Virus e tecnologia: perché sono importanti scelte etiche

Mariarosaria Taddeo

[1] Oxford Internet Institute, University of Oxford, UK

[2] Alan Turing Institute, London, UK

mariarosaria.taddeo@oii.ox.ac.uk

La lotta al Covid-19 è un acceleratore della transizione digitale. Perche' questa sia umanamente ed ecologicamente sostenibile è necessaria tuttavia una governance della tecnologia che tenga conto di problemi ancora irrisolti come la protezione della privacy di gruppo, il divario digitale, il ruolo e le responsabilità delle aziende fornitrici di servizi digitali. Si tratta di opportunità che le società, chiamate a ripensare sé stesse dopo la pandemia, non possono sprecare.

*"Chi vive di digitale, muore di digitale" (Floridi 2014). Così il filosofo Luciano Floridi ha evidenziato le potenziali minacce poste dalla sicurezza informatica alle società dell'informazione (mature), che dipendono (si aspettano di poter dipendere) dalle tecnologie digitali per funzionare e prosperare (Floridi 2016). Oggi, mentre la pandemia di Covid-19 imperversa nel mondo, sembra che chi vive di digitale possa anche salvarsi per via del digitale. Il ruolo salvifico del digitale può essere letto sia metaforicamente, sia letteralmente. In senso metaforico, il digitale ci salva perché in tempi di emergenza non è solo uno strumento conveniente, ma è necessario per consentire alle società di continuare a funzionare, sostenendone le attività sociali ed economiche. In senso letterale, le tecnologie digitali facilitano il monitoraggio, il tracciamento e la prevenzione dei contagi, risultando dunque fondamentali presidi di salute pubblica (Ting et al. 2020).

Che sia metaforico o letterale, il potenziale benefico del digitale durante una pandemia comporta però seri rischi etici. Si consideri, ad esempio, l'uso di tecnologie digitali per tracciare la diffusione del virus. Ad oggi, sono 59 gli Stati che usano sistemi digitali a questo fine. Il numero è destinato a crescere, perché altri paesi stanno sviluppando soluzioni analoghe.[1] Questi sistemi si affidano spesso ai dati trasmessi dai telefoni cellulari per tracciare gli spostamenti e i contatti delle persone. Qui subentrano seri rischi etici, legali e sociali, che vanno dalla divulgazione di dati personali alla costruzione di sistemi di sorveglianza di massa capaci di ledere seriamente le libertà civili e i diritti umani (Taddeo 2014).

* Questo articolo e' stato pubblicato da Aspenia (89), Aspen Institute Italia, June 2020, www.aspeninstitute.it

[1] Samuel Woodhams, "COVID-19 Digital Rights Tracker", *Top10VPN*, 20/3/2020

Da quando i governi nazionali hanno cominciato a prendere in considerazione l'uso dei sistemi di monitoraggio e tracciamento, è sorto un acceso dibattito sulle implicazioni etiche, legali e sociali di questi sistemi. Il dibattito ha spinto molti governi a scegliere metodi e sistemi che minimizzano la raccolta dei dati e proteggono la privacy individuale (la maggior parte delle soluzioni usa dati legati al Bluetooth invece di dati legati al Gps o al WiFi) e riducono le minacce alla sicurezza e mitigano il rischio di una sorveglianza di massa. Per esempio, utilizzando protocolli distribuiti come il Decentralized Privacy-Preserving Proximity Tracing (Tracciamento di prossimità decentrato che tutela la privacy), o DP-3T.[2]

Il dibattito sui risvolti etici, legali e sociali dei sistemi di monitoraggio digitali non si è sviluppato in un vuoto giuridico e normativo. In ambito di Unione Europea, ad esempio, l'articolo 5 del Regolamento generale sulla protezione dei dati (GDPR) prescrive di contenere al massimo i dati raccolti, mentre l'articolo 9 regolamenta la raccolta e l'uso di dati personali in casi di gravi minacce per la salute di carattere internazionale. Similmente, i principi che informano la decisione di limitare i diritti umani per contrastare la pandemia sono rinvenibili nella Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, nella Convenzione internazionale sui diritti civili e politici delle Nazioni Unite e nei Princìpi di Siracusa delle Nazioni Unite (Morley et al. 2020b).

I tre documenti, letti congiuntamente, rimarcano che qualsiasi misura volta a limitare i diritti umani in tempo di crisi deve restare nell'ambito della legalità e dev'essere:

> "*must be necessary, proportional, scientifically valid and time- bound. These principles are derived from the European Convention on Human Rights, the International Covenant on Civil and Political Rights (ICCPR) and the United Nations Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights that limit how the ICCPR can be applied*" (Morley et al. 2020a).

