COVID e sovranità tecnologica. Il ruolo delle applicazioni per il tracciamento dei contatti

Silvia Vidor

La pandemia da COVID-19 e le difficoltà gestionali ad essa connesse hanno portato molti Paesi europei, nel corso della prima metà del 2020, a sviluppare dei supplementi tecnologici alle tradizionali modalità di tracciamento dei contatti. Le app COVID sono state al centro di discussioni relative alle modalità di trattamento dei dati estremamente sensibili da esse raccolti; ma l'attenzione dedicata al tema della privacy ha oscurato l'impatto di queste applicazioni sul continuo conflitto per la sovranità tecnologica e su questioni di rilevanza strategica. Il ruolo fondamentale svolto dal sistema di notifica di Google e Apple e dal Contact Shield di Huawei in alcune app COVID europee, tra cui l'italiana Immuni, costituisce un potenziale rischio in virtù della sua natura di componente non pienamente controllato ma sempre attivo all'interno di un software ad ampio utilizzo tra la popolazione. La scelta di tutelare la privacy dei contagiati in quarantena (destinatari originali delle misure di tracciamento dei contatti) ha portato ad esporre i dati di tutti i cittadini ad un altissimo rischio strategico. Si rende dunque necessario valutare l'utilità di queste app su larga scala, anche considerando i dati scientifici riguardanti la loro efficacia (o meno) nel contribuire al contenimento della pandemia.

Introduzione

Lo stato di emergenza epidemiologica da COVID-19 sviluppatosi nel corso del 2020 ha contribuito fortemente alla diffusione delle tecnologie di comunicazione a causa delle restrizioni nel movimento imposte dalle autorità. Insieme a nuovi software di collaborazione e comunicazione online sono comparsi anche programmi più direttamente connessi alla gestione della pandemia stessa: le app COVID per il tracciamento digitale dei contatti. L'impiego di questo genere di applicazioni per smartphone non ha effetti riconducibili soltanto alla sfera della sanità pubblica, ma

costituisce altresì un nuovo elemento nell'ambito della discussione sulla sovranità tecnologica nell'Unione Europea e nei suoi Stati Membri.

La sovranità tecnologica

Il concetto di sovranità tecnologica è recentemente riemerso in connessione alla possibilità per l'UE di ricoprire un ruolo di leadership nel campo digitale. In particolare, a destare preoccupazione è l'ampia influenza esercitata delle aziende extra-europee nel settore e il loro accesso ai dati dei cittadini europei[1]. Il raggiungimento della sovranità tecnologica europea permetterebbe all'UE di svincolarsi almeno in parte dall'attuale dipendenza da aziende principalmente USA (es. Google, Apple) e cinesi (Huawei) in favore di aziende innovative con sede in uno o più Stati Membri. Al di là di questioni economiche, la ricerca della sovranità tecnologica riguarda "il controllo di dati, software, standard e protocolli, processi, hardware, servizi e infrastrutture"[2]. Per gli Stati, inoltre, vi è la possibilità di servirsi di realtà private per influenzare i processi regionali e globali dell'innovazione – ma anche per scopi politici e di intelligence, come hanno dimostrato gli scontri USA-Cina[3]. L'introduzione di applicazioni per il tracciamento digitale dei contatti si inserisce in queste dinamiche; per cercare di comprenderne le modalità, tuttavia, è necessario considerarne l'origine e il funzionamento.

Le App COVID

Il tracciamento dei contatti non è una pratica emersa con il diffondersi del COVID-19: in modalità prevalentemente analogica si tratta di un metodo già utilizzato nel controllo

---

[1] European Parliamentary Research Service, 'Digital Sovereignty for Europe', European Parliament, luglio 2020, https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf.

[2] Luciano Floridi, 'The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU', *Philosophy & Technology* 33 (2020): 370-1, DOI:10.1007/s13347-020-00423-6.

[3] Eric Geller, 'Trump signs order setting stage to ban Huawei from U.S.', *Politico*, 15 maggio 2019, https://www.politico.com/story/2019/05/15/trump-ban-huawei-us-1042046.

di malattie come l'AIDS[4]. Alcune caratteristiche peculiari del virus SARS-CoV-2, come la presenza di infetti asintomatici ma contagiosi, in aggiunta al calo nel numero di operatori sanitari dedicati al tracciamento e ai numeri rapidamente in crescita dei malati da COVID-19 nel corso della prima fase della pandemia, hanno tuttavia reso il tracciamento analogico una pratica insostenibile.

