

App di *contact tracing* e tutela dell'affidamento digitale di Riccardo Borsari e Elena Montemezzi

La rapidità della diffusione del contagio da Covid-19 e le altissime percentuali di soggetti asintomatici in grado di veicolare il virus hanno reso imprescindibile procedere, sin dalle primissime fasi dell'emergenza in corso, al tracciamento e all'avvertimento dei soggetti che sono stati a contatto con persone a cui è stata diagnosticata la positività al virus.

L'obiettivo del "*contact tracing and warning*" è, infatti, consentire alle autorità sanitarie pubbliche di rapidamente identificare il maggior numero possibile di contatti confermati con un caso Covid-19, di chiedere loro di auto-isolarsi ove possibile e, nel caso in cui sviluppino sintomi, rapidamente sottoporli a test e isolamento. Lo scopo secondario del *contact tracing* è ricostruire, attraverso dati isolati e aggregati, modelli di infezione nella società (definiti "*infection patterns*") in base ai quali assumere decisioni di contenimento a livello locale.

Si tratta di un'azione fondamentale per il contenimento della diffusione dell'epidemia e indispensabile per affrontare la cosiddetta Fase 2 che seguirà il *lockdown*.

L'esperienza dei Paesi che hanno già affrontato la fase della riapertura insegna che l'utilizzo della tecnologia può fare la differenza: infatti, è chiaro che i metodi tradizionali e "manuali" di tracciamento dei contatti, oltre a comportare un enorme dispendio di risorse, sono del tutto insufficienti.

Nelle ultime settimane si è aperto, quindi, un dibattito sulle caratteristiche che le app di tracciamento devono possedere per essere compatibili con i principi che in Europa assicurano la tutela della privacy: evidentemente, nel territorio europeo non è replicabile il "modello Cina", dove sono stati sfruttati sia applicativi già presenti sugli smartphone dei cittadini (ad esempio WeChat e Alipay) sia soluzioni diverse, la cui adozione è stata spesso imposta o comunque connessa alla possibilità di ricevere servizi. Pertanto, il 15 aprile 2020 la Commissione europea, a seguito del confronto con il Comitato europeo sulla protezione dei dati (EDPB), ha emanato una guida pratica rivolta agli Stati membri. La guida, definita come una "cassetta degli attrezzi comune" ("*Common EU Toolbox for Member States*") è stata sviluppata dal Network e-Health (composto da autorità competenti in materia di salute digitale provenienti da ciascuno stato membro dell'Unione).

L'obiettivo dichiarato è quello di promuovere un approccio coordinato tra gli Stati membri che possa offrire un valido supporto alla graduale revoca delle misure di confinamento, in linea con quanto raccomandato dalla Commissione lo scorso 8 aprile 2020.

La guida elenca i requisiti essenziali per le app di tracciamento, che devono anzitutto essere pienamente conformi ai principi europei in materia di privacy e *data protection* (in primis i principi stabiliti dal Regolamento 2016/679/UE e dalla Direttiva E-privacy 2002/58/CE). Gli strumenti dovrebbero, altresì, essere implementati in stretta collaborazione con le autorità di salute pubblica e da queste approvati, e devono basarsi su dati anonimizzati e sfruttare le più recenti soluzioni tecnologiche per garantire la miglior tutela della privacy, come la tecnologia di prossimità Bluetooth.

La Commissione sottolinea che le app per il tracciamento dei contatti devono essere temporanee e installate su base volontaria, e devono altresì prevedere la auto-disattivazione con cancellazione di tutti i dati personali e delle informazioni di prossimità non appena la crisi sarà finita.

Infine, le app dovrebbero essere interoperabili in tutta l'Unione Europea, in modo che i cittadini siano protetti anche quando attraversano i confini statali.

La Guida si occupa anche del problema della diffusione di app definite come “illecite o dannose”, sensibilizzando gli Stati membri a implementare un sistema nazionale di accreditamento al fine di promuovere app statali che rispettino i requisiti. Non solo, la Commissione precisa che sarà necessaria una stretta collaborazione con gli *app stores* per promuovere le app nazionali ed eliminare dai cataloghi le app dannose.

Il primo passo ufficiale del Governo italiano non si è fatto attendere, anche a fronte del proliferare di iniziative regionali con caratteristiche molto diverse.

Lo scorso 16 aprile, infatti, è stata pubblicata l'ordinanza con cui il commissario straordinario per l'emergenza Covid 19 ha reso nota la scelta del Governo tra le varie applicazioni presentate alla Task Force precedentemente nominata: la preferenza è ricaduta sulla app Immuni, prodotta dalla società Bending Spoons S.p.a. La scelta è stata motivata sulla base della conformità della app rispetto al modello europeo delineato dal Consorzio PEPP-PT (un progetto nato dall'iniziativa di soggetti privati ma esplicitamente menzionato dalla Commissione europea tra le iniziative di interesse) e della idoneità a garantire il rispetto della privacy.

Secondo quanto reso noto, la app Immuni, che sarà scaricabile solo su base volontaria e gratuitamente, si compone di due parti. La prima è un sistema di tracciamento dei contatti che sfrutta la tecnologia Bluetooth Low Energy (BLE): i dati personali rimangono sul dispositivo, mentre all'utente viene assegnato un ID temporaneo che varia spesso e viene scambiato tramite Bluetooth con i dispositivi che vengano a trovarsi a distanza uguale o inferiore a un metro.

La app, quindi, conserva sul dispositivo di riferimento una lista di codici identificativi anonimi di tutti i dispositivi ai quali il primo è stato vicino. Nel caso in cui il proprietario del primo dispositivo risulti affetto dal virus, sarà possibile ricostruire a ritroso tutti i dispositivi incontrati e, quindi, rintracciare e isolare i potenziali contagiati.

