ARTICOLO DI PUNTOSICURO

Anno 22 - numero 4688 di Mercoledì 29 aprile 2020

Le APP di tracciamento fra tutela della salute pubblica e della privacy

Un approfondimento sui temi, in apparente conflitto, legati alla protezione dei dati personali e legati alla protezione della salute pubblica, soprattutto nei casi di pandemia.

Anche su Puntosicuro più volte il tema della protezione della salute pubblica, da confrontare con le esigenze di protezione dati personali, è stato più volte trattato. Non parliamo poi dei mezzi di comunicazione di massa, che parlano, e talvolta sproloquiano, proprio su questi argomenti. Si tratta di argomenti di estrema delicatezza, perché l'equilibrio fra questi diritti non è facile da trovare. Non per nulla, dalla commissione europea è stato pochi giorni fa trattato questo tema, mettendo a confronto i diversi strumenti che vengono attualmente sviluppati in diversi paesi europei, proprio per mettere a disposizione strumenti che possono mitigare la diffusione del contagio da COVID 19.

Ricordo che a livello europeo due sono gli organismi che stanno indagando su questi applicativi, vale a dire il supervisore europeo per la protezione dei dati ed il comitato europeo per la protezione dei dati. Il primo comitato tiene sotto controllo il trattamento di dati personali effettuati da agenzie europee, mentre il secondo comitato tiene sotto controllo l'attività delle autorità garanti nazionali.

L'analisi delle APP sul piano europeo

Il coordinatore della commissione sulle libertà civili, presso il parlamento europeo, ha sollecitato caldamente entrambi questi enti ad emettere al più presto delle linee guida, che possano essere utilizzate sia dagli sviluppatori di questi applicativi, sia dalle autorità di controllo nazionale, che devono alla fin fine garantire agli organi governativi che le **applicazioni**, che si pensa di utilizzare, siano conformi ai dettati del regolamento europeo. Un'attività di armonizzazione fra i vari paesi è anch'essa importantissima, perché la movimentazione fra i vari paesi di soggetti, contagiati o meno, è oggi libera e debbono essere offerte garanzie in merito alla presenza di soddisfacenti tutele in tutti paesi europei.

È bene ricordare che non solo in Europa si sta studiando questo problema, ma anche in molti altri paesi europei. Grazie ad uno studio legale specializzato, offro in allegato ai lettori una panoramica mondiale di ciò che si sta facendo in vari paesi e si offre quindi la possibilità di effettuare un confronto fra il differente approccio seguito in differenti paesi.

Ad esempio, un elemento fondamentale è la differenza di approccio nel rendere l'applicativo, comunque esso funzioni, obbligatorio per tutti soggetti positivi, oppure facoltativo. È facile vedere come in alcuni paesi, dove lo Stato tiene sotto stretto controllo i cittadini, come la Corea del Sud e Singapore, l'utilizzo di questo applicativo sia obbligatorio, mentre in altri paesi sia facoltativo. È evidente che il fatto che un soggetto positivo al COVID 19 accetti o rifiuti di essere inserito nel programma di gestione della app modifica in modo drammatico la efficienza ed efficacia di questi applicativi.

Incidentalmente, è bene sottolineare che sono ormai numerose le entità sanitarie, in Italia ed in altri paesi, che cercano di raccogliere una gigantesca quantità di dati, afferenti allo stato di salute di centinaia di migliaia di cittadini, con la dichiarata finalità di monitoraggio della situazione e prevenzione della diffusione del virus. Proprio recentemente, un caro collega, che gestisce una struttura di assistenza a soggetti disabili, ha ricevuto una richiesta perentoria, da parte dell'autorità locali della sanità pubblica, di comunicare una moltitudine di dati afferenti a soggetti assistiti e familiari. Egli mi ha chiesto un amichevole consulto e sono stato lieto di offrire il mio altrettanto amichevole parere.

Innanzitutto, se i soggetti interessati esprimono il loro consenso alla comunicazione di questi dati, non vi è alcun problema. Se invece il titolare del trattamento provvede a comunicare questi dati alle strutture pubbliche, senza aver ottenuto precedentemente il consenso dell'interessato, occorre trovare adeguate motivazioni, afferenti alla liceità e finalità di questo trattamento, effettuato in assenza di libero ed informato consenso. A questo proposito, ricordo il prezioso documento, già menzionato in passato, pubblicato dal comitato europeo per la protezione dei dati, che afferma come determinati trattamenti possano essere effettuati, anche in assenza di consenso dell'interessato, a condizione che il titolare, oppure il richiedente i dati, dia ampie, adeguate, credibili e legalmente sostenibili motivazioni per la richiesta avanzata al titolare, con tutte le garanzie del caso per il successivo trattamento dei dati e soprattutto confermando la presenza di termini perentori per la cancellazione di questi dati. Ad oggi aspettiamo ancora una risposta da parte delle pubbliche strutture!

Superato quindi il problema del consenso, obbligatorio o superabile da parte dell'interessato contagiato coinvolto, andiamo a vedere la pratica utilità di questi applicativi.