Tra i primi Paesi a tentare una strada diversa c'è stata la Corea del Sud. Come riportato dai *Korea Centers for Disease Control and Prevention*[5], fin dalla metà di febbraio 2020 il personale sanitario coreano integrava le informazioni ricevute dai pazienti in quarantena con dati GPS ottenuti dai cellulari dei malati, pagamenti con carta di credito e telecamere a circuito chiuso. Lo scopo di tale metodo era l'eventuale correzione di ricordi frammentari dei contagiati intervistati dal personale sanitario. A questo si sono aggiunte una serie di applicazioni per smartphone volte al monitoraggio di tali individui nel corso del loro periodo di isolamento[6]. Tuttavia, l'eccessiva invasività del metodo coreano – percepita come lesiva della privacy individuale – e le difficoltà connesse a un tracciamento dei contatti basato prevalentemente su modalità analogiche hanno spinto la maggior parte degli altri Paesi in un'altra direzione. In UE, gli Stati Membri hanno scelto di procedere nella creazione di app COVID per il tracciamento dei contatti tra le popolazioni intere, piuttosto che concentrarsi sugli individui in quarantena, nel tentativo di bilanciare la tutela della privacy dei cittadini con una più ampia efficacia nell'individuare i possibili contagiati e gli asintomatici. La decisione di espandere l'uso delle app COVID alla totalità dei cittadini ne costituisce un'evoluzione critica: se infatti il tracciamento di alcune centinaia o migliaia di individui in quarantena (peraltro

---

[4] Rita Rubin, 'Building an «Army of Disease Detectives» to Trace COVID-19 Contacts', *JAMA* 323, no. 23 (2020): 2357-60, DOI:10.1001/jama.2020.8880.

[5] Korea Centers for Disease Control & Prevention, 'Contact Transmission of COVID-19 in South Korea: Novel Investigation Techniques for Tracing Contacts', *Osong Public Health and Research Perspectives* 11, no. 1 (2020): 60-3, DOI:10.24171/j.phrp.2020.11.1.09.

[6] Max S. Kim, 'South Korea is watching quarantined citizens with a smartphone app', *MIT Technology Review*, 6 marzo 2020, https://www.technologyreview.com/2020/03/06/905459/coronavirus-south-korea-smartphone-app-quarantine/.

possibile sulla base delle limitazioni alla libertà individuale previste dalla legislazione attuale) solleva dibattiti sui rischi per la loro privacy, il tracciamento invasivo di decine di milioni di persone diventa invece una questione di rilevanza strategica – in particolare dato il coinvolgimento di aziende extraeuropee nella gestione dei dati.

Si prenda ad esempio il caso italiano. Il compito di sviluppare il tracciamento digitale dei contatti è stato affidato all'italiana Bending Spoons con l'app Immuni, lanciata nel giugno 2020, scaricata da oltre 10 milioni di persone e tuttora attiva[7]. In base al progetto presentato al Governo, il processo di tracciamento digitale dei contatti di Immuni è fondato sulla tecnologia Bluetooth, usata al fine di riconoscere le interazioni tra due dispositivi sui quali l'app è stata installata. I codici identificativi relativi a tali interazioni, cambiati più volte all'ora, sono cifrati e inviati alle autorità sanitarie solo in caso di esplicita autorizzazione del possessore del dispositivo nel momento in cui risultasse contagiato. In seguito a tale segnalazione, le persone entrate in contatto con un paziente positivo al SARS-CoV-2 vengono avvisate tramite apposita notifica dall'app[8]. Gli identificatori sono eliminati dopo 14 giorni. Immuni è tra le app COVID europee ad implementare il metodo "decentralizzato"[9], nel quale gli identificatori cifrati di dispositivo sono conservati nello *smartphone* stesso, in contrasto con il metodo "centralizzato", come quello impiegato dall'app francese, che prevede la conservazione degli identificatori su un server gestito dalle autorità pubbliche[10]. La raccolta dati è resa tuttavia possibile da due sistemi non europei: l'Exposure Notification di Google ed Apple, e il Contact Shield di Huawei.

---

[7] 'I numeri di Immuni', Immuni, ultimo accesso 30 marzo 2021, https://www.immuni.italia.it/dashboard.html.

