GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Garante per la protezione dei dati personali - Primi riscontri alle ipotesi avanzate all'interno del Gruppo di lavoro datadriven per l'emergenza COVID-19

Preg.mo Avv. Valter Campanile
Capo di Gabinetto
Ministro per l'Innovazione Tecnologica e Digitalizzazione

Roma, 7 aprile 2020

OGGETTO: primi riscontri alle ipotesi avanzate all'interno del Gruppo di lavoro datadriven per l'emergenza COVID-19

Premessa

Con la presente si intende in primo luogo porgere un cordiale ringraziamento al Gruppo di lavoro data-driven per l'emergenza COVID-19 e a tutti i soggetti coinvolti nell'iniziativa, rappresentando un profondo apprezzamento per il lavoro e gli approfondimenti svolti, tutti volti a ricercare la soluzione che meglio concilia la scelta di soluzioni tecniche per il contrasto dell'emergenza epidemiologica con tutti i diritti fondamentali coinvolti.

Al fine di coadiuvare il gruppo di lavoro nelle proprie riflessioni, si inviano alcune osservazioni informali, che in tale veste non anticipano né sostituiscono quelle del Garante sulle scelte definitive.

1. Volontarietà dell'utilizzo dell'app e trasparenza del trattamento

Si prende favorevolmente atto che è stata prevista la volontarietà della partecipazione, in primo luogo perché, l'efficacia dello strumento richiede inevitabilmente la collaborazione attiva del singolo, il quale deve essere sensibilizzato sul fatto che l'uso di tale applicazione può contenere il contagio (proprio e altrui). È indispensabile, a tal fine, che il singolo possa confidare nella trasparenza e nella correttezza delle caratteristiche del servizio nonché nell'assenza del perseguimento di scopi ulteriori e incompatibili con tale finalità. L'idea che lo strumento possa essere utilizzato anche per altri scopi potrebbe infatti disincentivare il suo utilizzo, pregiudicando la primaria finalità di salute pubblica che esso dovrebbe perseguire.

Il rispetto del principio di trasparenza e correttezza, inoltre, è una condizione essenziale per l'attivazione di un circuito fiduciario nei confronti delle istituzioni che impiegheranno la soluzione tecnologica prescelta, fornendo agli interessati un'informativa chiara, con modalità che ne garantiscano la massima pubblicità e diffusione, anche mediante i mezzi di comunicazione, e che, fra gli altri elementi, sia in grado di spiegare le particolari finalità del trattamento, le sue possibili implicazioni e modalità, e affronti anche il tema dell'esercizio dei diritti degli interessati.

2. Base giuridica del trattamento

Occorre precisare che la base giuridica del trattamento non può essere individuata nel consenso dell'interessato perché non sussistono i requisiti previsti dal Regolamento UE 2016/679 (cfr. cons. 42, 43 e 46, di seguito, "Regolamento"); ma deve essere ricondotta all'esecuzione di un compito di interesse pubblico, rispetto al quale sarà comunque prevista la volontarietà di adesione da parte dell'interessato, sulla base di disposizioni normative idonee, che costituiscano una misura necessaria e proporzionata in una società democratica (art. 6, parr. 1, lett. e), 3 e 4; art. 9, par. 2, lett. g) e i) del Regolamento).

È pertanto necessario che il relativo utilizzo sia fondato su un'idonea base normativa. Questa, oltre a dover specificare la finalità perseguita e limitare il trattamento al perdurare dello stato di emergenza, precisando che i dati personali dovranno essere in ogni caso cancellati una volta raggiunto lo scopo per il quale sono stati raccolti e non potranno essere utilizzati per finalità diverse e ulteriori, rispetto a quelle stabilite dalla norma e rese note all'interessato dovrà prevedere misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato. Allo stato, tale base normativa non è desumibile da alcuna disposizione vigente e dovrà quindi essere elaborata ex novo o integrando le fonti esistenti, acquisito il parere del Garante, cosi da precisare normativamente almeno la finalità in concreto perseguita, il titolare del trattamento e le conseguenze per gli interessati.

