Relazione tecnico-giuridica sui profili connessi all'eventuale adozione di una soluzione di contact tracing per il contrasto al COVID-19

Sottogruppo di lavoro "Profili giuridici della gestione dei dati connessa all'emergenza"

Sintesi del documento

Il presente documento riassume talune considerazioni di carattere giuridico - con particolare riferimento al diritto alla protezione dei dati personali e altri diritti fondamentali - relative all'eventuale utilizzazione di una soluzione integrata di *contact tracing* finalizzata esclusivamente a consentire ai cittadini che abbiano scelto liberamente di installare un'applicazione sui propri dispositivi e che siano risultati contagiati all'esito di diagnosi medica di informare - in forma anonima - altri cittadini - che a loro volta abbiano liberamente scelto di utilizzare la medesima applicazione - del rischio di contagio dovuto a un contatto e dell'opportunità di adottare talune cautele.
Il presente documento non si occupa, invece, di ogni eventuale diversa utilizzazione secondaria di tali soluzioni tecnologiche avente finalità diversa dal semplice *contact tracing* nei termini appena riassunti.
Le considerazioni che seguono sono basate sull'analisi della documentazione relativa a un subset di soluzioni tecnologiche tra quelle presentate nell'ambito della call lanciata dal Ministro per l'innovazione tecnologica e la digitalizzazione d'intesa con il Ministero della Salute ritenute dagli esperti tecnico-epidemiologici, sotto i profili di loro competenza, idonee a garantire gli obiettivi di contenimento della diffusione del virus e la progressiva revoca di taluni limiti e divieti adottati al medesimo fine nelle scorse settimane.
Le soluzioni tecnologiche esaminate più in linea con il quadro giuridico, in generale, funzionano come segue: il segnale Bluetooth LE (Low Energy) degli utenti che hanno scelto di installare una specifica applicazione viene registrato dalle analoghe applicazioni con le quali "entrano in contatto"; quando un utente viene diagnosticato contagiato dal COVID-19 il suo dispositivo trasmette i dati al server del soggetto pubblico che gestisce il sistema [alcune delle soluzioni valutate prevedono tale trasferimento su base sistematica e non condizionata], che provvede quindi a informare gli altri utenti - che abbiano egualmente volontariamente installato la medesima app - di essere a rischio contagio perché sono entrati in contatto con una persona risultata contagiata.
I presupposti essenziali delle valutazioni e considerazioni riassunte nel documento sono:
(a) che l'intero sistema integrato di *contact tracing* sia interamente gestito da uno o più soggetti pubblici e che il suo codice sia aperto e suscettibile di revisione da qualunque soggetto indipendente voglia studiarlo;
(b) che i dati trattati ai fini dell'esercizio del sistema siano "resi sufficientemente anonimi da impedire l'identificazione dell'interessato" [cfr. Considerando 26 GDPR] tenuto conto dell'insieme di fattori obiettivi, tra cui i costi, le tecnologie disponibili ed il valore della reidentificazione almeno in condizioni ordinarie e salvo il verificarsi di eventi patologici o, almeno, pseudoanonimi previa adozione di idonee misure idonee a limitare il rischio di identificazione degli interessati;
(c) che la decisione di usare la soluzione tecnologica sia liberamente assunta dai singoli cittadini;
(d) che raggiunta la finalità perseguita tutti i dati ovunque e in qualunque forma conservati, con l'eccezione di dati aggregati e pienamente anonimi a fini di ricerca o statistici, siano cancellati con conseguente garanzia assoluta per tutti i cittadini di ritrovarsi, dinanzi a soggetti pubblici e privati, nella medesima condizione nella quale si trovavano in epoca anteriore all'utilizzo della soluzione;
(e) che la soluzione adottata - nelle sue componenti tecnologiche e non tecnologiche - possa essere considerata, almeno in una dimensione prognostica, effettivamente efficace sul piano epidemiologico giacché, in difetto, diverrebbe difficile giustificare qualsivoglia, pur modesta e eventuale, compressione di diritti e libertà fondamentali.

(f) che la soluzione adotti misure tecniche ed organizzative che minimizzino i rischi di reidentificazione in ogni fase di vita del sistema (a titolo esemplificativo con variazione periodica e casuale dell'ID anonimo dell'applicazione).

Le analisi - parziali in quanto basate esclusivamente sulla documentazione acquisita nell'ambito della call e su alcune interviste telefoniche - e le valutazioni - preliminari e sommarie in considerazione del ridotto lasso di tempo avuto a disposizione - svolte nel corso dei lavori suggeriscono che una soluzione di *contact tracing* sia implementabile nel rispetto dei presupposti che precedono e che il suo utilizzo sia sostenibile nel rispetto del diritto alla protezione dei dati personali e degli altri diritti e libertà fondamentali.
Nel presente documento si forniscono taluni spunti di riflessione e raccomandazioni che, pur senza alcuna pretesa di esaustività, si auspica possano risultare utili al Governo nell'assunzione delle decisioni di propria competenza in relazione all'opportunità di adozione di una soluzione di *contact tracing e alle competenti Autorità amministrative indipendenti per lo svolgimento delle analisi e valutazioni* di propria competenza.