[8] Ministero per l'Innovazione Tecnologica e la Digitalizzazione, 'Report sottogruppo di lavoro 6', GitHub, ultimo accesso 30 marzo 2021, https://github.com/taskforce-covid-19/documenti/blob/master/sgdl_6_Tecnologie_Governo_Emergenza/sgdl6_relazione_contact_tracing.pdf.

[9] 'Immuni's High-Level Description', GitHub, ultimo accesso 29 marzo 2021, https://github.com/immuni-app/immuni-documentation.

[10] Policy Department for Economic, Scientific and Quality of Life Policies, 'National COVID-19 contact tracing apps', European Parliament, maggio 2020, https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/652711/IPOL_BRI(2020)652711_EN.pdf.

App COVID e sovranità tecnologica

Nell'aprile 2020, i giganti tecnologici USA Google ed Apple hanno annunciato la decisione di contribuire congiuntamente ai tentativi di tracciamento digitale dei contatti tramite la creazione di un sistema di notifica basato su Bluetooth[11]. In assenza di tale sistema di notifica legato al sistema operativo, le app COVID non avrebbero la possibilità di mantenere l'accesso al Bluetooth a meno di mantenere l'applicazione sempre attiva sullo schermo dello *smartphone*, consumandone rapidamente la batteria. Un sistema simile è stato successivamente sviluppato dalla cinese Huawei per poter essere applicato negli *smartphone* di sua produzione[12]. La presenza quasi obbligata di tali sistemi per il funzionamento delle app COVID decentralizzate costituisce un rischio da valutare con cautela.

Le applicazioni di tracciamento digitale dei contatti rendono potenzialmente possibile l'accesso a una vasta quantità di dati sensibili relativi ai propri utenti. Il fatto che i dati trattati siano sottoposti ad un processo di cifratura non rappresenta necessariamente una tutela sufficiente: i sistemi di crittografia sono già stati bersaglio di misure governative nel tentativo di inserire *front-* o *backdoors* (o di sfruttare errori umani[13]) che permettano l'accesso su richiesta delle forze dell'ordine o delle agenzie di intelligence[14]. Va poi considerato che il sistema Google-Apple raccoglie comunque una quantità

[11] 'Apple and Google partner on COVID-19 contact tracing technology', Newsroom, Apple, ultima modifica 10 aprile 2020, https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/.

[12] 'Contact Shield', Huawei, ultimo accesso 31 marzo 2021, https://developer.huawei.com/consumer/en/doc/development/HMSCore-Guides-V5/contactshield--0000001057494465-V5.

[13] Ross J. Anderson, 'Whither Cryptography?', *Information Management & Computer Security* 2, no. 5 (1994): 13-20, DOI: 10.1108/09685229410792961.

[14] Susan Landau, 'Making Sense from Snowden: What's Significant in the NSA Surveillance Revelations', *IEEE Security and Privacy* 11, no. 4 (2013): 54-63, DOI:10.1109/MSP.2013.90.

considerevole di dati relativi ai suoi utenti[15]. Dal lato server, né il sistema Google-Apple né quello di Huawei sono *open source*[16] – il che rende significativamente più complesso verificarne il funzionamento, le modalità di raccolta e trattamento dati, e la presenza di eventuali vulnerabilità o *backdoor* attivabili con un aggiornamento. Il rischio è quello di un passaggio di considerevoli quantità di dati impiegabili a fini di intelligence dai privati che gestiscono le tecnologie in questione ai governi dei Paesi nei quali tali aziende hanno sede, che sia su base volontaria o costrittiva (ad esempio attraverso le cosiddette "FISA letters" negli USA[17], o tramite la Legge Nazionale sull'Intelligence del 2017 in Cina[18]).

L'implicazione fondamentale dell'adozione di queste tecnologie per le sovranità tecnologiche italiana ed europea è una perdita di controllo sui dati dei propri cittadini. La scelta di applicare il tracciamento dei contatti a popolazioni intere piuttosto che limitarlo ai contagiati in quarantena, contrariamente al modello sudcoreano, espande tale rischio potenzialmente ai dati di tutti i cittadini, anche considerando i ripetuti inviti

---

[15] Douglas J. Leith, Stephen Farrell, 'Contact Tracing App Privacy: What Data Is Shared By Europe's GAEN Contact Tracing Apps', 18 luglio 2020, https://www.scss.tcd.ie/Doug.Leith/pubs/contact_tracing_app_traffic.pdf.

