Minds and Machines (2020) 30:171–176
https://doi.org/10.1007/s11023-020-09528-5

EDITORIAL

The Ethical Governance of the Digital During and After the COVID-19 Pandemic

Mariarosaria Taddeo[1,2]

Published online: 12 June 2020

"Those who live by the digit, die by the digit" (Floridi 2014a), stresses Floridi to highlight that cybersecurity risks pose serious threats to (mature) information societies (Floridi 2016)—societies that (expect to be able to) depend on digital technologies to function and prosper. These days, while the COVID-19 pandemic scourges the world, it seems that those who live by the digit *may* also be saved by the digit. This is true both metaphorically and literally. Metaphorically, in times of crisis the digital is not just convenient, it is a necessary enabler for societies to function, as it sustains social and economic activities. The phrase also works literally, for digital technologies support scientific research working on the virus and facilitate public-health approaches to monitor, detect, and prevent the spreading of SARS-CoV-2 (Ting et al. 2020).

Whether understood metaphorically or literally, the potential for good of digital technologies in time of a pandemic poses some serious ethical risks both for individual and societies. Consider, for example, the use of digital technologies to track the spreading of the virus. At the time of writing, 60 countries are using some form of digital tracking and tracing systems (DTTS) to this end.[1] This number will grow, as more countries are developing similar measures. DTTS often rely on smartphones' data to track people's locations and contacts. This poses legal and ethical risks, ranging from pervasive (and excessive) access to individuals' personal data to forms of mass-surveillance, which put human rights and civil liberties under a sharp devaluative pressure (Taddeo 2014).

As the use of DTTS started to be considered, a wide debate on the ethical, legal, and social implication (ELSI) of these systems has emerged. Eventually, this debate has helped to inform the choice of governments to use methods and protocols that minimise data collection and protect individual privacy (most DTTS use Bluetooth data rather than GPS or WiFi data), reduce security threats, and mitigate the risks

[1] https://www.top10vpn.com/research/investigations/covid-19-digital-rights-tracker/.

✉ Mariarosaria Taddeo
mariarosaria.taddeo@oii.ox.ac.uk

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

[2] Alan Turing Institute, London, UK

for mass surveillance by implementing decentralised protocols—such as Decentralized Privacy-Preserving Proximity Tracing (DP-3T).[2]

The debate on the ELSI of DTTS has also shown that the use of digital technologies to tackle the pandemic does not occur in a vacuum of regulations and principles.

> "[A DTTS] 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. 2020), emphasis added).

Elsewhere, together with other members (Jessica Morley, Josh Cowls and Luciano Floridi) of the Digital Ethics Lab of the University of Oxford, we defined a framework to guide the design, development, and use of DTTS in an *ethically justifiable* way (Morley et al. 2020). The framework rests on the principles extracted from the aforementioned documents and specifies 16 factors that DTTS have to meet to be ethically justified. The factors are designed to answer the validation and verification questions - 'are we building the right DTT system?' and 'are we building the DTT system in the right way?' - identified in (Floridi 2020).[3]

DTTS that are not ethically justifiable should not be deployed. Aside from the threat to human rights, they pose severe short- and long-term problems. As argued in (Morley et al. 2020), in the short-term, they may present a huge opportunity cost. Individuals are likely reject any DTTS that encroach upon their rights wasting the time, efforts and resources invested in developing the specific system, and which could have been used to develop alternative and better solutions. In the long-term, deploying non-ethically justified DTTS will put in place processes which risk undermining fundamental values and rights of our societies and may be difficult to revert after the pandemic. Taken together, the short- and the long-term problems may erode citizens' trust in governments and public institutions (Primiero and Taddeo 2012; Taddeo 2017a, b; Floridi 2020).

So far, the debate on DTTS has focused on their impact on individuals and their rights, but short- and long-term problems with DTTS concern societies at large and the governance of digital technologies. This is evident when considering the impact of DTTS on *group* privacy (Floridi 2014a, b); the digital divide and social justice in information societies (see also Floridi 2020); and the role and responsibilities of online service providers (OSPs), like Apple and Google (Taddeo and Floridi 2015, 2017). While all these problems existed before the pandemic, the growing reliance of digital technology to tackle the crisis has exacerbated the need to address them.

Let me begin with group privacy. This is:

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

[3] Ethical guidelines for the ethical use of DTTS have also been provided by the World Health Organisation, https://www.who.int/publications-detail/WHO-2019-nCoV-Ethics_Contact_tracing_apps-2020.1.