1. Il contesto di riferimento

Nel quadro delle azioni finalizzate al contrasto al COVID-19 il Governo intende esplorare l'eventualità di utilizzare idonee soluzioni tecnologiche al duplice scopo di contenere la diffusione del virus e consentire la progressiva eliminazione dei limiti, vincoli e divieti alla libertà di movimento e all'esercizio di attività professionali, commerciali e produttive che ci si è visti costretti ad adottare nelle ultime settimane.
In tale contesto il Ministro per l'innovazione tecnologica e la digitalizzazione, d'intesa con il Ministro della Salute, ha promosso una call pubblica finalizzata alla ricognizione delle soluzioni esistenti e affidato a un gruppo interdisciplinare di esperti (informatici, data scientist, epidemiologi, economisti e giuristi), tra l'altro, il compito di supportare il Dipartimento per l'innovazione tecnologica e la digitalizzazione della Presidenza del Consiglio dei Ministri e il Ministero della Salute nell'analisi e valutazione delle diverse soluzioni tecnologiche così identificate.

Il presente documento redatto dai componenti di un sottogruppo del predetto gruppo di lavoro dedicato allo studio e alla valutazione dei profili giuridici connessi al trattamento dei dati – personali e non – nell'attuale periodo di emergenza ha il duplice scopo di:

(a) identificare le principali questioni connesse al diritto alla protezione dei dati personali e, più in generale, ai diritti fondamentali che verrebbero in rilievo qualora il Governo decidesse di adottare soluzioni di c.d. *contact tracing*;
(b) svolgere un'analisi preliminare – sulla sola base delle informazioni fornite dai proponenti – dell'impatto privacy e sul versante degli altri diritti fondamentali di quelle tra le soluzioni tecnologiche identificate nell'ambito della citata call che siano risultate idonee, sotto il profilo tecnico-epidemiologico, al raggiungimento degli obiettivi perseguiti dal Governo.

Il presente documento non intende, invece, naturalmente, anticipare in alcun modo le valutazioni che, qualora il Governo decidesse di utilizzare una o più delle soluzioni tecnologiche identificate nell'ambito della call e della successiva attività del Gruppo di lavoro, competeranno al Garante per la protezione dei dati personali e/o all'Autorità per le Garanzie nelle Comunicazioni e/o all'Autorità Garante per la concorrenza e il mercato nell'esercizio dei relativi poteri.

2. L'obiettivo perseguito attraverso le soluzioni tecnologiche oggetto di valutazione e le loro funzionalità generali

La situazione attuale

Quando un cittadino viene identificato come contagiato - o anche solo potenzialmente contagiato - gli viene chiesto di segnalare con quali persone sia entrato in contatto nelle precedenti due/tre settimane e di informarle del rischio di essere state, a loro volta, contagiate affinché contattino gli operatori sanitari allo scopo di verificare l'eventuale contagio e, medio tempore, adottino misure idonee a evitare ulteriori contagi.

Tale processo sconta una serie di limiti:

(i) il soggetto contagiato può non conoscere [es: sconosciuti con i quali ha condiviso una corsa su un mezzo pubblico o la permanenza in un esercizio commerciale] o non ricordare i soggetti con i quali è entrato in contatto nel periodo di riferimento e/o non essere in grado di contattarli;

(ii) i soggetti eventualmente contagiati, possono non conoscere, non ricordare o non essere comunque in grado di contattare le ulteriori persone con le quali sono, a loro volta, entrate in contatto;

(iii) il soggetto contagiato - o come si è detto potenziale contagiato - è costretto a informare il personale sanitario dei nominativi delle persone con le quali è entrato in contatto nelle due/tre settimane precedenti e a informare tali persone del suo stato di contagiato e/o potenziale contagiato;

(iv) l'informazione relativa alla possibile esposizione a un rischio di contagio non è tempestiva perché affidata a un sistema manuale e volontario nonché all'utilizzo di informazioni di contatto non necessariamente utili [quelle in possesso del contagiato o potenziale contagiato o recuperate da questi e/o dagli operatori sanitari].

Si tratta di limiti che minano in maniera rilevante l'efficacia del processo e comprimono sensibilmente la privacy degli interessati mettendo in circolazione dati particolari (sanitari) al di fuori delle regole e garanzie previste dalla disciplina vigente.

Le soluzioni di contact tracing oggetto di valutazione

I limiti evidenziati nell'attuale approccio sembrano astrattamente superabili attraverso il ricorso a adeguate soluzioni tecnologiche di c.d. *contact tracing* già utilizzate - con formule e declinazioni sensibilmente diverse - in taluni Paesi stranieri.

