DOI: 10.2436/15.2000.69.37

Seguretat informàtica i pandèmies

Josep Domingo-Ferrer[1]

Departament d'Enginyeria Informàtica i Matemàtiques
de la Universitat Rovira i Virgili

Les dades massives són útils per revelar patrons, tendències i associacions, especialment les relatives al comportament i a les interaccions dels humans en un context de pandèmia. Tanmateix, per tal de satisfer la legislació de protecció de dades i els valors ètics, la utilitat no pot ésser l'únic principi rector a l'hora de compartir i de publicar dades. El Reglament General de Protecció de Dades (RGPD) de la Unió Europea, que està esdevenint un estàndard global *de facto*, estableix uns quants requisits que constrenyen la recollida i la gestió d'informació identificable personalment (IIP). Aquests requisits tenen a veure amb els valors ètics següents: privadesa, autonomia, seguretat, equitat i transparència.

Les dades anonimitzades, és a dir, dades transformades de manera que no es puguin associar amb cap individu concret, tenen l'avantatge de no ésser subjectes a l'RGPD. Per tant, sempre que es pugui cal fer servir dades anonimitzades en comptes d'IIP.

Concretament, l'ús massiu de la geolocalització via telèfon mòbil per lluitar contra la COVID-19 ha estat molt eficaç a la Xina, a Corea del Sud i en altres països asiàtics. Ara bé, la geolocalització xoca amb els principis de l'RGPD. Segons el Consell Europeu de Protecció de Dades (European Data Protection Board, 2020), l'RGPD permet a les autoritats europees de processar dades personals dels ciutadans en el context d'una pandèmia, segons el que estableixin les lleis dels estats membres. Aquest Consell afirma que hom hauria d'anonimitzar sempre que fos possible les dades geolocalitzades fornides pels operadors de telecomunicació, de manera que els ciutadans als quals corresponen no siguin reidentificables. Sobre aquesta base és, doncs, perfectament acceptable de fer estudis de mobilitat aplicats a la lluita anti-COVID-19 amb dades de mobilitat anonimitzades.

1. A/e: *josep.domingo@urv.cat*.

En canvi, fer-ho amb les dades geolocalitzades sense anonimització que acumulen les companyies de telecomunicació és qüestionable: aquestes companyies les tenen amb el nostre consentiment (el contracte que hi hem signat) i, per tant, legalment, però no poden fer-ne processaments secundaris o transferir-les a tercers sense anonimització.

De tota manera, hi ha altres situacions sanitàries que requereixen l'ús d'IIP en algun moment. Aquest és, per exemple, el cas si cal rastrejar l'evolució dels pacients al llarg del temps i a través de diversos hospitals. Això és certament difícil de fer amb dades anonimitzades. Ara bé, aquesta mena d'estudis els fan els metges, i poden obtenir el consentiment explícit dels pacients afectats.

En canvi, les *aplis* COVID-19 de telèfon mòbil per rastrejar contactes poden funcionar sense recollir informació identificable personalment gràcies al protocol DP-3T (Troncoso *et al.*, 2020). Ara bé, malgrat això, l'adopció de les *aplis* de rastreig de contactes no té gaire èxit als països occidentals (Hsu, 2020; Savage, 2020). Creiem que aquest fracàs relatiu té raons tan tècniques com motivacionals:

— El protocol de comunicació que fan servir aquestes aplis és Bluetooth, que és incapaç de distingir si dues persones estan separades per una paret prima o no, per exemple. Aquesta incapacitat pot causar falsos positius: no és el mateix haver estat prop d'un positiu sense cap obstacle al mig que haver estat a la cambra del costat.

— El ciutadà té poca motivació per instal·lar i engegar una *apli* que només li pot portar males notícies (t'has de confinar o fer-te una prova), que a més poden ser falses (a causa de la probabilitat de fals positiu).

El ciutadà tindria més incentius si l'*apli* li oferís també estadístiques geolocalitzades o altra informació complementària (Nanni *et al.*, 2020-2021). Per exemple, si li digués quin és el risc de contagi a les zones per on passa o per on té pensat de passar.

En resum, per molt que es facin servir dades personals per a una bona causa (lluita contra la pandèmia), cal observar la legislació vigent i donar incentius adequats a la ciutadania perquè hi col·labori de grat.

Bibliografia

European Data Protection Board (2020). *Statement on the processing of personal data in the context of the COVID-19 outbreak* (19 de març).

Hsu, J. (2020) «Contact tracing apps struggle to be both effective and private». *IEEE Spectrum* (octubre), p. 56-59.

Nanni, M.; Andrienko, G.; Barabási, A.-L.; Boldrini, C.; Bonchi, F.; Cattuto, C.; Chiaromonte, F.; Comandé, G.; Conti, M.; Coté, M.; Dignum, F.;

Dignum, V.; Domingo-Ferrer, J.; Ferragina, P.; Giannotti, F.; Guidotti, R.; Helbing, D.; Kaski, K.; Kertesz, J.; Lehmann, S.; Lepri, B.; Lukowicz, P.; Matwin, S.; Megías-Jiménez, D.; Monreale, A.; Morik, K.; Oliver, N.; Passarella, A.; Passerini, A.; Pedreschi, D.; Pentland, A.; Pianesi, F.; Pratesi, F.; Rinzivillo, S.; Ruggieri, S.; Siebes, A.; Trasarti, R.; Van den Hoven, J.; Vespignani, A. (2020, 2021). «Give more data, awareness and control to individual citizens, and they will help COVID-19 containment». *Transactions on Data Privacy* 13(1), p. 65-66 and *Ethics and Information Technology*, to appear.

Reglament General de Protecció de Dades de la UE (2016) [en línia]: <https://gdpr-info.eu>

Savage, N. (2020) «Tracking COVID, discreetly». *Communications of the ACM*, 63(12), p. 9-11.

Troncoso, C., *et al.* (2020) «Decentralized Privacy-Preserving Proximity Tracing» (25 maig) [en línia]: <https://github.com/DP-3T/documents/blob/8240523d60e27f7d203a1a52992a71add7e83efc/DP3T%20White%20Paper.pdf>