> "Privacy as a group right is a right held by a group as a group rather than by its members severally. It is the group, not its members, that is correctly identified as the right-holder. A typical example is the right of self-determination, which is held by a nation as a whole" (Floridi 2014a, b, 1).

The protection of group privacy is crucial in the age of big data and artificial intelligence, where data collection is often finalised to identify categories, *groups*, of individuals rather than to single out a specific person. Consider commercial profiling, for example, it rests on the identification of groups (e.g. those who like Amarone or rock-folk music, those who live in the UK), and is independent from the identification of a specific data subject (e.g. Mariarosaria). Nonetheless, profiling poses serious problems with respect to the fair treatment of the groups that it identifies. The nefarious case the Allegheny Family Screening Tool used to assess the risk of child abuse and referring African-American and biracial families to court three times more often than white families offers a good example of the case in point.[4]

In the case of the pandemic-data, groups may include those who were infected; those who bear mourning due to COVID-19; those who used the tracking app, or those who did not; those who walked in a park on a given day or the whole population of a block; town; a city; a region; even a country. Data on groups are key to tackle the pandemic and drive governmental decisions, like when and where to lift restrictive measures, but they can also lead to new forms of unfair treatment for the members of these groups. For this reason, it is crucial that privacy-focused policies and regulations extend their scope beyond the protection of identification of individuals (individual privacy) to include also the identification of categories of individuals (group privacy) to protect the rights and ensure fair treatment of these groups. This is why, regulation should be in place to ensure that data collected by any DTTS during the pandemic will be deleted once the crisis will be overcome and to guarantee that access to any related aggregated and anonymised data will be strictly regulated and permitted only for scientific purposes.

Focus now on the digital divide. Eurostat reports that in 2018, in EU-28 (henceforth the Eurozone) an average of 76% of individuals accessed the internet daily.[5] These data confirm that the Eurozone hosts information societies, albeit with different degrees of maturity. This is also the case of the UK and Italy. The two countries of the Eurozone with the highest levels of deaths attributed to the COVID-19 and where a DTTS may be deployed soon to tackle the pandemic while the lockdown is lifted.[6] A UK study estimates that in 2018, only 20% of people in the UK have between zero to limited abilities to use the internet to perform simple tasks, like sending an email. In Italy, a study reports that 67.9% of the overall population accessed internet at least once in 2019.

[4] https://www.wired.com/story/excerpt-from-automating-inequality/.

[5] https://ec.europa.eu/eurostat/statistics-explained/index.php/Digital_economy_and_society_statistics_-_households_and_individuals#Internet_access.

[6] https://www.worldometers.info/coronavirus/.

When reading these data with respect to access to, and use of, DTTS and other digital health services that require access to the internet, they reveal that big parts of the population (20% of the whole population in the UK, 32.1% of the Italian population, and 24% over the Eurozone) are likely to be excluded from these services, even when these are key to protect public health. The same percentage of the population is also excluded from digital services that support education, professional opportunities, and social interactions. In information societies, the digital divide is a concrete separation between big parts of the population and key services. It jeopardises the fair distribution of opportunities and the respect of fundamental rights, like the right to health.

So far the debate on the digital divide has been addressed only tangentially, as the discussion focused on the lower possible adoption rate necessary to the success of the DTTS, and different figures have been proposed ranging from 'as long as [we] have a two-digit figure' to 56% of the overall population (Servick 2020). However, if DTTS are effective in limiting the spread of the infections, then bridging the divide and enable access and ability to use digital technology for all sectors of society becomes an even more pressing problem. Measures designed to enable those with low level of digital literacy or limited access to digital technology need to be established. These should include, for example, design and development strategies to ensure that DTTS will be available irrespective of the specific hardware (mobile phones, computers) that individuals may use, as well as an extreme user-friendly design of these systems, and education campaigns.

Finally, consider the role and responsibility of OSPs, in this specific case Apple and Google. The two companies agreed to collaborate to create a shared application programming interface (API) for Bluetooth-based contact-tracing apps installed on Apple and Google phones. This collaboration is vital to the success of state-sponsored apps, because it will ensure that they will run smoothly on iOS and Android phones, facilitating user-experience and, hence, the large uptake of the app.