Le più efficaci - a parere del sottogruppo che le ha valutate sotto il profilo tecnico-epidemiologico - tra le soluzioni individuate nell'ambito della call di cui si è detto dispongono - o potrebbero disporre all'esito dell'adozione di taluni correttivi emersi nel corso delle valutazioni degli scriventi - presentano le seguenti caratteristiche:

(a) identificazione delle istanze di installazione delle applicazioni su dispositivi dei cittadini che hanno preventivamente scaricato e installato l'app attraverso l'utilizzo di codici anonimi di identificazione delle singole installazioni dell'app [gli identificativi sono o, almeno, dovrebbero essere privi di qualsivoglia potenzialità identificativa dei cittadini possessori dei dispositivi];

(b) registrazione continua di un "diario dei contatti" con gli altri dispositivi con i quali entrano in contatto in un raggio compatibile con l'eventuale contagio nonché del dato relativo alla durata del contatto [tali informazioni sono o dovrebbero essere inaccessibili, in quanto registrate in forma crittografata, allo stesso titolare del dispositivo] ;

(c) indifferentemente

c.1) trasferimento dei dati archiviati nel citato “diario dei contatti” presente sul dispositivo del soggetto contagiato a un server gestito dal gestore del servizio solo a seguito dell’accertamento da parte degli operatori sanitari dello status di contagiato previo invio sul dispositivo del soggetto in questione di un apposito codice;
c.2) trasferimento sistematico di tutti i “diari dei contatti” degli utenti dell’app sul server del gestore del servizio a prescindere dal verificarsi di una specifica condizione;
(d) identificazione, attraverso un apposito algoritmo, ad opera del gestore del servizio, di un elenco di dispositivi posseduti da soggetti esposti a rischio contagio in quanto entrati in contatto, in circostanze di spazio e di tempo idonee a consentire il contagio, con il dispositivo del soggetto contagiato e, dunque, presumibilmente con quest’ultimo;
(e) invio intra-app a tali dispositivi di un messaggio contenente un’informazione relativa al rischio di contagio - senza alcuna menzione di dati identificativi del soggetto contagiato - con contestuale invito a adottare misure idonee a evitare ulteriori eventuali contagi e a contattare gli operatori sanitari preposti [il messaggio in questione dovrebbe essere instradato utilizzando esclusivamente l’identificativo che contraddistingue ciascuna installazione della app e non richiedere l’incrocio di tali informazioni non direttamente identificative con alcuna altra informazione di recapito];
(f) cancellazione di tutti i dati non anonimi o aggregati oggetto di trattamento - sia dai dispositivi dei singoli che dal server centrale - successivamente alla fine dell’emergenza .
(g) variazione periodica e casuale dell’ID anonimo dell’applicazione.

Le soluzioni tecnologiche in questione, inoltre, prevedono a volte una funzionalità di “diario clinico” attraverso la quale l’utente può annotare e tenere traccia di eventuali sintomi - anche lievi - e essere avvisato sull’opportunità di contattare gli operatori sanitari o adottare eventuali diversi accorgimenti.
I dati registrati nel diario clinico, tuttavia, restano all’interno del dispositivo, nell’esclusiva disponibilità del possessore - come fossero annotati su un taccuino completamente indipendente dall’app quale attività a carattere esclusivamente personale o domestico - e non sono in nessun caso condivisi con terzi.
I trattamenti di dati personali anche particolari connessi a tale funzionalità, pertanto, non formano oggetto di valutazione nel presente documento in quanto non appaiono suscettibili di evidenziare questioni peculiari rispetto a quelle caratteristici del rapporto tradizionale tra paziente e operatori sanitari.
Le stesse soluzioni, inoltre, generalmente dispongono di potenzialità di geolocalizzazione degli utenti che, tuttavia, nell’impostazione di base sono disattivate ed in ogni caso attivabili volontariamente solo dall’utente.
Sul punto si tornerà nel prosieguo per formulare alcune considerazioni di carattere generale.
L’implementazione di una soluzione tecnologica avente le caratteristiche qui sopra sinteticamente riassunte consentirebbe, in astratto di ovviare ai limiti evidenziati nel paragrafo precedente in relazione ai processi attualmente in uso in quanto, tra l’altro:

(a) sottrae la ricostruzione dei contatti del soggetto contagiato alla sua conoscenza e/o memoria;
(b) permette la diffusione immediata del messaggio relativo al potenziale contagio e alla necessità di adottare specifiche cautele a tutti i soggetti esposti a rischio contagio;
(c) consente che l’informazione di cui sub (b) sia comunicata in forma anonima e senza conoscere i destinatari.

Le soluzioni in questione, peraltro, se opportunamente configurate - e previa eventuale adozione di idonee misure tecnico-organizzative di minimizzazione dei trattamenti - appaiono capaci di garantire il risultato attraverso il trattamento di dati in forma anonima o, comunque, dotati di una ridottissima capacità identificativa, peraltro solo eventuale e indiretta, nella sola ipotesi in cui si verifichino eventi patologici.
In particolare, sulla base delle informazioni acquisite nell'ambito della call e nel corso delle interviste con taluni tra i soggetti proponenti di alcune delle soluzioni, sembra possibile affermare che il sistema integrato - app da installarsi sui dispositivi degli utenti, server centrale destinato allo storage del "diario dei contatti" e all'identificazione delle istanze di installazione dell'applicazione dei soggetti esposti a rischio di contagio, sistema di comunicazione di una positività di contagio al server e propagazione dell'allerta alle istanze di installazione dei dispositivi dei soggetti a rischio contagio - non necessiti, per il suo funzionamento, di alcun trattamento di dati personali potendo funzionare attraverso una rete nell'ambito della quale tutti i dispositivi coinvolti sono contraddistinti da identificativi completamente autonomi.