Mancava una traduzione di questi princìpi in linee-guida etiche che potessero essere usate per guidare la progettazione, lo sviluppo e l'uso dei sistemi di monitoraggio e tracciamento. Ecco perché, insieme ad altri ricercatori – Jessica Morley, Josh Cowls e Luciano Floridi – del Digital Ethics Lab dell'Università di Oxford, abbiamo definito una *framework* entro cui concepire, sviluppare e applicare tali sistemi in modo eticamente giustificabile (Morley et al. 2020a). Il *framework* si basa sui quattro principi fondamentali tratti dai documenti sopracitati e si articola in sedici requisiti che i sistemi devono soddisfare per essere eticamente giustificati.

Gli apparati di monitoraggio e tracciamento che non soddisfano queste caratteristiche non andrebbero usati. A parte i rischi per i diritti umani, essi pongono seri problemi a breve e lungo termine per le nostre società. Nell'immediato, il rischio più grande e quello posto dai costi di opportunità: molti cittadini potrebbero giustamente rifiutare di usare sistemi che ne ledono i diritti. In questo caso, gli apparati sarebbero un fallimento, vanificando così il tempo, gli sforzi e i mezzi investiti, a svantaggio di soluzioni alternative e migliori. Alla lunga, dispiegare sistemi di monitoraggio e tracciamento non etici

[2] https://github.com/DP-3T/documents

mette in moto processi che rischiano di minare stabilmente i diritti e i valori fondanti delle nostre società e che saranno difficili da smantellare una volta superata la crisi. Nel complesso, i problemi di breve e lungo termine possono erodere la fiducia dei cittadini nei governi e nelle istituzioni pubbliche (Primiero and Taddeo 2012; Taddeo 2017).

I suddetti rischi non riguardano tanto i singoli individui, quanto le società nel loro insieme. Ecco perché è di cruciale importanza sviluppare una *governance* etica della sfera digitale, conciliando diritti e rischi dei singoli con i rischi e le opportunità sociali. Sinora, il dibattito sui sistemi in questione si è incentrato (con successo) sull'impatto individuale, ma restano seri problemi sociali che attendono soluzioni urgenti. I più pressanti sono tre: la protezione della *privacy di gruppo* (Luciano Floridi 2014); il divario digitale; il ruolo e le responsabilità delle aziende che forniscono servizi digitali, come Apple e Google (Taddeo and Floridi 2015; 2017). Questi problemi preesistono alla pandemia, ma l'uso crescente delle tecnologie digitali per gestire la crisi li ha esacerbati, rendendo urgente affrontarli.

Privacy di gruppo. Cominciamo dalla privacy di gruppo, che nella definizione di Floridi è

> "un diritto attribuito ad un gruppo, più che ai singoli membri dello stesso. È il gruppo, non i suoi membri singolarmente presi, ad essere correttamente identificabile come il soggetto del diritto. Un tipico esempio è il diritto all'autodeterminazione, detenuto da una nazione nel suo insieme" (Floridi 2014, 1).

La protezione della privacy di gruppo è fondamentale nell'era del big data e dell'intelligenza artificiale, dove la raccolta dei dati è spesso finalizzata a determinare categorie, gruppi di individui, piuttosto che singole persone. La profilazione commerciale, ad esempio, si basa sull'identificazione di gruppi (chi predilige vino rosso; chi ascolta musica folk-rock; quelli che vivono nel Regno Unito) e prescinde dal singolo individuo (Mariarosaria). Tuttavia, questa pratica pone seri problemi circa il corretto trattamento dei gruppi che identifica. I casi infausti degli algoritmi di Google che profilano gli utenti a seconda dal genere uomo/donna e mostrano offerte di lavoro altamente retribuite più spesso agli uomini che alle donne, o che propongono servizi di controllo della fedina penale quando si fanno delle ricerche che includono nomi o cognomi tipicamente afroamericani, ne sono esempi lampanti. [3]