L'individuazione di una chiara ed esplicita base giuridica, oltre che costituire una necessità, potrà determinare un maggiore tasso di accettazione e adesione alla soluzione tecnologica offerta da parte della collettività, in un contesto di ancora maggiore trasparenza e fiducia.

3. Privacy by design

La puntuale individuazione delle finalità per le quali si vorrebbe ricorrere all'utilizzo di una app è essenziale, non solo per rispettare il principio di privacy by design, ma proprio per progettare, nel dettaglio, soluzioni in grado di soddisfare le diverse esigenze correlate all'emergenza e per la valutazione della proporzionalità delle misure che si intendono adottare, tenendo conto dei gravi rischi per le libertà e i diritti degli interessati che potrebbero derivare dal trattamento.

Tali rischi, che dovranno essere accuratamente individuati e valutati nell'ambito di una valutazione di impatto, non riguardano solo quelli relativi alla perdita di riservatezza, ma comprendono anche quelli derivanti dall'utilizzo di informazioni non esatte, che potrebbero determinare alte percentuali di errore, con conseguenze pregiudizievoli sia sui diritti e sulle libertà dei singoli individui (falsi positivi o falsi contatti), sia sulle scelte dei decisori pubblici.

Nel fare ciò, occorre valutare, nel rispetto del principio di precauzione, l'adeguatezza del complesso delle misure di contenimento che si intendono introdurre, sia in relazione ai risultati prefissati, che alle risorse e agli strumenti a disposizione per raggiungerli, sulla base di indicatori qualitativi e ove possibile, quantitativi volti a dimostrarne in modo inequivoco l'efficacia.

Attesi i predetti margini di errore, occorrerà in ogni caso evitare sistemi basati su decisioni interamente automatizzate che si fondano esclusivamente sui dati raccolti attraverso l'applicazione, prevedendo sempre la possibilità di un intervento umano in grado di valutare i risultati e, se del caso, correggerli, affiancando le attuali modalità di ricostruzione della catena epidemiologica che richiedono l'intervento degli operatori sanitari per determinare le misure di sanità pubblica da adottare nei confronti degli interessati.

4. Finalità del trattamento e conseguenze per gli interessati

Da un primo esame dei documenti di sintesi trasmessi non emerge con chiarezza come si configuri il trattamento dei dati che si intende porre in essere nel ricostruire i contatti interpersonali di possibile contagiato, attraverso le applicazioni in esame, con particolare riferimento alle conseguenze per la filiera dei contatti di un soggetto risultato positivo.

In sostanza, non si comprende se, ricostruiti i contatti, si intenda:

- avvisare tali soggetti dell'avvenuta esposizione al rischio di contagio, oppure,
- attivare nei loro confronti iniziative di sanità pubblica.

Nel primo caso si tenderebbe a ricostruire i contatti per allertare la popolazione interessata di una possibile esposizione al rischio contagio, rimettendo agli stessi soggetti avvisati il compito di procedere, in via autonoma e secondo la propria coscienza, a contattare il personale sanitario preposto, secondo le indicazioni nazionali fornite nelle ultime settimane. In tal caso è

assolutamente necessario definire puntualmente il contenuto del messaggio inviato tramite l'applicazione, sia con riferimento ai dettagli dell'esposizione al potenziale contagio; sia in merito ai comportamenti che il soggetto avvisato dovrà tenere dopo aver ricevuto il messaggio (es. chi contattare, adozione di misure di prevenzione ulteriori, ecc.). In tal caso, la finalità perseguita sembrerebbe essere riconducibile a quella preventiva di allerta pubblica per finalità di protezione civile e autoprotezione. Nel secondo caso, una volta riscostruiti i contatti del contagiato, dovrebbe essere previsto l'intervento di un operatore di sanità pubblica che procederebbe a intervistare tali soggetti, al fine di programmare, sulla base di quanto appreso dagli stessi, le misure di sanità pubblica necessarie (tampone, isolamento, ricovero, ulteriori iniziative nei confronti di altri soggetti, ecc.). Come previsto dalle disposizioni vigenti, non sarebbe lasciata all'interessato la decisione di rivolgersi alle strutture sanitarie deputate al controllo dell'epidemia da COVID 19, essendo le stesse strutture di sanità pubblica a interpellare i contatti stretti del contagiato. In tale ipotesi, l'attività dovrebbe essere coordinata dalle strutture sanitarie a ciò deputate (asl, servizi di prevenzione, ISS).