È, peraltro, evidente che le considerazioni che precedono circa il carattere normalmente anonimo o, almeno, pseudoanonimo dei dati trattati nell'esercizio del sistema verrebbero meno qualora si decidesse di attivare le funzionalità/potenzialità di geolocalizzazione delle quali sono dotate diverse tra le soluzioni esaminate: in questo caso, infatti, sussisterebbero tutta una serie di ipotesi nelle quali l'identificativo ancorché anonimo del dispositivo sul quale è installata un'app associato a dati di geolocalizzazione potrebbe consentire l'identificazione del possessore del dispositivo.
Ai fini del presente documento, tuttavia, non si prende in considerazione tale eventualità non essendo per un verso proposta come necessaria ai fini del funzionamento della più parte delle soluzioni tecnologiche esaminate e non apparendo, per altro verso, opportuna sotto il profilo della tutela dei diritti fondamentali la sua attivazione in questa fase.

Raccomandazioni
Preferenza per una soluzione che contempli il trattamento di soli dati anonimi

È evidente - ed è risultato palese in occasione della diffusione delle prime notizie relative alla circostanza che il Governo sta valutando l'eventuale adozione di una soluzione tecnologica di contact tracing - l'esistenza di una diffusa preoccupazione nella popolazione per l'eventualità che l'attuale emergenza sia in qualche modo utilizzata per introdurre nel Paese forme di monitoraggio o controllo di massa della popolazione ispirate a modelli in uso in altri ordinamenti.
È egualmente evidente che tale preoccupazione - peraltro fondata su solide basi costituzionalistiche - rischia di minare il successo dell'iniziativa disincentivando una parte potenzialmente anche rilevante della popolazione dall'utilizzo della soluzione in questione.
In tale contesto si raccomanda di valutare con particolare attenzione la possibilità di scegliere, tra le diverse opzioni disponibili, quella che appare capace di garantire un risultato in linea con gli obiettivi perseguiti previa utilizzazione di dati anonimi o, almeno, dotati di capacità identificativa degli interessati nella sola ipotesi di episodi patologici quali incidenti o attacchi malevoli.
In questa prospettiva si suggerisce altresì di astenersi dall'associare alle soluzioni tecnologiche qui considerate qualsivoglia funzionalità di geolocalizzazione soddisfacendo, eventualmente, la diversa esigenza di monitoraggio dei focolai di diffusione persistente del virus così come delle zone a rischio diffusione calante mediante il ricorso a sistemi e soluzioni autonomi e distinti.
L'anonimato - assoluto o quasi assoluto - dell'interessato nell'utilizzo della soluzione tecnologica eventualmente prescelta si presenta come un valore irrinunciabile da garantire sia sul piano del

bilanciamento dei diritti fondamentali sia ai fini del successo dell'iniziativa che ha nell'adesione convinta e spontanea dei cittadini un fattore strategico.
Non sembra lecito aprire la porta a eventuali compressioni della privacy e di altri diritti fondamentali laddove il perseguimento dell'obiettivo appaia possibile anche attraverso il ricorso a tecnologie che non impongono tale compressione

