L'INTERVISTA

di Luigi Garofalo 13 maggio 2020

Emilio Tosi (Univ. Milano-Bicocca): "App Immuni e tracciamento digitale? I rischi e le possibili migliorie"

Intervista all'avv. Emilio Tosi, Professore Associato abilitato di diritto privato - Università degli Studi di Milano Bicocca e Direttore Centro Studi Diritto delle Nuove Tecnologie®: " Bene escludere la geolocalizzazione dei singoli utenti, ferma restando l'ammissibilità della geolocalizzazione dei dati aggregati e anonimi".

Dati di prossimità e garanzia di anonimato nel modello operativo di **Immuni**, l'App prescelta dal Ministero dell'Innovazione per la sorveglianza sanitaria digitale: quali rischi e quali migliorie possibili in sede di conversione in legge. Ecco alcune domande che abbiamo rivolto al Prof. Avv. **Emilio Tosi**, Professore Associato

Abilitato di Diritto Privato – Università degli Studi di Milano Bicocca e Direttore Centro Studi Diritto delle Nuove Tecnologie - DNT®.

Key4biz. Entro quali limiti il diritto alla privacy può essere compresso da un'App di tracciamento dei contagi?

Emilio Tosi. Come ho già avuto modo di chiarire sempre sulle pagine di Key4Biz il diritto alla riservatezza e alla protezione dei dati personali sono diritti fondamentali sì, ma elastici, ossia possono essere compressi – temporaneamente – per ragioni di salute pubblica, come previsto dall'articolo 9.2 del GDPR e dall'art.15 della direttiva ePrivacy in un quadro di regole scritte dal Parlamento nel rispetto dei principi di bilanciamento degli interessi, proporzionalità, necessità, ragionevolezza, trasparenza e accountability.
È dunque al Parlamento – legislatore in via ordinaria – a cui in questa seconda fase della gestione della pandemia Covid- 19 occorre restituire la centralità prevista dalla Costituzione.
Come giustamente ricordato anche dal Pres. Prof.ssa Cartabia nella Relazione annuale 2019 della Corte Costituzionale, la nostra Costituzione "non contempla un diritto speciale per i tempi eccezionali(…) ma offre la bussola anche per navigare per l'alto mare aperto nei tempi di crisi, a cominciare proprio dalla leale collaborazione fra le istituzioni".
L'App in corso di implementazione, per quanto noto, dovrebbe essere compatibile con il GDPR e uniformata alle prescrizioni

rilasciate da EDPB nelle Linee-guida 04/2020 sull'uso dei dati di localizzazione e degli strumenti per il tracciamento dei contatti nel contesto dell'emergenza legata al COVID-19 oltre che del Garante nel Parere del 29 aprile 2020sulla proposta normativa per la previsione di una applicazione volta al tracciamento dei contagi da COVID-19.

Trasparenza, proporzionalità, minimizzazione dei dati e temporaneità sono principi tendenzialmente recepiti, seppur con qualche prospettiva di miglioramento in sede di conversione in legge, dal DL 28/20 e dovranno riflettersi necessarimente anche sulla regolamentazione attuativa dell'applicativo scelto dal Ministero dell'innovazione per la sorveglianza digitale.

A tale scopo risponde l'art 6 del DL 28/20 che statuisce, fra l'altro, quanto segue:

"Al solo fine di allertare le persone che siano entrate in contatto stretto con soggetti risultati positivi e tutelarne la salute attraverso le previste misure di prevenzione nell'ambito delle misure di sanita' pubblica legate all'emergenza COVID-19, e' istituita una piattaforma unica nazionale per la gestione del sistema di allerta dei soggetti che, a tal fine, hanno installato, su base volontaria, un'apposita applicazione sui dispositivi di telefonia mobile".

Key4biz. L'adozione di una App anticontagio a livello nazionale può avere effetti non desiderati?

Emilio Tosi. Si può creare un falso senso di sicurezza nei cittadini

nel caso in cui l'App non sia preceduta da adeguata campagna informativa nazionale e non sia supportata da adeguate misure tecnologiche, procedurali e organizzative.

Il rischio che si corre è quello di creare affidamento sociale incolpevole nella cittadinanza su uno strumento che da solo non è certo risolutivo.

Occorre essere chiari: nessun potere taumaturgico può essere associato al mero utilizzo dell'App.

Si tratta solo di un utile strumento complementare nel quadro complessivo delle azioni messe a terra dal Governo per il contrasto al Covid-19 che va ad integrare, non sostituire, il contact tracing analogico.

L'art- 6 del DL 28/20 precisa correttamente che:

"Le modalita' operative del sistema di allerta tramite la piattaforma informatica di cui al presente comma sono complementari alle ordinarie modalita' in uso nell'ambito del Servizio sanitario nazionale".

Questo al cittadino, si ribadisce, deve essere reso ben chiaro dalle Istituzioni attraverso campagna informativa ad hoc: altrimenti si rischia di ingenerare, corre l'obbligo di essere sottolineato nuovamente, una falsa percezione di sicurezza che potrebbe addirittura essere controproducente.