In tale ultima ipotesi, riconducibile a una finalità di tutela della sanità pubblica, l'app costituirebbe pertanto un ausilio per gli operatori sanitari nella ricostruzione della filiera dei contatti, che si affianca alle metodologie, utilizzate fino a oggi, per includere tutti i potenziali soggetti a rischio eventualmente anche non rilevati dall'app.

In questa prospettiva appare necessario aver preventivamente organizzato modalità efficaci e rapide per consentire agli operatori di attivare tempestivamente le misure necessarie nei confronti dei soggetti esposti al rischio.

5. Ruoli e responsabilità dei soggetti coinvolti nel trattamento

Dalla documentazione fornita non emerge quali siano i soggetti coinvolti nel trattamento (titolare, contitolare, responsabile) e i dati personali effettivamente trattati da ciascuno di essi.

Per valutare i profili di protezione dei dati personali, è di fondamentale importanza individuare correttamente la titolarità del trattamento che dovrebbe essere ricondotta, proprio in relazione alle specifiche finalità, a uno o più soggetti pubblici (es.: ISS, ASL, Regioni, ecc.).

Assai rilevante, in considerazione dell'elevato rischio dei trattamenti in questione, si rivelerà l'oculata scelta e individuazione dei partner tecnologici (responsabili del trattamento), indispensabili per una gestione adeguata della complessa infrastruttura IT a cui l'app si dovrà appoggiare, alla quale occorrerà prestare la massima attenzione, tanto più se questi fossero stabiliti al di fuori dell'UE, avendo cura di privilegiare, piuttosto, nel rispetto del principio di precauzione, soggetti situati in territorio italiano, affidabili e dotati di proprie infrastrutture IT, organizzati anche in forma societaria, ma in partecipazione o in controllo pubblico, con esperienza pluriennale nella gestione di piattaforme complesse, che comportano la raccolta di dati, anche relativi alla salute, dalle app installate sui dispositivi degli utenti, e si interfacciano già con un elevato numero di enti e operatori pubblici garantendo un accesso selettivo ai dati (es. Sogei).

È necessario, inoltre, definire con chiarezza, fin dall'inizio, il ruolo e le responsabilità del soggetto fornitore dell'app, precisando se lo stesso si limiti a cedere la tecnologia per i successivi utilizzi ovvero sia chiamato a svolgere taluni trattamenti, che andrebbero in tale caso precisati, che ricadrebbero comunque sotto la responsabilità del titolare.

6. Alcune osservazioni sulle caratteristiche delle app in esame

La documentazione fornita non consente di valutare puntualmente gli aspetti di sicurezza del trattamento, sia in relazione alle app che in relazione ai sistemi di backend, né le specifiche misure di garanzia, comprese la minimizzazione, la pseudonimizzazione e la cifratura dei dati, controllo e tracciamento degli accessi, che invece dovranno essere rigorosamente individuati, una volta chiarite le modalità di utilizzo degli strumenti tecnologici, prevedendo meccanismi automatici di cancellazione dei dati personali – sia sui sistemi di backend e sui sistemi intermedi eventualmente previsti e da chiunque gestiti sia, infine, sul dispositivo mobile dell'utente – alla conclusione dei tempi di conservazione necessari al contenimento del contagio.

A prescindere dalla soluzione che verrà preferita dal Gruppo di lavoro, si ritiene indispensabile che qualsiasi app debba poter essere rimodulata in base alle esigenze in concreto individuate dai decisori pubblici, prevedendo soluzioni flessibili e suscettibili di essere modificate all'occorrenza, consentendo l'integrazione nel trattamento dei principi della protezione dei dati. Ciò anche perché le esigenze di contenimento potrebbero cambiare nel tempo.