Nel caso dei dati raccolti per contrastare la pandemia, i gruppi potrebbero includere gli infettati, chi piange qualcuno ucciso dal virus, chi ha usato la app di tracciamento e chi no, chi ha visitato un parco in un determinato giorno, l'intera popolazione di un paese, di una città, di una regione o finanche di una nazione. I dati aggregati sono fondamentali per contrastare la pandemia e guidare le decisioni dei governi, ad esempio dove e quando allentare le misure restrittive, ma se usati male possono portare a discriminazioni o a decisioni eticamente problematiche. Pertanto, è cruciale che le politiche e i regolamenti a tutela della privacy siano estesi oltre l'identificazione dei singoli (privacy individuale) a ricomprendere anche le categorie (privacy di gruppo), per proteggere la privacy e, più in generale, i diritti

[3] Julia Carpenter, "Google's algorithm shows prestigious job ads to men, but not to women", *Independent*, 7/7/2015.

dei gruppi delineati mediante l'uso di queste informazioni. La lotta ai virus, specialmente in caso di pandemia, ci insegna che la protezione del gruppo (l'immunità di gregge) è essenziale per salvare i singoli individui. Nell'era dei big data e dell'intelligenza artificiale, questa è una lezione che vale anche per i diritti.

Il *digital divide*. Un recente studio condotto nel Regno Unito stima che nel 2018 solo il 20% dei britannici possedeva nessuna o scarse capacità di usare internet per svolgere compiti semplici, come spedire una e-mail. Un altro studio riporta che nel corso del 2019, in Italia, il 67,9% della popolazione ha effettuato almeno un accesso a Internet. Questi dati mostrano che Italia e Regno Unito sono società dell'informazione mature, i cui membri vivono onlife: non sono mai solo online, ma non sono neanche mai totalmente offline.

Tuttavia, se si leggono questi dati nell'ottica dei sistemi di monitoraggio e tracciamento con fini di salute pubblica, emerge che ampie fette della popolazione (il 21% dei britannici e il 29% degli italiani) risulterebbero escluse dall'accesso a servizi sanitari digitalizzati. Nelle società dell'informazione mature, il divario digitale diventa una vera barriera che si erge tra settori rilevanti della popolazione e servizi fondamentali (sanità, ma anche istruzione, lavoro e interazioni sociali). Un muro che potrebbe impedire l'equa distribuzione delle opportunità e il rispetto dei diritti fondamentali, come quello alla salute. Servono dunque misure volte ad ampliare la distribuzione e l'accesso alle tecnologie digitali e a promuovere l'alfabetizzazione digitale, per assicurare che servizi di base, ormai digitalizzati, siano accessibili a tutti. Allo stesso modo, se i sistemi di monitoraggio e tracciamento dei contagi si riveleranno efficaci, sarà cruciale disporre misure per renderli accessibili anche a quanti hanno uno scarso livello di alfabetizzazione digitale.

Il ruolo dei *providers*. Infine, consideriamo il ruolo delle aziende che forniscono servizi digitali, nel caso specifico Apple e Google. Le due aziende hanno acconsentito a creare insieme un'interfaccia di programmazione (API) per applicazioni di tracciamento dei contatti basate sulla tecnologia Bluetooth, installate sui telefoni con software iOS (Apple) e Android (Google). La collaborazione è cruciale per il successo delle app governative di tracciamento, perché assicura che esse funzionino bene su entrambi i sistemi operativi, favorendone dunque l'uso da parte degli cittadini. Il che è a sua volta fondamentale, perché i sistemi di tracciamento risultano efficaci se li usa almeno il 50-70% della popolazione.[4]

La collaborazione Apple-Google non va inquadrata solo sotto il profilo tecnico. Le scelte ingegneristiche operate in sede di programmazione non sono eticamente neutre e condizionano le applicazioni sviluppate sulla base della loro API. Al riguardo, va notato che la crescente adesione dei governi europei al protocollo DP-3T segue alla decisione di Google e Apple di usarlo per la loro API. Tutto bene, nella misura in cui il protocollo DP-3T garantisce maggiori protezioni per la privacy individuale rispetto ai protocolli centralizzati. Tuttavia, fa riflettere che siano stati le due aziende, non le autorità pubbliche, a scegliere

[4] Mariangela Celiberti, "Immuni app: cos'è, come funziona, dove scaricarla, uscita Android e iOS", *Italian Times*, 3/5/2020.

come sviluppare gli strumenti da cui potrebbero scaturire i sistemi di tracciamento (le app) promossi dai governi.