Inoltre, come ha giustamente osservato anche il Garante Soro in un suo recente intervento pubblico, la App senza test Covid massivi

(tamponi, test sierologici e test rapidi c.d. “pungidito”) – che ancora oggi sono somministrati con il contagocce – rischia di servire a poco o nulla.

Il Garante Soro pone correttamente un limite al tracciamento di massa delle persone osservando criticamente che sfugge l’utilità: “di una sorveglianza generalizzata alla quale non dovesse conseguire sia una gestione efficiente e trasparente di una mole così estesa di dati, sia un conseguente test diagnostico altrettanto generalizzato e sincronizzato”.

Non è prudente polarizzare, quindi, l’attenzione solo sulla App: si rischiano appunto effetti indesiderati.

Cito l’esempio per tutti dei falsi positivi e negativi. Anche l’EPDB raccomanda che tutte le procedure e i processi, compresi gli algoritmi implementati dalle App per il tracciamento dei contatti, debbano svolgersi “sotto la stretta sorveglianza di personale qualificato al fine di limitare il verificarsi di falsi positivi e negativi. In particolare, le indicazioni fornite in merito ai passi da compiere successivamente alla ricezione di un alert non dovrebbero basarsi unicamente su un trattamento automatizzato”.

Inoltre, si consideri che l’efficacia di un App di contact tracing può essere influenzata non solo dal numero di soggetti che decidono di istallarla (dato sensibilmente variabile dal 30% al 60% secondo varie analisi ad oggi disponibili) ma anche da eterogenei e non meno importanti fattori umani oltre che dai limiti intriseci della tecnologia prescelta: falsi positivi e falsi negativi, il non

uso, l'utilizzo non corretto e l'abuso costituiscono alcuni significativi esempi ostativi al successo di un App di tracciamento digitale dei contagi

Key4biz. Cosa ne pensa della possiblità di integrare dati di prossimità rilevati dal bluetooth e dati geolocalizzazione: potrebbe confliggere con il GDPR?

Emilio Tosi. Il Ministero dell'Innovazione ha chiarito di escludere l'utilizzo di dati relativi alla geolocalizzazione.

L'art. 6, comma 2 del DL 28/20 pervero attualmente esclude solo la geolocalizzazione dei singoli utenti:

"c) il trattamento effettuato per allertare i contatti sia basato sul trattamento di dati di prossimita' dei dispositivi, resi anonimi oppure, ove ciò non sia possibile, pseudonimizzati; è esclusa in ogni caso la geolocalizzazione dei singoli utenti;"

Non pare, quindi, ostativo, ribadisco, per il trattamento dei dati di geolocalizzazione aggregati.

Anche il Parere del Garante sull'App COVID-19 del 29 aprile 2020 è stato rlasciato positivamente sulla base del seguente assunto:

"e) selettività e minimizzazione dei dati: i dati raccolti devono poter tracciare i contatti stretti e non i movimenti o l'ubicazione del soggetto. Devono essere raccolti solo i dati strettamente necessari ai fini della individuazione dei possibili contagi, con tecniche di anonimizzazione e pseudonimizzazione affidabili. Anche la conservazione deve limitarsi al periodo strettamente necessario, da valutarsi sulla base delle decisioni dell'autorità sanitaria su

parametri oggettivi come il periodo di incubazione. A tal riguardo le disposizioni dello schema di norma su tali aspetti è opportuno che siano ulteriormente articolate in sede di attuazione dal Ministero della salute ai sensi del comma 2, anche con riferimento alla sorte dei dati raccolti sul dispositivo di chi, in un momento successivo all'installazione dell'applicazione, abbia poi deciso di disinstallarla".

Bene escludere la geolocalizzazione dei singoli utenti, ferma restando l'ammissibilità della geolocalizzazione dei dati aggregati e anonimi.

Certo dall'incrocio di dati di prossimità rilevati dai Bluetooth con i dati di geolocalizzazione del GPS dello smartphone l'anonimato dell'interessato si indebolisce progressivamente: bene quindi ha fatto il Ministero dell'Innovazione ad escludere tale possibilità.

Se poi aggiungiamo l'abbinamento delle prime due cifre del Cap (come ha annunciato De Rosa, il responsabile tecnologico del dipartimento della ministra Pisano, n.d.r.) l'indebolimento è ulteriore: più ampliamo il novero dei dati trattati più rendiamo fragile la tutela dell'anonimato dell'interessato rendendo non solo possibile ma anche più facile l'identificazione del soggetto vigilato.

Centrale in proposito – a prescindere dalle FAQ del Ministero dell'Innovazione che non hanno efficacia normativa ma solo informativa – sarà il sistema di garanzie dettagliate nella normativa regolamentare oltre a quanto rappresentato nella Valutazione di impatto del trattamento che dovrà essere rilasciata dal Ministero della Salute prima dell'inizio del trattamento con l'App prescelta.

