I pericoli del tracciamento digitale dei contatti

Gli stati di necessità, cioè quelle situazioni in cui qualche circostanza imprevista costringe ad affrontare problemi eccezionali, sono un terreno privilegiato per il "soluzionismo digitale". Ma le soluzioni tecnologiche (ormai sempre più digitali) non sono mai risolutive a meno che non siano compatibili con lo scenario sociale e organizzativo.

(Articolo pubblicato il 17 aprile su “Link&Think” *link-and-think.blogspot.com*)

di Enrico Nardelli e Isabella Corradini

Si sta discutendo in questi giorni di come gestire il ritorno alla "normalità" abolendo le misure di distanziamento sociale ma assicurando il controllo della situazione sanitaria. A tal scopo è stato proposto il cosiddetto tracciamento digitale dei contatti, ovvero tenere traccia degli incontri tra le persone in modo tale da poter rapidamente risalire, nel caso in cui una persona venga trovata positiva al test, ai suoi contatti dei giorni precedenti e bloccare ulteriori contagi.

È bene chiarire che il tracciamento dei contatti è una procedura standard dell'OMS per le malattie infettive e viene usualmente condotta in modo manuale dal personale sanitario intervistando la persona infetta. Si sostiene però che nel caso di grandi numeri di infetti la procedura manuale è insufficiente e serve un approccio "automatico" basato appunto sulla tecnologia digitale.

Sfatiamo subito l'idea che la tecnologia possa fare tutto da sola. Lo dice il responsabile dell'unica soluzione di tracciamento dei contatti effettivamente realizzata e che ha funzionato. «Nessun sistema di tracciamento digitale dei contatti può rimpiazzare quello manuale» ha scritto il responsabile del sistema usato a Singapore. Serve comunque dotare il sistema sanitario nazionale di adeguate risorse che sinora non si sono viste e, anzi, nel decennio passato sono state diminuite.

Ricordiamo poi che tracciare i contatti vuol dire entrare nella sfera dei dati personali, violare la zona di riservatezza personale garantita da leggi italiane ed europee. Si dice che sia possibile farlo senza violare la privacy. È davvero possibile? Esaminiamo la faccenda dal un punto di vista tecnico, a grandi linee per rendere l'esposizione comprensibile a tutti.

Tracciare automaticamente con cui una persona entra in contatto si può fare in due modi: assoluto e relativo. Si fa in modo "assoluto" appoggiandosi sul gestore della rete di telefonia mobile, che sa costantemente dove sia ogni dispositivo: grossolanamente, se il GPS è spento, con precisione se il GPS è attivo. Mentre in assenza del GPS è in generale difficile stabilire con certezza se il "contatto" sia avvenuto in modo che abbia senso sanitario (se due persone sono a 1 o 10 metri di distanza è epidemiologicamente molto diverso) col GPS questi problemi sono superati. Il gestore potrebbe quindi per ogni numero di telefono registrare l'elenco dei contatti, con durata e posizione. Il problema di questa soluzione è che chiunque viene in possesso di questa lista possiede un controllo sociale enorme, anche in assenza di infezioni. Non è un caso che il tracciamento digitale delle persone, in tutti i paesi democratici, richiede che le forze di polizia debbano preventivamente ottenere, caso per caso, l'autorizzazione della magistratura sulla base di circostanziate evidenze. Autorizzarle per l'intera popolazione vorrebbe mettere in discussione le fondamenta della società democratica.

Vediamo allora la soluzione "relativa". In questa, utilizzando uno dei sensori di comunicazione disponibili sullo smartphone ed un'opportuna app, è ogni dispositivo a registrare localmente l'elenco dei suoi contatti, con durata e posizione. In tal caso nessun soggetto ottiene questo controllo sociale e, si dice, l'app può essere realizzata in modo tale che ogni contatto venga registrato usando un identificativo anonimo e non riconducibile al proprietario. Ma se non li possiamo individuare come potremmo avvisarli di essere stati in contatto con un infetto? Perché sarebbe ogni telefono a determinarlo localmente, utilizzando gli identificativi anonimi degli infetti, che verrebbero distribuiti a tutti da un servizio centralizzato che li ottiene da chi, a seguito dei test, comunica volontariamente di essere infetto.

Però, come molte organizzazioni per la protezione dei diritti civili hanno sottolineato, un'app di questo genere dovrebbe esser realizzata in modo "aperto", ovvero le regole del suo scambio dati con le altre app e tutte le istruzioni che esegue sullo smartphone per tener traccia dei contatti dovrebbero poter essere liberamente esaminate, in modo tale che nessuno corra il rischio di trovare sul suo telefono un'app che fa cose diverse. Però, se l'app è aperta, è in grado di comunicare con ogni altra app che segue le stesse regole.

Allora, immaginate di aver scoperto che siete stati in contatto con un infetto per la prima volta 3 giorni fa. Se quella persona l'avete incontrata anche in tutti i giorni successivi, nella vostra storia locale vi saranno altrettante segnalazioni di persone infette in tutti quei giorni. La app ufficiale magari non dirà niente di tutto questo, ma solo di rivolgersi ad una struttura sanitaria per un controllo. Si può però facilmente immaginare che possa nascere un mercato di app "derivate" che vi offrono queste informazioni. Un'app "derivata" vi dirà, per ogni giorno, quante volte in un quel giorno avete incontrato un certo infetto e se in uno stesso giorno ne avete incontrato uno solo o più di uno. Questa app "derivata" non potrà dirvi se gli incontri dei giorni diversi si riferiscono alle stesse persone ma, considerando che in una situazione di normalità ognuno di noi ha una certa regolarità di incontri e ci sono relativamente pochi infetti in giro, queste informazioni combinate con il ricordo di ciò che avete fatto vi permetterebbero di dedurre parecchio.