In tale prospettiva, sulla base della documentazione fornita, si rileva che entrambe le soluzioni ritenute maggiormente affidabili dal

Gruppo di lavoro si basano sull'uso della tecnologia BT-LE che, nelle modalità in cui se ne prefigura l'utilizzo, appare essere quella più idonea a raggiungere l'obiettivo prefisso, in un'ottica privacy-oriented, poiché consente di individuare la catena dei contagi, rilevando con sufficiente accuratezza la distanza tra soggetti che, avendo con sé uno smartphone o altro tipo di dispositivo su cui è attiva e funzionante la app, entrano nella reciproca sfera di rilevamento con quella tecnologia. Tale tipo di rilevamento non produce nelle modalità in cui è proposto nelle soluzioni prospettate, una raccolta sistematica e centralizzata dei dati personali.

Occorre tuttavia prestare attenzione alla corretta definizione della distanza di rilevamento e del tempo di esposizione (durata del contatto), parametri che determinano la selezione dei contatti a reale rischio di contagio, perché una metrica spazio-temporale troppo ampia potrebbe amplificare il numero dei contatti da tracciare in assenza di un vero rischio e penalizzando l'efficienza del sistema nel suo complesso, mentre delle metriche eccessivamente ristrette potrebbero viceversa sottrarre dei contatti significativi.

Un'altra osservazione riguarda il fatto che le proprietà di maggiore o minore compliance alla disciplina di protezione dei dati personali dovrebbero riferirsi al sistema di tracciamento nel suo complesso e, più in generale, al sistema informativo di back-office a cui i dati raccolti vengono, in certe condizioni, conferiti.

Sarà importante quindi che le caratteristiche tecniche e organizzative del sistema informativo forniscano, unitamente a quelle delle singole componenti applicative, sufficienti garanzie in ordine alla protezione dei dati trattati, compreso il profilo della sicurezza, anche a garanzia della maggiore accettabilità sociale della soluzione prescelta.

Dal punto di vista tecnico, si confida nella possibilità che gli sviluppatori delle soluzioni prescelte possano individuare opportune misure tecniche per sopperire ad alcuni deficit di interoperabilità tra i due principali ambienti operativi (Apple iOS e Android) usati su dispositivi smartphone, che attualmente appaiono condizionare l'efficacia di applicazioni basate sulla tecnologia BT-LE per via di limitazioni presenti in particolare, nell'ambiente iOS a scopi di sicurezza e che, se non superate, rischiano di rendere meno efficace il rilevamento dei contatti, considerata l'attuale ripartizione dell'utenza che vede una forte presenza di dispositivi basati su quell'ambiente operativo (circa il 30%, a fronte del 70% di utenza Android in Italia sul totale degli smartphone).

Rispetto a quanto indicato nella relazione sui profili giuridici, occorre precisare che, in ogni caso, i dati raccolti e successivamente trattati dalle app in esame non possono essere considerati anonimi. Infatti, a determinate condizioni, potrebbe essere possibile/necessario che l'autorità pubblica competente identifichi nuovamente l'interessato.

Pertanto è corretto ricondurre i dati trattati alle seguenti categorie:

a) dati personali, in quanto sono considerati tali anche gli "identificativi online prodotti dai dispositivi, quali gli indirizzi IP, marcatori temporali (cookies) o identificativi di altro tipo, quali i tag di identificazione a radiofrequenza" (cfr. cons. 30 e art. 4, par. 1, punto 1), del Regolamento);

b) dati personali sottoposti a pseudonimizzazione, ossia data personali che "potrebbero essere attribuiti a una persona fisica mediante l'utilizzo di ulteriori informazioni" (cfr. cons. 26 e 29, e art. 4, par. 1, punto 5), del Regolamento), ad esempio nel caso di utilizzo di identificativi dinamici dei dispositivi.

L'Ufficio del Garante è in ogni caso a disposizione per collaborare e fornire soluzioni tecnico-giuridiche su ogni dubbio e/o criticità emerse o che dovessero emergere in materia di protezione dei dati personali da qualunque soluzione adottata.

Avv. Giuseppe Busia
Segretario generale del Garante per la protezione dei dati personali