Apple's and Google's collaboration should not be seen as merely providing much-needed technical means. The design choices of API are value-laden and constraint the design choices of the apps relying on this API, defining their affordances. Notably, the growing adherence of European governments to the decentralised protocol followed Google's and Apple's decision to use it for their API. This is all good, insofar as it protects users' privacy, but it remains puzzling that a decision driven by OSPs will shape the way in which public authorities may design and use their apps and the extent to which these will respect the privacy of their citizens.

The collaboration between Apple and Google to support public health efforts in time of the pandemic should be welcome. But we should not overlook that it points at the key role that OSPs play in our societies, as designers and providers of essential infrastructures and services that enable information societies to work and prosper. We should start from this collaboration to consider carefully which role OSPs have, and *should have*, in mature information societies; what are the moral responsibilities that this role entails; how should these responsibilities be regulated; *how* should OSPs participate in the governance of the digital.

These questions are not new. They frame a central problem of the academic debate in Digital Ethics (Taddeo and Floridi 2015, 2017), but one that policies and

governance frameworks have struggled to address. In the current crisis, the lack of coherent answers to these questions has left governments with no guidance as to how to interact with OSPs who are designing, providing, and shaping the governance of tracking app, which without the support of OSPs may be unattainable, less effective or (paradoxically) come at the expenses of human rights.

In a leaked draft of Shaping Europe's Digital Future, the of the Council of the European Union states that EU Member States should "thoroughly analyse the experiences gained from the COVID-19 pandemic" to shape future policies approach to digital capabilities, especially focusing on areas like "e-Health, digital education, e-Government, data sharing and broadband connectivity".[7] This is all correct, but is set to be insufficient. Any policy for the governance of the digital will only be successful insofar as it will encompass ethical guidelines. Before living, dying, or being saved by the digit, our societies are transformed by it. This transformation is deep, long-term, and may spurs severe unintended, negative consequences. Ethical guidance is needed to minimise the risks, foster possible socially good uses of digital technologies, and ensure that the digital transformation will be humanly and environmentally sustainable, even more so when societies are called to redesign themselves after a global crisis like the one spurred by the COVID pandemic.

References

Floridi, L. (2014a). *The fourth revolution, how the infosphere is reshaping human reality*. Oxford: Oxford University Press.

Floridi, L. (2014b). Open data, data protection, and group privacy. *Philosophy & Technology, 27*(1), 1–3. https://doi.org/10.1007/s13347-014-0157-8.

Floridi, L. (2016). Mature information societies—a matter of expectations. *Philosophy & Technology, 29*(1), 1–4. https://doi.org/10.1007/s13347-016-0214-6.

Floridi, L. (2020). Mind the app - considerations on the ethical risks of COVID-19 apps. *Philosophy and Technology*, *34*(2).

Morley, J., Cowls, J., Taddeo, M., & Floridi, L. (2020). Ethical guidelines for COVID-19 tracing apps. *Nature, 582,* 29–31.

Primiero, G., & Taddeo, M. (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.

Servick, K. (2020). COVID-19 contact tracing apps are coming to a phone near you. how will we know whether they work? *Science*. https://doi.org/10.1126/science.abc9379.

Taddeo, M. (2014). The struggle between liberties and authorities in the information age. *Science and Engineering Ethics*. https://doi.org/10.1007/s11948-014-9586-0.

Taddeo, M. (2017a). Trusting digital technologies correctly. *Minds and Machines*. https://doi.org/10.1007/s11023-017-9450-5.

Taddeo, M. (2017b). The moral responsibilities of online service providers. In M. Taddeo & L. Floridi (Eds.), *The responsibilities of online service providers* (31st ed., pp. 13–42). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-47852-4_2.

Taddeo, M., & Floridi, L. (2015). The debate on the moral responsibilities of online service providers. *Science and Engineering Ethics*. https://doi.org/10.1007/s11948-015-9734-1.

[7] https://www.euractiv.com/section/digital/news/leak-eu-in-push-for-digital-transformation-after-covid-19-crisis/.

Taddeo, M., & Floridi, L. (2017). The moral responsibilities of online service providers. In M. Taddeo & L. Floridi (Eds.), *The Responsibilities of Online Service Providers* (Vol. 31, pp. 13–42). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-47852-4_2.

Ting, D. S., Wei, L. C., Dzau, V., & Wong, T. Y. (2020). Digital technology and COVID-19. *Nature Medicine, 26*(4), 459–461. https://doi.org/10.1038/s41591-020-0824-5.