Lo sforzo congiunto di Apple e Google per sostenere la sanità pubblica in tempi di pandemia dev'essere benvenuto. Non va però trascurato il ruolo centrale giocato oggi dai fornitori di servizi digitali, che concepiscono e gestiscono infrastrutture e servizi chiave senza i quali le società (mature) dell'informazione non potrebbero funzionare e prosperare. A partire da questa collaborazione, dovremmo cominciare a valutare attentamente il ruolo che questi soggetti svolgono e dovrebbero svolgere nelle nostre società, le responsabilità morali connesse a tale ruolo, il modo di regolamentarli e come includerli nei processi di *governance* della sfera digitale. Queste non sono domande nuove, per esempio occupano un posto centrale nel dibattito accademico sull'Etica del Digitale. Tuttavia, la sfera politica e governativa ha faticato sin qui ad affrontarle. Nella crisi attuale, la mancanza di risposte coerenti a queste domande ha lasciato i governi nazionali e sovranazionali senza una guida su come interagire con le aziende che forniscono servizi digitali, che senza il loro supporto sarebbero spesso inattingibili.

In una bozza del documento sul Futuro digitale dell'Europa filtrata alla stampa, il Consiglio Europeo afferma che gli Stati membri dell'UE dovrebbero "analizzare attentamente le esperienze maturate durante la pandemia di Covid-19" per plasmare le future politiche in materia di capacità digitali, concentrandosi specialmente su ambiti quali "gli strumenti online per la salute, l'alfabetizzazione digitale, le applicazioni digitali nella pubblica amministrazione, la condivisione dei dati e la connettività a banda larga".[5] Tutto giusto, ma non basta. Qualsiasi politica per il governo della sfera digitale dovrà, per essere efficace, incorporare linee guida etiche. Prima che vivere e morire di digitale, o esserne salvati, le nostre società ne sono trasformate. Questa trasformazione è profonda, duratura, e potrebbe causare gravi conseguenze negative. Servono criteri etici per assicurare che la transizione digitale sia umanamente ed ecologicamente sostenibile, specie oggi che le società sono chiamate a ripensare sé stesse dopo la pandemia.

Bibliografia

Floridi, Luciano. 2014. *The Fourth Revolution, How the Infosphere Is Reshaping Human Reality*. Oxford: Oxford University Press.

Floridi, Luciano. 2014. 'Open Data, Data Protection, and Group Privacy'. *Philosophy & Technology* 27 (1): 1–3. https://doi.org/10.1007/s13347-014-0157-8.

Floridi, Luciano. 2016. 'Mature Information Societies—a Matter of Expectations'. *Philosophy & Technology* 29 (1): 1–4. https://doi.org/10.1007/s13347-016-0214-6.

Morley, Jessica, Josh Cowls, Mariarosaria Taddeo, and Luciano Floridi. 2020a. 'Ethical Guidelines for COVID-19 Tracing Apps'. *Nature* 582: 29–31.

Morley, Jessica, Josh Cowls, Mariarosaria Taddeo, and Luciano Floridi. 2020b. 'Ethical Guidelines for SARS-CoV-2 Digital Tracking and Tracing Systems'. *SSRN Electronic Journal.* https://doi.org/10.2139/ssrn.3582550.

[5] Samuel Stolton, "LEAK: EU in push for digital transformation after COVID-19 crisis", *EurActiv*, 6/4/2020.

Primiero, Giuseppe, and Mariarosaria Taddeo. 2012. 'A Modal Type Theory for Formalizing Trusted Communications'. *Journal of Applied Logic* 10 (1): 92–114. https://doi.org/10.1016/j.jal.2011.12.002.

Taddeo, Mariarosaria. 2014. 'The Struggle Between Liberties and Authorities in the Information Age'. *Science and Engineering Ethics*, September, 1–14. https://doi.org/10.1007/s11948-014-9586-0.

Taddeo, Mariarosaria. 2017. 'Trusting Digital Technologies Correctly'. *Minds and Machines* 27 (4): 565–68. https://doi.org/10.1007/s11023-017-9450-5.

Taddeo, Mariarosaria, and Luciano Floridi. 2015. 'The Debate on the Moral Responsibilities of Online Service Providers'. *Science and Engineering Ethics*, November. https://doi.org/10.1007/s11948-015-9734-1.

Taddeo, Mariarosaria. 2017. 'The Moral Responsibilities of Online Service Providers'. In *The Responsibilities of Online Service Providers*, edited by Mariarosaria Taddeo and Luciano Floridi, 31:13–42. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-47852-4_2.

Ting, Daniel Shu Wei, Lawrence Carin, Victor Dzau, and Tien Y. Wong. 2020. 'Digital Technology and COVID-19'. *Nature Medicine* 26 (4): 459–61. https://doi.org/10.1038/s41591-020-0824-5.