3. Principali questioni di diritto sottese all'implementazione delle soluzioni tecnologiche individuate

(A) Ragionevole probabilità di efficacia della soluzione

Sotto il profilo giuridico – tanto che si guardi al diritto alla protezione dei dati personali, tanto che si guardi a qualsiasi altro diritto fondamentale – la questione della sostenibilità del ricorso a una soluzione avente le funzionalità descritte nei paragrafi precedenti va, innanzitutto, affrontata e risolta in una logica di bilanciamento dei diritti, considerando sostenibile la parziale compressione di taluni diritti in vista della tutela di altri in ossequio a un criterio di necessità e proporzionalità.
Com'è noto, le norme in materia di protezione dei dati personali sono quelle attualmente vigenti e precisamente, per l'Italia, il Regolamento UE 2016/679 (GDPR) e il Decreto Legislativo 196/2003 (nel testo modificato dal D.Lgs. 101/2018), mentre per la Repubblica di San Marino, la Legge 171/2018. Inoltre, restano sempre valide le norme sovranazionali in subiecta materia e, in particolare, quelle contenute nella nota "Convenzione 108+", così come, per l'Europa, la Carta dei Diritti Fondamentali dell'Unione Europea che qualifica i diritti alla riservatezza e alla protezione dei dati personali come diritti fondamentali, nonché la legislazione europea.
In tale contesto normativo è evidente che, laddove non sussistessero sufficienti elementi a supporto dell'efficacia della soluzione tecnologica ipotizzata in termini di tutela della salute pubblica, difficilmente potrebbe accedersi a un giudizio di sostenibilità delle necessarie limitazioni e compressioni del diritto alla protezione dei dati e/o di altri diritti fondamentali per quanto esse possano risultare modeste e contenute previa adozione delle soluzioni oggetto della raccomandazione che precede.
In questa prospettiva, prima ancora di addentrarsi nell'esame delle questioni giuridiche connesse alla progettazione e sviluppo di talune specifiche soluzioni tecnologiche, sembra essenziale affrontare la questione della sussistenza di idonei elementi utili a ritenere che l'app eventualmente prescelta come componente del sistema integrato di contact tracing possa effettivamente essere scaricata e utilizzata regolarmente da una percentuale rilevante della popolazione da identificarsi sulla base degli studi epidemiologici in corso.
Nella medesima prospettiva, peraltro, appare altresì opportuno tenere presente che il solo presupposto che precede sarebbe, comunque, scarsamente produttivo degli effetti sperati qualora l'adozione di un'idonea soluzione tecnologica non fosse accompagnata da un'efficace organizzazione dei necessari presidi sanitari e dell'attività logistica necessaria, tra l'altro, alla distribuzione e esecuzione dei test tra i cittadini.
Al riguardo occorre tener presente - come risulta chiaro anche dall'esame delle esperienze straniere - che la componente tecnologica è, in ogni caso, "solo" una delle componenti di un sistema di contact tracing, inidonea, isolatamente considerata, a garantirne l'efficacia.
In assenza dei presupposti che precedono, pertanto, l'adozione delle soluzioni tecnologiche ipotizzate risulterebbero improduttive di benefici significativi in termini di contenimento della diffusione del contagio.
Al riguardo non si dispone, allo stato, di elementi idonei a fondare alcuna valutazione sul punto con specifico riferimento alle soluzioni oggetto della call.
Sul versante economico-sociale, peraltro, si è consapevoli che il nostro Paese, pur collocandosi al 24º posto fra i 28 Stati membri dell'UE nell'indice di digitalizzazione dell'economia e della società (DESI) della Commissione europea per il 2019, come indicato nel medesimo rapporto, "[...]è in buona posizione, sebbene ancora al di sotto della media dell'UE, in materia di connettività e servizi

pubblici digitali. I servizi pubblici online e open data sono prontamente disponibili e la diffusione dei servizi medici digitali è ben consolidata".
Si segnala, quindi, al riguardo, che, proprio tenendo conto delle condizioni di scarsa digitalizzazione del Paese sia sul versante infrastrutturale che culturale e educativo, l'obiettivo di ampia diffusione dell'app, specie qualora il download e l'utilizzo fossero affidati esclusivamente a una scelta volontaria del singolo cittadino, appare estremamente ambizioso.

Raccomandazioni
Alla luce delle considerazioni che precedono si raccomanda di anteporre a qualsivoglia valutazione relativa all'adozione di una specifica soluzione tecnologica, analisi e valutazioni relative agli strumenti - comunicativi, regolamentari e tecnologici - utilizzabili al fine di rendere raggiungibile il predetto obiettivo di diffusione e utilizzo della soluzione da parte della necessaria percentuale minima di popolazione.
Tale raccomandazione ha, peraltro, un duplice riflesso giuridico:
(a) come si è detto dalla potenziale efficacia della soluzione in termini di tutela della salute pubblica dipende ampiamente la sua sostenibilità in termini di impatto su altri diritti e libertà fondamentali;
(b) taluni degli strumenti utilizzabili per aumentare la diffusione della soluzione e il suo utilizzo da parte dei cittadini potrebbero incidere sulla base giuridica del trattamento dei dati personali.

(B) Esclusione dell'obbligo e adozione di strumenti di incentivazione all'utilizzo della soluzione tecnologica

Il conseguimento dell'obiettivo di effettivo utilizzo della soluzione tecnologica da parte di una adeguata percentuale della popolazione potrebbe essere difficilmente conseguibile qualora ci si limiti a promuoverne il download e l'uso attraverso un'idonea campagna di comunicazione, lasciando poi la decisione completamente affidata alla scelta individuale del singolo cittadino. Tuttavia, la strada della previsione ex lege di un obbligo di utilizzo dell'app, pur non preclusa, appare costituzionalmente non agevole (cfr. Corte cost., sent. n. 5/2018) e controindicata da ragioni di ordine pratico-giuridico.
La soluzione che appare più perseguibile è una incentivazione al download e all'uso della soluzione tecnologica in questione fondata sulle elevate garanzie da essa prestate.