La seconda funzione di Immuni è un diario clinico contenente i dati anagrafici e sanitari del singolo utente (sesso, età, malattie pregresse, assunzione di farmaci), che dovrebbe essere aggiornato tutti i giorni con eventuali sintomi e cambiamenti dello stato di salute. Dalle notizie disponibili, pare che in caso di contagio l'utente potrà, previo esplicito consenso, condividere i dati in questione con i sanitari per agevolare la diagnosi e la scelta del trattamento di cura.

Nei giorni immediatamente successivi all'ordinanza del 16 aprile si sono scatenati commenti e critiche, in molti casi forse premature alla luce delle (scarse) informazioni rese note.

Un dato è, tuttavia, sufficientemente certo: questa tecnologia può essere efficace solo se la app sarà scaricata e utilizzata almeno dal 60% della popolazione.

Si tratta di un risultato piuttosto ambizioso (per usare un eufemismo), se consideriamo ad esempio che gli italiani con un profilo Facebook sono meno del 50% della popolazione complessiva.

In considerazione degli evidenti “limiti intrinseci” del modello basato sulla volontarietà dello strumento, vi è chi ha ipotizzato che l'adesione possa essere in qualche modo “incentivata” introducendo limiti alla circolazione per chi non risulti in possesso dell'applicazione e vi è anche chi sostiene che l'unica strada percorribile sia la previsione dell'obbligatorietà dell'adozione della app.

Tali ipotesi vanno, tuttavia, attentamente ponderate alla luce dei principi stabiliti anzitutto dal GDPR, che prevede, in particolare, che il consenso dell'interessato sia valido solo ove sia prestato liberamente e in assenza di condizioni.

Per quanto riguarda la possibilità di ancorare il trattamento a una base giuridica diversa dal consenso, effettivamente il GDPR riconosce la liceità del trattamento qualora sia necessario per l'esecuzione di

un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento e, tuttavia, impone che il trattamento dei dati personali (ivi compresi i dati appartenenti a particolari categorie) per motivi di interesse pubblico rilevante sia basato sul diritto dello Stato membro, richiedendo quindi un vaglio parlamentare (riserva di legge relativa) che tenga conto della necessaria aderenza ai principi dettati dal GDPR (in particolare artt. 5, 25, 30, 32) e dal d. lgs. n. 101/2018.

Si tratta di valutazioni per nulla semplici e dall'esito non scontato: il rischio è che una lunga discussione parlamentare conduca a un vicolo cieco, mentre il tempo a disposizione trascorre inesorabilmente.

L'obiettivo posto dalla Commissione europea (che, vale la pena precisarlo, non ha previsto opzioni alternative alla volontarietà dello strumento) può essere perseguito in modo ancora diverso, tenendo presente e interpretando estensivamente uno dei principi che reggono l'impianto GDPR e che dovremmo avere ormai metabolizzato: il principio di *accountability*. Non vi è dubbio che il Governo, nel decidere i contenuti tecnici della app in corso di implementazione, debba operare un necessario bilanciamento di interessi tra la tutela della salute pubblica (e individuale) e la tutela della privacy dei propri cittadini. Dar conto ai potenziali interessati di questa delicata operazione implicherebbe una scelta coraggiosa in termini di serietà e trasparenza, e potrebbe altresì agevolare il raggiungimento della percentuale necessaria di adesioni.

Come già segnalato dal Presidente del Comitato europeo sulla protezione dei dati personali (EDPB) nella lettera alla Commissione europea del 14 aprile 2020, infatti, l'adozione volontaria dipende strettamente dal livello di fiducia individuale: ne deriva la necessità di attribuire massima importanza ai principi in materia di protezione dati e l'opportunità di adottare un atteggiamento di *disclosure* in relazione alla motivazione delle scelte effettuate e alle precauzioni adottate.

Le iniziative di promozione dovrebbero, quindi, essere precedute dalla condivisione di una serie di informazioni con l'opinione pubblica: *in primis*, dovrebbero essere chiarite le tipologie di dati personali oggetto di trattamento, le relative finalità e il rispetto del principio di minimizzazione (e, più in generale, tutti i contenuti necessari dell'informativa che sarà resa poi agli utenti).

In ottica di trasparenza, il Governo dovrebbe altresì rendere pubblica la valutazione d'impatto preventiva (DPIA), obbligatoria nel caso di specie ai sensi dell'art. 35 del GDPR.

Dovrebbero essere illustrate le misure di sicurezza adottate anche con riferimento a eventuali *data center* di archiviazione per l'*upload* dei dati di tracciamento dei soggetti risultati positivi. Nel caso in cui fosse possibile ricondurre *ex post* i dati anonimizzati di trattamento (o i dati relativi al diario clinico) ai soggetti coinvolti, andrebbero illustrati i rischi derivanti da un possibile *data breach* e le misure adottate per prevenire tale eventualità. Ciò vale, a maggior ragione, nel caso in cui il soggetto privato titolare della licenza dovesse essere autorizzato a svolgere attività di manutenzione che permette l'accesso ai dati personali.

Infine il codice sorgente, che secondo le linee guida della Commissione europea dovrebbe essere *open source*: l'ordinanza del Commissario straordinario indica che il codice sorgente sarà messo a disposizione del Governo ma non è chiaro se sarà garantito il controllo diffuso e, quindi, se il codice sarà messo a disposizione della collettività.

L'auspicio è che la *disclosure* vada di pari passo con lo sviluppo dell'applicazione, in modo che il Governo possa tener conto anche delle informazioni relative alla percezione dello strumento da parte dei cittadini: in questo modo lo sforzo di implementazione non andrà vanificato a causa del (legittimo) timore degli interessati di rinunciare a garanzie di tutela.