opinioni degli utenti espresse nella fase di sperimentazione, raccolte con le modalità sopra descritte, siano tenute in debita considerazione per il previsto aggiornamento della valutazione d'impatto e per il miglioramento del Sistema Immuni.

RITENUTO

In ragione dell'esigenza di avviare il Sistema di allerta Covid-19, il trattamento di dati personali effettuato nell'ambito di tale Sistema può essere considerato proporzionato, essendo state previste misure volte a garantire in misura sufficiente il rispetto dei diritti e le libertà degli interessati attenuandone i rischi derivanti dal trattamento.

Nel presente provvedimento sono contenute alcune prescrizioni volte a rafforzare le garanzie nei confronti dei soggetti i cui dati siano trattati nell'ambito del sistema di allerta Covid 19. Le misure prescritte potranno essere adottate nel corso della sperimentazione del Sistema, così da garantire che in fase attuativa ogni residua criticità sia risolta.

Si rammenta, infine, che la raccolta dei dati personali trattati attraverso tale sistema, da parte di soggetti non autorizzati, determina un trattamento di dati personali illecito (anche sotto il profilo penale, ove ne sussistano gli ulteriori requisiti di fattispecie). Analogamente, i dati raccolti attraverso il predetto sistema non possono essere trattati per finalità non previste dal richiamato art. 6 del d.l. n. 28/2020 ed in particolare per assumere decisioni nei confronti dell'interessato suscettibili di arrecargli pregiudizio.

TUTTO CIÒ PREMESSO, IL GARANTE

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

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

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

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

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

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

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

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

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

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

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

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

12) adottare misure tecniche e organizzative per mitigare i rischi derivanti dall'upload di TEK non riferite a soggetti positivi a seguito di eventuali errori materiali o diagnostici (§ 7.3);

b) ai sensi e per gli effetti dell'art. 157 del Codice, richiede al Ministero della salute di comunicare quali iniziative siano state intraprese al fine di dare attuazione a quanto previsto nel presente provvedimento, entro il termine di 30 giorni dalla data della ricezione del presente provvedimento.

Ai sensi dell'art. 78 del Regolamento, nonché degli artt. 152 del Codice e 10 del d.lgs. 1° settembre 2011, n. 150, avverso il presente provvedimento può essere proposta opposizione all'autorità giudiziaria ordinaria con ricorso depositato al tribunale ordinario del luogo ove ha la residenza il titolare del trattamento dei dati, entro il termine di trenta giorni dalla data di comunicazione del provvedimento stesso.

Roma, 1° giugno 2020

IL PRESIDENTE

SORO ANTONIO GIUSEPPE
GARANTE PER LA PROTEZIONE DEI DATI PERSONALI
PRESIDENTE
01.06.2020 12:22:31 UTC

IL RELATORE

SORO ANTONIO GIUSEPPE
GARANTE PER LA PROTEZIONE DEI DATI PERSONALI
PRESIDENTE
01.06.2020 12:23:45 UTC

IL SEGRETARIO GENERALE

BUSIA GIUSEPPE ANTONIO PIETRO
GARANTE PER LA PROTEZIONE DEI DATI PERSONALI
SEGRETARIO GENERALE
01.06.2020 12:13:34 UTC