18/04/2020
Sito Web

key4biz

Immuni, dal Cloud alla DPIA. Tutti i dubbi sull'app per il contact tracing

LINK: https://www.key4biz.it/immuni-dal-cloud-alla-dpia-tutti-i-dubbi-sullapp-per-il-contact-tracing/300971/

Di Prof. Avv. Alessandro del Ninno Studio Legale Tonucci & Partners Ecco tutti gli aspetti alla luce dei quali dovremo - quando ne saremo messi in condizione - esaminare e valutare la app 'Immuni', per comprendere se la protezione dei nostri dati e della nostra riservatezza resti davvero immune a trattamenti non conformi. La società Bending Spoons (che prende il nome dai cucchiaini piegati dalla forza del pensiero in Matrix) ha dunque "piegato" la resistenza delle altre 318 app di contact tracing che erano state proposte nell'ambito delle fast call di Innova per l'Italia.... È ancora presto - e si sa ancora poco - per dare giudizi definitivi di conformità tecnico-legale della app, per una serie di ragioni. Il primo motivo è - come si legge nell'ordinanza firmata dal Commissario Arcuri - che la app prescelta appare non del tutto sviluppata, se è vero che Bending Spoons si impegna "a completare gli sviluppi informatici che si renderanno necessari per consentire la messa in esercizio del sistema nazionale di contact tracing digitale". Dunque occorrerà vedere se "gli sviluppi informatici del sistema nazionale di contact tracing digitale" confermeranno le premesse di cui si parla e cioè che la app funzionerà su base volontaria, non dovrebbe utilizzare la geolocalizzazione ma solo la tecnologia il Bluetooth con raggio di azione di 1 metro e consentire il trattamento dei dati personali in modalità decentralizzata, in locale sul dispositivo. Condizioni che vengono richiamate anche dal Comitato Europeo per la protezione dei dati personali ("EDPB") nella sua recente lettera alla Commissione UE sulle app di contact tracing dello scorso 14 aprile. La mancanza di trasparenza Tuttavia dubbi emergono: il primo è sulla mancanza di trasparenza. La app è stata scelta senza alcuna possibilità di prendere visione della documentazione (che non mi risulta sia stata resa pubblica) del Gruppo di Lavoro di esperti data-driven e delle relative valutazioni a base della scelta. Ad oggi la conformità data protection è solo dichiarata. Sarebbe assai apprezzabile che - come suggerito nella sopra citata lettera dell'EDPD sulle app di contact tracing - che Bending Spoon mettesse a disposizione di tutti noi la Valutazione di Impatto sulla protezione dei dati personali (DPIA) che senza dubbio deve aver obbligatoriamente effettuato. Da questa potremmo anche capire in che termini la app sia stata sviluppata alla luce dei princìpi - pure obbligatori - di privacy by design e privacy by default. Ritengo che la maggiore trasparenza possibile aiuterebbe anche ad aumentare il tasso di adesione volontaria alla app Immuni: se come utente e cittadino ho potuto preliminarmente verificare (ad esempio dalla DPIA resa pubblica) il rispetto dei princìpi sul trattamento che l'EDPB richiama (minimizzazione, proporzionalità adeguatezza, anonimità, misure di sicurezza, etc) sarò più portato ad aderire. Ma i dubbi non riguardano solo la insufficiente trasparenza. Penso ad esempio al cloud che sembra - per l'app Immuni (il cui nome, a dirla tutta, è anche fuorviante... perché serve al contrario a tracciare gli infetti mentre sembra essere un richiamo

ad un tool sulla immunità, fa riflettere...) - l'unica modalità possibile per svolgere calcoli complessi. Intanto, sempre richiamando la lettera dell'EDPB, vi si legge che "I calcoli basati su algoritmi nell'ambito di app di contact tracing dovrebbero operare sotto lo stretto controllo e la supervisione di personale qualificato in modo da prevenire casi di falsi positivi e negativi e in nessun caso ci si deve affidare a procedimenti solo e del tutto completamente automatizzati, anche per le indicazioni successive". Quale tipo di Cloud? Quindi mi piacerebbe capire meglio di che cloud parliamo (intervengono fornitori privati, tipo Google?), dove sono i server di cui si servirebbe il "sistema nazionale di contact tracing" (perché c'è anche un problema connesso al funzionamento dei servizi cloud e al trasferimento di dati delicati che può avvenire al di fuori della UE: si sa che i dati nel cloud non sono fissi su server, ma possono risiedere in server diversi anche nel corso di una stessa giornata, e il problema della ubicazione dei server è una criticità che i Garanti privacy mondiali evidenziano fin dalle Conclusioni della Conferenza mondiale della privacy del 2012 in Uruguay). Tra l'altro non è chiaro - nella prospettiva della data retention - che fine fanno i dati oggetto di calcolo sui server in cloud, una volta che vi sia stato l'esito algoritmico: anche le politiche di conservazione e cancellazione dovrebbero essere chiarite da Bending Spoon. Reale anonimità del dato Altro ambito che mi piacerebbe approfondire: la reale anonimità del dato (penso ad esempio alla lista anonima dei contatti da caricare sul server). Spero che la app Immuni proceda ad implementare le tecniche di anonimizzazione che sono state ritenute valide dai Garanti Europei nel noto Parere 5/2014 sulle tecniche di anonimizzazione... Poco chiaro il flusso dei dati cittadino-medico È infine poco chiaro appare critico l'insieme dei flussi di comunicazione (inclusi i dati salvati solo in locale sul dispositivo ed inerenti il delicatissimo "diario clinico") tra cittadino che dovesse risultare positivo al test di Sars-Cov-2 e interrogatorio effettuato dal medico dotato di una sua versione della applicazione (di cui si sa parimenti poco): vanno approfondite le modalità relative alla possibilità di sbloccare volontariamente, con un codice, la lista dei contatti anonimizzati di chi ha incrociato per far arrivare una notifica a chi è a rischio contagio. Sul punto il Garante suggeriva nella sua recente audizione parlamentare che il soggetto risultato positivo dovrebbe fornire l'identificativo IMEI del dispositivo direttamente alla ASL di competenza che sarebbe poi tenuta a trasmetterlo a un server pubblico centrale per consentirgli così di ricostruire, tramite un calcolo algoritmico, i contatti tenuti con altre persone le quali si siano, parimenti, avvalse dell'app Bluetooth. Queste ultime - sempre seguendo i corretti suggerimenti del Garante privacy italiano (relatore dell'EDPB nella recente lettera sul contact tracing) riceverebbero poi una segnalazione (nella forma di un alert sul sistema) di potenziale contagio, con l'invito a sottoporsi ad accertamenti. In tal modo, il tracciamento sarebbe affidato a un flusso di dati pseudonimizzati, suscettibili di reidentificazione solo in caso di rilevata positività. E anche in tali circostanze, comunque, la stessa comunicazione tra server centrale (non in cloud) ed app dei potenziali contagiati avverrebbe senza consentirne la reidentificazione (proprio come richiesto dalla lettera dell'EDPB), così minimizzando l'impatto della misura sulla privacy

individuale.