Ragioni di ordine pratico e giuridico suggeriscono questa raccomandazione.
A solo titolo esemplificativo si rileva che:
- non sussisterebbero efficaci strumenti di *enforcement* nell'ipotesi di inadempimento anche diffuso all'obbligo e/o di artificiosa sottrazione all'obbligo medesimo [es: utenti che potrebbero scaricare l'app ma utilizzare poi in maniera anomala il dispositivo spegnendolo in taluni momenti o separandosene];
- un obbligo o un incentivo che impatti sull'esercizio di diritti e libertà rischierebbe di essere percepito dai cittadini come un'ingerenza eccessiva dello Stato in scelte di carattere personale e, probabilmente, considerata una "forzatura" normativa finalizzata a consentire forme di controllo di massa della popolazione;
- talune fasce della popolazione, probabilmente, si troveranno in una condizione di oggettiva difficoltà di utilizzo della soluzione non disponendo di uno smartphone o non essendo in grado di usare la soluzione per questioni anagrafiche, legate al proprio stato di salute (ipovedenti o portatori

di altri handicap, detenuti), culturali o economiche. Peraltro, queste annovererebbero fasce già vulnerabili della popolazione esacerbando un digital divide e discriminazioni inammissibili

- nella loro versione di base, le soluzioni tecnologiche esaminate non tengono traccia di eventuali disattivazioni del bluetooth e/o di usi anomali dello smartphone con la conseguenza che sussisterebbe il rischio di garantire benefici a cittadini che installino e usino l'app per il tempo strettamente necessario alla "conquista" del beneficio;
- è difficilmente aggirabile, praticamente prima che giuridicamente, il problema delle conseguenze dell'eventuale violazione dell'obbligo\impegno incentivato da parte del cittadino: ipotizzare una sanzione per l'ipotesi in cui il cittadino, ad esempio, spenga lo smartphone durante determinate fasce orarie o non lo porti con sé, sembra piuttosto difficile anche alla luce della difficoltà di accertamento del carattere doloso o anche solo gravemente colposo della condotta [es: lo smartphone può spegnersi per incolpevole esaurimento della carica, può essere dimenticato a casa, può trovarsi in una posizione di assenza di campo ecc.].

Peraltro, sotto il profilo della disciplina sulla protezione dei dati personali taluni sistemi di incentivazione all'utilizzo della soluzione e, dunque, alla prestazione dell'eventuale consenso ai connessi trattamenti di dati personali rischierebbero di compromettere la libertà della prestazione del consenso e, conseguentemente, la sua validità, rendendo necessario identificare una diversa base giuridica per i trattamenti di dati personali [cfr sul punto si veda il paragrafo (C) che segue].

Raccomandazioni

Si sconsiglia, di introdurre qualsivoglia obbligo legale di utilizzo della soluzione tecnologica.
Si suggerisce di affidare il ricorso a tale soluzione ad una adesione libera, ancorché incentivata, del singolo utente.
Sono assolutamente sconsigliate, perché di dubbia costituzionalità, forme di incentivo che graduino\limitino l'accesso dei cittadini a servizi altrimenti fruibili secondo principi di parità di trattamento o che vincolino l'esercizio di diritti di libertà all'adozione dell'app.
Alla luce delle considerazioni precedenti e volendo evitare incentivi tali da far venir meno il carattere volontario della decisione, l'adozione massiva della soluzione prescelta pare meglio essere affidata ad una campagna informativa per l'adesione volontaria capace di sviluppare fenomeni di incentivazione dolce tali però da non comprimere se non addirittura violare diritti e libertà fondamentali.
Valido esempio concreto potrebbe essere l'invio per sms a tutti i cittadini iscritti ai servizi di alert della protezione civile locale o nazionale del link per scaricare l'app con messaggio del tipo "Oggi salvo vite umane , oggi salvo la mia vita, installo "….". Analoga campagna push potrebbe essere aggiunta nella messaggistica di fatturazione e pubblicitaria dei soggetti privati che aderiscono all'iniziativa.

(C) Implementabilità del sistema attraverso trattamento di dati esclusivamente anonimi o base giuridica del trattamento dei dati personali eventualmente sotteso al funzionamento dell'app