Anche le Linee Guida EDPB raccomandano attenzione precisando che:

“L’anonimizzazione fa riferimento all’uso di una serie di tecniche finalizzate a eliminare la possibilità di collegare i dati a una persona fisica identificata o identificabile con uno sforzo “ragionevole”. Questo “test di ragionevolezza” deve tenere conto sia degli aspetti oggettivi (tempi, mezzi tecnici) sia di elementi di contesto che possono variare caso per caso (rarità di un fenomeno, la densità di popolazione, la natura e il volume dei dati). Se i dati non superano tale test, non sono anonimizzati e pertanto rientrano nel campo di applicazione del regolamento generale sulla protezione dei dati”.

E ancora la valutazione della robustezza della tecnica di anonimizzazione adottata dipende da tre fattori: (i) individuabilità (singling out) (possibilità di isolare una persona all’interno di un gruppo sulla base dei dati); (ii) correlabilità (possibilità di correlare due record riguardanti la stessa persona); (iii) inferenza (possibilità di dedurre, con probabilità significativa, informazioni sconosciute relative a una persona).

Infine, sempre EDPB, rileva correttamente che i dati relativi all’ubicazione ritenuti anonimipossono di fatto non esserlo. Le tracce di mobilità dei singoli individui sono caratterizzate intrinsecamente da forte correlazione e univocità. Pertanto, in determinate circostanze possono essere vulnerabili ai tentativi di re-identificazione: più incrociamo dati più aumentiamo il rischio di reidentificazione.

Key4biz. In sede di conversione in Parlamento del decreto-legge in quale altro modo più robusto si potrebbe legiferare per tutelare i dati dei cittadini?

Emilio Tosi. Innanzitutto, in conformità anche alle linee guida EDPB già citate, potrebbe essere resa più esplicita e chiara la filiera soggettiva degli attori coinvolti nel processo di istituzione e gestione della piattaforma unica nazionale evitando di utilizzare il sistema poco chiaro del rinvio ad altri testi normativi. L'art.6 – commi 1 e 5 – potrebbero essere riformulati in termini più chiari e trasparenti, intelleggibili anche al cittadino comune, trattandosi di intervento normativo interferente con diritti fondamentali della persona.

Si potrebbe essere più trasparenti – già in sede di conversione in Legge – in relazione all'esclusione dell'incrocio dei dati Bluetooth, GPS e CAP – ammesso e non concesso che alla fine vengano tutti utilizzati dalla nuova App – esplicitando le principali macromisure adottabili per prevenire il rischio di reidentificazione: misure dettagliate nella normativa attuativa.

Inoltre, esplicitare chiaramente quali dati saranno centralizzati e quali conservati anche o esclusivamente conservati nei dispositivi mobili dell'interessato.

In terzo luogo, si potrebbe esser più trasparenti anche sulla durata dell'emergenza: non credo sia opportuno indicare una data troppo breve sapendo di doverla prorogare.

Sebbene nulla si dice sulla possibilità di proroga della durata oltre e a quali condizioni.

Attualmente l'art. 6 comma 6 del DL 28/20 stabilisce che:

"L'utilizzo dell'applicazione e della piattaforma, nonche' ogni trattamento di dati personali effettuato ai sensi al presente articolo sono interrotti alla data di cessazione dello stato di emergenza disposto con delibera del Consiglio dei ministri del 31 gennaio 2020, e comunque non oltre il 31 dicembre 2020, ed entro la medesima data tutti i dati personali trattati devono essere cancellati o resi definitivamente anonimi".

La durata al 31/12/2020 potrebbe essere eccessivamente ottimistica e, quindi, non trasparente per i cittadini perché verosimilmente soggetta a proroga. Un termine massimo di 12 mesi dall'entrata in vigore potrebbe essere più appropriato: termine che il Ministro della Salute potrà certamente abbreviare nel caso in cui l'emergenza cessi prima di tale data.

Inoltre, andrebbe espressamente previsto che la reiterazione della durata del trattamento non potrà essere prorogata utilizzando lo strumento omnibus del milleproroghe ma con una legge ad hoc, occorrendo.

Come noto in Italia le situazioni temporanee sono suscettibili di protrarsi senza fine.

Ancora manca un tentativo di regolamentazione delle App regionali: oltre alla statuizione di principio che la piattaforma unica di allerta è nazionale potrebbe essere questo il contesto normativo appropriato per mettere ordine e meglio chiarire i limiti di operatività di analoghe

iniziative regionali prevedendo regole uniformi a tutela dei dati dei cittadini. Altrimenti si rischi il caos e l'insuccesso della stessa piattaforma nazionale.

Infine, occorere sviluppare la parte relativa agli obblighi informativi che non si esauriscono nell'ambito delimitato dell'informativa privacy richiesta dal GDPR ma che richiedono, invero, una specifica strategia di comunicazione e una campagna informativa, a beneficio della cittadinanza, che andrebbe attuata preliminarmente alla diffusione dell'App per un uso consapevole e per mitigare i rischi di false aspettative.

La mancanza di comunicazione pubblica efficace e di trasparenza può minare la fiducia delle persone, generare fallaci aspettative di sicurezza, affidamento incolpevole pericoloso per tutti i cittadini: sia per coloro che sceglieranno di utilizzarla sia per coloro che riterranno di poterne fare a meno.