[16] Con sistemi *open source* si intendono generalmente software caratterizzati da una licenza che permette la modifica, l'uso e la redistribuzione del loro codice sorgente. Tipicamente, il codice sorgente dei sistemi *open source* è disponibile su Internet, fatto che ne permette l'analisi da parte dei visualizzatori. Per una panoramica di vantaggi e svantaggi dei sistemi *open source*, si rimanda alla bibliografia di seguito:

Fitzgerald, Brian. 'The Transformation of Open Source Software.' *MIS Quarterly* 30, no. 3 (settembre 2006): 587-98. DOI: 10.2307/25148740.

Gacek, Cristina, and Budi Arief. 'The many meanings of open source.' *IEEE Software* 21, no. 1 (gennaio-febbraio 2004): 34-40. DOI: 10.1109/MS.2004.1259206.

Hoepman, Jaap-Henk, and Bart Jacobs. 'Increased security though open source.' *Communications of the ACM* 50, no. 1 (gennaio 2007): 79-83. DOI: 10.1145/1188913.1188921.

Massacci, Fabio, and Ivan Pashchenko. 'Technical Leverage: Dependencies Are a Mixed Blessing.' *IEEE Security & Privacy* 19, no. 3 (maggio-giugno 2021): 58-62. DOI: 10.1109/MSEC.2021.3065627.

[17] Congressional Research Service, 'Foreign Intelligence Surveillance Act (FISA): An Overview', U.S. Congress, ultima modifica 6 aprile 2021, https://crsreports.congress.gov/product/pdf/IF/IF11451.

[18] Murray S. Tanner, 'Beijing's New National Intelligence Law: From Defense to Offense', *Lawfare*, 20 luglio 2017, https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense

a scaricare le app COVID per migliorarne l'ipotetica efficacia. Ciò è avvenuto nonostante ad oggi non sia stato ancora dimostrato il contributo positivo di applicazioni come Immuni nel limitare la diffusione del COVID-19, mentre soltanto una frazione minima dei contagiati è individuata tramite le app[19].

Conclusione

La diffusione delle app COVID ha rappresentato un tentativo di gestione della pandemia attraverso strumenti tecnologici che potessero aumentare l'efficacia del tracciamento dei contatti senza la necessità di impiegare operatori sanitari. Tuttavia, la loro potenziale inefficacia è fonte di ulteriori dubbi riguardo la necessità di esporre la sovranità tecnologica europea ai rischi derivanti dalla dipendenza da tecnologie straniere (già sollevati in passato in relazione ai componenti dei sistemi d'arma[20]), che diventano sempre più critici con l'aumentare della diffusione di tali tecnologie tra gli utenti europei. La decisione di tracciare milioni di cittadini invece che limitare l'invasività ai quarantenati seguendo il modello sudcoreano, in particolare, porta i problemi connessi all'uso delle app COVID a un alto livello di rischio strategico che avrebbe reso necessaria una valutazione più prudente in sede di scelta del miglior metodo da adottare per il tracciamento digitale dei contatti. L'inclusione dei sistemi di notifica Google-Apple e Huawei nelle app sviluppate dai vari Stati europei (dovuta all'ampia presenza di tali aziende nel settore degli *smartphone*), così come l'idea del tracciamento digitale dei contatti esteso a tutti i cittadini, devono essere ripensate in un'ottica che consideri le conseguenze sul piano strategico e di sicurezza. Le app COVID sono l'ennesimo segnale di una società europea sempre più fondata sul digitale, ma ancora basata su tecnologie straniere sulle quali non può permettersi di fare pieno affidamento.

---

[19] Immuni, 'I numeri di Immuni'.

[20] Martin Edmonds, Matthew Uttley and George Hayhurst, 'UK and US dependence on foreign technology in
defence research and development', *Science and Public Policy* 17, no. 3 (1990): 157-169, DOI:10.1093/SPP/17.3.157.

SILVIA VIDOR è assegnista di ricerca presso il Dipartimento di Ingegneria e Scienza dell'Informazione dell'Università degli Studi di Trento. Laureata con lode in International Security Studies presso la Scuola Superiore Sant'Anna di Pisa e l'Università di Trento, i suoi interessi di ricerca riguardano la sicurezza cibernetica, la privacy e la governance delle nuove tecnologie. Questo lavoro è stato supportato in parte dal Framework H2020 dell'Unione Europea tramite i progetti n° 770138 (OPTICS2) e 830929 (CyberSec4Europe).