Alla nascita di app "derivate" possono contribuire anche motivazioni di natura psicologica e sociale. Da un lato, infatti, il desiderio di sapere, quello che chiamiamo curiosità umana, è una molla potentissima, alla quale pochi sfuggono. Ma c'è in ballo anche la combinazione tra il bisogno di preservare la propria salute e quella delle persone care. Inoltre, il bombardamento quotidiano su regole e comportanti da seguire per tutelare la salute di tutti finisce per sviluppare comportamenti di diffidenza nei confronti dell' "altro", talvolta al limite della paranoia. Basta vedere come in questo periodo, camminando per strada, si tende ad aumentare le distanze dagli altri, arrivando persino a cambiare marciapiede. È facile da questo scivolare in un clima di sospetto generalizzato, di cui le cronache quotidiane di vicini e runner denunciati ci hanno già fornito numerosi esempi.

Oltre al problema effettivo di una possibile violazione della privacy, quindi, questo clima di sospetto genera altre considerazioni. Sappiamo, infatti, che la soluzione "relativa" per il tracciamento digitale dei contatti sopra accennata richiede di essere usata da almeno il 60% delle persone, per essere utile. È chiaro quindi che entrerebbe in gioco una fortissima pressione sociale per spingere ad omologarsi nel suo uso e creando pregiudizi nei confronti di chi, per qualunque motivo, decide di non farne uso.

Come ovviare a queste criticità?
L'unica possibilità che intravediamo è quella di usare applicazioni "ufficiali" che "parlano" solo con altre applicazioni ufficiali. Per garantire questo bisognerebbe far sì che le applicazioni ufficiali siano realizzate dalle società internazionali che attualmente hanno il monopolio dei sistemi operativi per la telefonia cellulare (Android e iOS). In un mondo in cui i dati delle persone sono il nuovo petrolio, affidare il controllo della nostra privacy in mano ad aziende che perseguono un obiettivo di business ed hanno un potere economico superiore a quello di molti Stati non sembra una mossa vantaggiosa per i cittadini. Non a caso le relative società si sono già mosse in questa direzione. Siamo noi che non dovremmo cedere quei dati digitali che sono ormai parte integrante del nostro essere.

Per completare poi il quadro, va spesa qualche parola sulla sicurezza della tecnologia di base che potrebbe essere usata. Qui le scelte possibili sono solo due: il WiFi e il Bluetooth. Purtroppo, entrambe, nella modalità che dovrebbero essere usate per il tracciamento dei contatti, offrono il fianco a vulnerabilità che potrebbero compromettere l'integrità dei dispositivi digitali mobili.

Richiedere infatti che tutti i cittadini vadano in giro con il Bluetooth (o altra tecnologia) costantemente disponibile per comunicare è di fatto equivalente a chiedere loro di non chiudere a chiave la porta di casa perché deve passare il dottore per una visita medica. Nel mondo reale equivarrebbe ad esporre le case di tutti i cittadini ad un elevato rischio di intrusione. Lo stesso accadrebbe nel mondo digitale, con la differenze che qui tutto accade senza la nostra percezione. I dispositivi di tutti si troverebbero sottoposti a scansioni a tappeto da parte dei "cattivi" che, ormai, non hanno bisogno di essere hacker di professione, dal momento che le cassette degli attrezzi per scardinare le "case digitali" si trovano sul mercato a prezzi abbordabili.

Una volta entrati, il problema non sarebbe più tanto quello relativo ai dati dell'app di tracciamento dei contatti ma quello, più grave, di avere un intruso ostile all'interno di ciò che è ormai strettamente integrato nella nostra esistenza, lo smartphone, depositario di tutti i nostri segreti, personali e professionali. L'unica contro-misura sarebbe aggiornare costantemente il proprio telefono. Ma quanti di noi lo fanno? Vogliamo davvero poggiare la privacy dei cittadini sulla certezza (!?) che abbiano tutti aggiornato il proprio smartphone?

Nelle discussioni in corso si dà per scontato che le soluzioni digitali siano comunque utili, nonostante chi le abbia usate estensivamente perché le aveva già a disposizione, Singapore, abbia dovuto poi mettere il paese in quarantena. Nonostante le organizzazioni internazionali sopra citate abbiano sottolineato la necessità, per misure di questo genere, di effettuare preventivamente valutazioni costi-benefici dei potenziali risultati ottenibili. Dove sono tali analisi?

Gli stati di necessità, cioè quelle situazioni in cui qualche circostanza imprevista costringe ad affrontare problemi eccezionali, sono un terreno privilegiato per il soluzionismo digitale, dal momento che la ristrettezza di risorse e la necessità di “fare presto” premono per accorciare i tempi della decisione. L’emergenza sanitaria che stiamo vivendo è esemplare da questo punto di vista. Basare una soluzione di massa (che ha comunque bisogno per funzionare di tutta di una serie di misure di contorno - come hanno osservato sia il Garante Italiano della Privacy che le varie organizzazioni internazionali) su una tecnologia che ha dimostrato nel corso degli anni di non avere le spalle robuste rispetto alla sicurezza mi sembra una scelta che, anche se "tecnicamente" interessante, sia da rigettare dal punto di vista sociale e politico.

Il problema è analogo a quello di molti altri casi: le soluzioni tecnologiche (ormai sempre più digitali) non sono mai risolutive a meno che non siano compatibili con lo scenario socio-organizzativo, dotate di adeguate risorse finanziarie e materiali, e supportate dalla volontà politica.

Se questi elementi mancano, rimangono solo la distruzione delle relazioni sociali e la svendita della nostra libertà, quindi della democrazia.