# Il tifo contro immuni non ha senso - Intervista ad Antonello Soro

### Il tifo contro immuni non ha senso

Intervista ad Antonello Soro, Presidente del Garante per la protezione dei dati personali
*(Di Salvo Ingargiola, Fortune Italia, 2 luglio 2020)*

Il soggetto che risulta positivo al Covid-19 fornisce, volontariamente, l'identificativo Imei del proprio dispositivo cellulare all'Asl di competenza che poi è tenuta a trasmetterla al server centrale per consentirgli di ricostruire, tramite un calcolo algoritmico, la rete di contatti. Da qui parte il 'viaggio' dei dati sensibili dell'app Immuni, voluta dal Governo per fronteggiare l'emergenza Covid, e autorizzata dal Garante per la protezione dei dati personali. "Le informazioni - chiarisce il Garante, Antonello Soro - non finiscono mai nelle mani di soggetti terzi che non hanno titolo ad acquisirli come Google, Apple o Bending Spoons", la società che ha materialmente ideato e progetto la App, 150 dipendenti, 90 mln di dollari di vendite nel 2019, detenuta per il 2% dal fondo cinese Nuo Capital.

*"Le scelte del Governo italiano, che noi abbiamo condiviso essendosi conformate alle indicazioni da noi rese prima e dopo l'emanazione della norma di riferimento (art. 6 Dl n. 28/2020), sono state anche un punto di riferimento nelle valutazioni fatte dal Board dei garanti europei", spiega Soro, presidente dell'Autorità che si occupa di proteggere la privacy dei cittadini italiani dal 2012. Sono tante e variegate le nuove sfide legate a questo tema, in un contesto come quello attuale, con nuove opportunità e rischi che arrivano dalla Rete.*

Secondo il Garante Soro *"sì è vero, lo strumento tecnologico è importante ma è solo il pezzo di una strategia nella quale è fondamentale tutto ciò che avviene a valle. Nel momento in cui si riesce ad avere la collaborazione del cittadino che contribuisce a ricostruire la rete epidemiologica (secondo gli esperti, per essere efficace, l'app deve essere scaricata da almeno il 60% degli italiani), il Sistema sanitario deve essere velocissimo nell'effèttuare i test diagnostici*".

Già, è anche una questione di tempo. Se è vero, infatti, che l'app Immuni, essendo un sistema decentralizzato, consente di detenere i dati dell'utente nel suo dispositivo in una prima fase, è altrettanto vero che, nel momento in cui si riscontra un caso positivo, come si diceva all'inizio, le stesse informazioni sensibili iniziano a 'muoversi'. E da questo momento in poi che, in modo particolare, si accendono i riflettori su tempi e modalità. Il principio da seguire - come ha spiegato la stessa Autorità Garante nell'audizione informale, in videoconferenza, lo scorso 8 aprile, in commissione Trasporti alla Camera dei deputati - è garantire "il minor ricorso possibile a dati identificativi, sia in fase di raccolta sia di conservazione'". In altre parole, la soluzione del 'diario dei contatti' registrato nel cellulare dell'utente è stata considerata preferibile proprio perché così si è deciso di evitare la conservazione in banche dati di gestori, con tutte le criticità messe in evidenza dalla giurisprudenza della Corte di giustizia europea in tema di data retention.

*"Gli Stati e i governi europei - ammette Soro - hanno sensibilità differenti. Alcuni Paesi hanno adottato soluzioni simili alla nostra, altri invece no". Il traguardo di un software europeo che definisse criteri omogenei e comuni a tutti i Paesi europei non è stato raggiunto. Sfumato questo obiettivo, come è stato sottolineato qualche settimana fa dal Comitato Ue per la protezione dei dati personali (Edpb), la condivisione dei data tramite le app, di persone a cui è stato diagnostico il Covid-19, deve essere attivata solo su base volontaria. E, passaggio ancor più importante e delicato, secondo l'European Data Protection Board l'obiettivo dell'interoperabilità di tali strumenti adottati nei diversi Paesi europei non dovrebbe essere perseguito, proprio per evitare di estendere la raccolta di dati personali oltre ciò che è necessario. "La persona che risulta positiva al tampone - chiarisce il garante Soro - oltre ad adottare tutte le misure già previste dalle normative vigenti, potrà offrire ma solo volontariamente la catena dei propri contatti. È un'informazione che, però, diventa importante se molti utilizzano l'applicativo".*

Sotto questo aspetto, il giudizio del Garante è chiaro: "*C'è una norma esplicita, prevista dalla disciplina generale: chi dovesse raccogliere i dati personali, non avendone titolo, compie un illecito trattamento degli stessi. Una pratica che può essere sanzionata sia a livello amministrativo sia penale"*. Ecco perché secondo Soro non ha senso 'tifare' contro l'app Immuni che, secondo lui, ha garanzie sufficienti in materia di privacy. *"Non capisco, anche dopo l'accoglimento di tutte le indicazioni del Garante (tra cui avere espresso come preferibile la tecnologia bluetooth che consente la ricostruzione a ritroso dei contatti, scartando al contrario l'opzione della geolocalizzazione, ndr) l'insistenza con cui molti, ancora, nonostante tutto, sollevano dubbi e scoraggiano i cittadini. È un atteggiamento che, di certo, non contribuisce a creare quel clima di fiducia che è fondamentale per rendere efficace lo strumento".*

Tutte le precauzioni sembrano essere state prese. E anche se il Comitato europeo per la protezione dei dati, in un documento contenente le linee guida sulle app di tracciamento, pubblicato ad aprile, dice con chiarezza che *"tali strumenti possono comportare un rischio elevato per i diritti e le libertà delle persone"*, in Italia, secondo Soro, *"l'App Immuni contiene garanzie sufficienti dal punto di vista della protezione del dato. Il rischio* - taglia corto - *è inferiore rispetto a quello generale che si corre tutte le volte che tali informazioni vengono trattate nella dimensione digitale"*. In altre parole, l'app Immuni è stata promossa anche se, è vero, come ammette lo stesso Garante Soro, *"dobbiamo mettere in conto sempre la possibilità remota che ci sia un hacker che, nonostante un sistema di sicurezza molto forte e solido come quello gestito da Sogei, tra i più affidabili e presidiato anche dal punto di vista militare, abbia la capacità di 'bucare' i! server. Tutto può capitare: anche il Pentagono ha subito un accesso abusivo"*.