Alcune delle soluzioni tecnologiche oggetto di valutazione sembrerebbero implicare - il condizionale è necessaria conseguenza dell'assenza di informazioni sufficientemente puntuali nella documentazione sin qui acquisita - un trattamento di dati personali ancorché in misura estremamente contenuta e, anzi, in alcuni casi ai limiti - previa adozione di talune possibili misure di minimizzazione dei trattamenti - della definizione di dato personale e, conseguentemente dell'applicabilità della vigente disciplina nazionale e europea in materia di privacy.
Il funzionamento di base delle soluzioni tecnologiche prese in esame - o almeno di quelle risultate più rispondenti ai requisiti tecnico-epidemiologici - prevede la circolazione di soli dati non identificativi scambiati tra dispositivi contraddistinti da identificativi insuscettibili di rivelare, almeno direttamente, l'identità dei possessori; più correttamente, probabilmente – salvo miglior verifica tecnica – dati pseudoanonimi.
I due unici momenti dell'intero processo di *contact tracing* identificati come astrattamente idonei a impattare - pur senza annullarla - sulla validità di tale assunto appaiono essere rappresentati dal dialogo tra il dispositivo dell'utente e il server centrale ai fini del trasferimento - eventuale e episodico oppure sistematico a seconda delle soluzioni prescelte - del "diario dei contatti" e dal dialogo tra il dispositivo dell'operatore sanitario e il server del gestore del sistema finalizzato all'attivazione del processo di contatto dei soggetti a rischio contagio.
Nel primo momento, infatti, il server centrale, come si è anticipato, è tecnicamente nella condizione - peraltro necessaria ai fini del funzionamento del protocollo di comunicazione TCP/IP - di identificare l'indirizzo IP dal quale proviene il "diario dei contatti" preso in carico.
Analogamente nel secondo momento l'operatore sanitario, evidentemente, all'atto della trasmissione del codice per l'attivazione del processo di contatto dei soggetti a rischio contagio ha preventivamente identificato anagraficamente il proprio paziente e, pertanto, disponendo altresì (sebbene anche qui in modo istantaneo e transitorio) dell'identificativo univoco della installazione sul dispositivo del paziente medesimo potrebbe ricondurre tale ultimo dato a una specifica identità anagrafica.
In entrambi i casi, peraltro, appare possibile fare in modo che il gestore del sistema di *contact tracing* non raccolga alcun dato identificativo diretto o indiretto [indirizzo IP del dispositivo del soggetto dal quale provengono le informazioni archiviate nel diario dei contatti nel primo caso e dati anagrafici del soggetto contagiato nel secondo] e che pertanto, come si è anticipato, il suo trattamento possa sostanzialmente considerarsi, salvo quanto si dirà nel prosieguo, un trattamento di dati anonimi.

In particolare:
(a) in relazione al primo dei due momenti, come si è anticipato sopra, potrebbe ipotizzarsi l'interposizione di un proxy gestito da una terza parte fidata che raccolga la comunicazione cifrata dei diari dei contatti dai possessori dei dispositivi e la inoltri al server del gestore del sistema dopo aver proceduto alla definitiva cancellazione dell'indirizzo IP identificativo del mittente; in questo modo al gestore del sistema, titolare del trattamento, perverrebbero esclusivamente dati resi sufficientemente anonimi da impedire l'identificazione dell'interessato tenuto conto dell'insieme di fattori obiettivi tra cui i costi, le tecnologie disponibili ed il valore della reidentificazione;
(b) in relazione al secondo dei due momenti, come pure si è anticipato, potrebbe ipotizzarsi che l'operatore sanitario, nella sua qualità di titolare autonomo o di responsabile nominato da un autonomo - rispetto al gestore del sistema di contact tracing - titolare del trattamento dei dati acquisiti nell'ambito del rapporto con il paziente - incidentalmente utente dell'app - qualora accerti il verificarsi della condizione idonea a giustificare l'invio dell'alert ai dispositivi entrati in contatto

con quello del soggetto contagiato proceda alla comunicazione al server del gestore del sistema dell'input all'invio del predetto alert. In tal caso sarebbe sufficiente che contestualmente all'invio, il sistema utilizzato dall'operatore sanitario eliminasse definitivamente ogni associazione tra l'identificativo dell'installazione dell'app e l'identità anagrafica del paziente dell'operatore sanitario.

Tali accortezze farebbero sì che il gestore del sistema si trovi anche in questo flusso di input a ricevere esclusivamente "dati resi sufficientemente anonimi da impedire l'identificazione dell'interessato" tenuto conto dell'insieme di fattori obiettivi, tra cui i costi, le tecnologie disponibili ed il valore della reidentificazione. Ovviamente anche in questo caso con la sola eccezione di eventuali incidenti o attacchi idonei a consegnare nelle mani di un medesimo soggetto la pluralità di elementi informativi necessari al fine di realizzare l'associazione tra dati anonimi e dati direttamente o indirettamente personali.

Si tratta di un'ipotesi remota ma ineliminabile in ragione della quale, nel prosieguo, si preferisce considerare il trattamento posto in essere dal gestore del sistema come un trattamento comunque rientrante, sebbene solo in una dimensione cautelativa, nell'ambito di applicazione della disciplina in materia di protezione dei dati personali.

In tale contesto la principale questione da affrontare nel valutare l'impatto privacy è, evidentemente, quella relativa alla base giuridica del trattamento di dati personali che viene in rilievo nell'esercizio del sistema.

In linea di principio tale base giuridica potrebbe essere identificata nel consenso dell'interessato, trattandosi di una soluzione astrattamente compatibile con la circostanza che presupposti necessari per l'inizio di ogni trattamento sono il download dell'app, l'installazione sul dispositivo dell'interessato e l'utilizzo dell'app medesima sebbene in modalità "passiva" ovvero in background.

L'identificazione nel consenso della base giuridica del trattamento in questione, peraltro, potrebbe essere quella meglio capace di tener conto anche dell'eventualità - remota ma ineliminabile per quanto si è detto - che i dati oggetto di trattamento, al verificarsi di un evento patologico, siano in grado di reidentificare un interessato e associargli un dato particolare quale l'aver effettuato un tampone con un determinato esito.