L'utilità delle APP di tracciamento

Essi si dividono, come già accennato in due grandi categorie, a seconda che, come si presume di fare in Italia, la segnalazione di prossimità ad un soggetto contagiato sia circoscritta, equivalente all'ormai famoso campanellino, che secoli fa i soggetti lebbrosi dovevano portare alla caviglia, oppure l'applicativo sia inquadrato in un sistema, più generale e certamente più penetrante, di localizzazione e gestione di soggetti contagiati. In questa seconda categoria di applicativi rientrerebbe certamente il cosiddetto braccialetto elettronico, o applicativo equivalente, che mira non tanto a verificare se il soggetto contagiato si trovi in vicinanza di altri soggetti, quanto il fatto che il soggetto contagiato rispetti i vincoli della quarantena, evitando di allontanarsi dal domicilio obbligato, appunto in fase di quarantena. Un applicativo di questo genere deve tenere sotto controllo tutti i movimenti e gli spostamenti del soggetto coinvolto, indipendentemente dal fatto che questo soggetto si avvicini o meno a soggetti terzi. D'altro canto, è evidente che il rischio legato a spostamenti illeciti del soggetto contagiato può portare ad un aumento delle possibilità di contagio di soggetti terzi. Applicativi di questo genere, ovviamente assai più flessibili, possono funzionare in vari modi: ad esempio, il soggetto contagiato è dotato di un braccialetto elettronico, con rilevatore **GPS** e scheda Sim. Tutti i movimenti del soggetto vengono tracciati dal dispositivo GPS e vengono inviati ad una struttura centrale di ricezione. La struttura effettua un confronto tra la posizione effettiva del soggetto e l'area corrispondente alle posizioni autorizzate e lancia un allarme, ove si verifichi un disallineamento.

Un applicativo di questo genere è già in uso da tempo sugli automezzi, destinati al trasporto di merci pregiate (oppure furgoni per il trasporto valori), che si spostano nella penisola. A bordo dell'automezzo si trova un dispositivo, simile a un braccialetto elettronico, che trasmette in continuazione i dati ad una centrale di comando e controllo. Ove l'automezzo si sposti fuori delle zone autorizzate, ad esempio esca da un percorso autostradale, la centrale riceve un allarme e si attivano le procedure di pronto intervento. Questa architettura viene chiamata, con termine anglosassone, " **geofencing**". Viene creata una sorta di recinzione elettronica, tracciata sulla carta geografica, che determina gli ambiti di spostamento accettabili per l'automezzo, oppure per la persona sotto controllo. Un applicativo di questo genere è estremamente efficace, ma richiede l'allestimento di una mostruosa centrale di ricezione e gestione delle segnalazioni di allarme, in grado di tenere sotto controllo centinaia di migliaia di persone in tutta Italia. La messa in piedi in tale struttura non può certo avvenire dall'oggi al domani e richiede risorse economiche e temporali assolutamente gigantesche. D'altro canto, un tale approccio offrirebbe un elevato livello di garanzia di controllo sul soggetto contagiato, tale da minimizzare la possibilità che egli possa contagiare altri soggetti. Si parte ovviamente dal principio

che, finché il soggetto contagiato si trova nella zona di quarantena, il rischio verso terzi sia bassissimo.

La seconda categoria di applicativi, quelli appunto corrispondenti al campanello del lebbroso, non ha certamente l'invasività della soluzione appena illustrata, in quanto non tiene sotto controllo la posizione del soggetto contagiato, ma offre uno strumento ai soggetti terzi di essere messi in guardia, in caso di eccessivo avvicinamento. Esiste poi tutt'una serie di variazioni su questi due grandi temi.

Una delle variazioni, ad esempio, consiste nel fatto che la segnalazione di avvicinamento eccessiva ad un soggetto contagiato non venga direttamente trasmessa, tramite Bluetooth, allo smartphone del soggetto che si trova lì vicino, ma venga trasmessa ad una centrale di comando e controllo, che a sua volta potrà verificare quali smartphones si trovino nelle immediate vicinanze del soggetto contagiato, inviando loro un messaggio di allerta. Questa soluzione è evidentemente molto più invasiva, dal punto di vista della protezione dei dati, perché la centrale di comando e controllo conosce tutti gli spostamenti del soggetto contagiato ed anche le posizioni relative, rispetto a un soggetto che si trovi nelle vicinanze.

Le garanzie tecniche di protezione dei dati

Si è parlato da più parti di applicativi, che utilizzano **dati personali**, protetti da anonimato. È evidente che ciò non è possibile, almeno in via assoluta, in quanto almeno i dati personali del soggetto contagiato devono necessariamente essere caricati nella app del contagiato stesso, oppure disponibili presso la centrale nazionale di comando e controllo. A seconda della soluzione adottata, nel caso del campanellino che suona non è necessario conoscere i dati dei soggetti che si trovino nelle vicinanze del contagiato, e quindi a rischio, mentre in altre soluzioni bisogna conoscere anche i dati personali del soggetto esposto a rischio di contagio, per inviargli un messaggio di allarme. Se il lettore si prenderà il disturbo di leggere il ponderoso documento allegato, potrà vedere come in molti paesi si sono scelti approcci molto diversi e risulta al momento non facile individuare quale sia l'approccio più affidabile e maggiormente garantistico, nei confronti della protezione dei dati.

A questo proposito, non desidero ripetere quanto **già scrissi in una precedente notizia**, circa tutte le garanzie tecniche di protezione dei dati che devono essere offerte da chiunque voglia sviluppare una qualsivoglia applicazione, che tratti dati personali critici. Ancora una volta, il riferimento a norme italiane, europee od internazionali rappresenta un elemento di garanzia non trascurabile, circa la professionalità dell'approccio di chi sviluppa l'applicativo e la garanzia del rispetto della regola d'arte, in fase di progettazione ed utilizzo dell'applicativo stesso.

Come annunciato in precedenza, siamo in attesa di ulteriori notizie sulla soluzione il governo sceglierà, dopo aver ovviamente ricevuto il via libera della nostra autorità garante.

Adalberto Biasiotti

Covid-19 Data Protection Guidance (pdf)