Tale soluzione, tuttavia, presenta taluni limiti:
1) la libertà del consenso, come è noto necessario presupposto per la sua validità, rischia di essere compromessa dagli eventuali meccanismi di incentivazione all'uso dell'app e, dunque, al connesso trattamento di dati personali;
2) la libera revoca del consenso potrebbe avere implicazioni sul funzionamento dell'intero sistema;
3) a seguito della duplice manifestazione di volontà relativa all'installazione e all'utilizzo dell'app - eventualmente da far constare attraverso accettazione di termini d'uso - tutti i trattamenti strumentali al funzionamento del sistema di contact tracing appaiono necessari con la conseguenza che l'eventuale consenso risulterebbe, di fatto, obbligatorio risultando impossibile, in difetto, il funzionamento dell'applicazione per le finalità sue proprie.

Anche in considerazione delle perplessità emerse con riferimento all'identificazione del consenso come base giuridica dei trattamenti connessi al funzionamento del sistema di contact tracing si suggerisce di affidare l'eventuale adozione di tale sistema a un decreto legge che, con riferimento ai profili oggetto del presente documento, potrebbe stabilire:

(a) che il gestore del proxy e quello del sistema, rispettivamente con riferimento, alla raccolta, anonimizzazione e all'inoltro al gestore del sistema nonché alla raccolta e alla conservazione sono legittimati a trattare i dati degli utenti - come si è detto "sufficientemente anonimi" ai sensi del GDPR - a condizione che gli utenti medesimi abbiano manifestato liberamente l'adesione ai termini d'uso dell'applicazione i quali dovranno chiarire i trattamenti posti in essere da ciascun soggetto;
(b) che gli operatori sanitari sono obbligati a inserire i dati relativi all'eventuale diagnosi di contagio nel sistema di contact tracing attivando così l'alert destinato ai soggetti a rischio di contagio [art. 9.2.h Regolamento].

O, in alternativa, stabilire:

(a) che il gestore del proxy, con riferimento alla raccolta, anonimizzazione e inoltro dei dati, e il gestore del sistema, con riferimento alla raccolta e alla conservazione, sono legittimati al trattamento dei dati medesimi sulla base dell'eventuale consenso dell'interessato;
(b) che gli operatori sanitari sono obbligati a inserire i dati relativi all'eventuale diagnosi di contagio nel sistema di contact tracing attivando così l'alert destinato ai soggetti a rischio di contagio [art. 9.2.h Regolamento].

Nella sostanza si tratta di scegliere se identificare o meno la base giuridica del trattamento nel consenso degli interessati, anche se solo in misura parziale e limitatamente al solo trattamento da parte del gestore del server proxy e del gestore del sistema dei dati riconducibili all'interessato tramite l'IP di invio. In ogni caso si muoverebbe dal presupposto che, probabilmente, tale scelta non è indispensabile sotto un profilo tecnico-giuridico ma indiscutibilmente potrebbe risultare - ove la si ritenga legittima in applicazione della disciplina vigente nonostante le perplessità sopra evidenziate - a rendere più facilmente sostenibile sul versante politico-mediatico l'eventuale decisione di adozione di una soluzione di contact tracing.
Si tratta di due opzioni tra cui appare difficile identificarne una ideale e da preferire certamente sull'altra.
Si tratta, quindi, di due distinte opzioni che portano a qualificare diversamente la natura giuridica del consenso prestato.
In un'ottica di obbligo legale, il consenso dell'utente è una condizione per l'applicabilità della legge; il consenso è, perciò, un evento, assimilabile all'atto giuridico in senso stretto.
In un'ottica negoziale, il consenso dell'utente è una manifestazione di volontà ad aderire alle condizioni previste dalla legge per usufruire della prestazione; il contesto è qui assimilabile ai negozi a fonte eteronoma, cioè ai negozi che sono disciplinati non dalla volontà delle parti, ma dalla legge.
Il precipitato giuridico, ossia la portata pratica, di tale distinzione, ad esempio, si può riscontrare nell'ipotesi di scaricamento dell'app da parte di soggetto incapace naturale. Quid iuris? Nel primo caso (atto giuridico in senso stretto), si ritiene che l'attività non impedirebbe la raccolta dei dati, laddove, nel secondo caso (atto negoziale) il vizio del consenso renderebbe, invece, revocabile (ex nunc)/annullabile (ex tunc) il trattamento successivo del flusso di informazioni inviate.
Ma l'analisi giuridica si deve arrestare dinnanzi alle superiori scelte di politica legislativa.
Il medesimo decreto legge dovrebbe altresì precisare, sempre limitatamente ai profili oggetto del presente documento: 1) l'obbligo del gestore del server proxy di procedere alla immediata cancellazione di ogni associazione tra ID dell'applicazione e IP di invio dei dati; 2) l'obbligo di adozione di misure tecniche ed organizzative tali da impedire la memorizzazione dell'associazione tra identità della persona fisica e ID dell'installazione dell'app all'atto dell'inserimento delle positività da parte del personale sanitario.