HPLS (2021) 43:3
https://doi.org/10.1007/s40656-020-00354-7

NOTES & COMMENTS

The meaning of Freedom after Covid-19

Mirko Farina[1] · **Andrea Lavazza**[2]

Received: 30 August 2020 / Accepted: 24 November 2020 / Published online: 8 January 2021
© Springer Nature Switzerland AG 2021

Abstract Many governments have seen digital health technologies as promising tools to tackle the current COVID-19 pandemic. A much-talked example in this context involves the recent deluge of digital contact tracing apps (DCT) aimed at detecting Covid-19 exposure. In this short contribution we look at the bio-political justification of this phenomenon and reflect on whether DCT apps constitute, as it is often argued, a serious potential breach of our right to privacy. Despite praising efforts attempting to develop legal and ethical frameworks for DCT apps' usage; we argue that such endeavours are not sufficient to tackle the more fundamental problem of mass surveillance, which will remain largely unaddressed unless we deal with the biopolitical arguments presented and resort to a technical and structural defence.

Keywords Civil liberties · COVID-19 · Government tracking

During the current COVID-19 pandemic, policy makers begun considering people's immunity as the cornerstone of public health policies aimed at protecting

This commentary article belongs to the Topical Collection "Seeing Clearly Through COVID-19: Current and future questions for the history and philosophy of the life sciences", edited by G. Boniolo and L. Onaga.

✉ Mirko Farina
m.farina@innopolis.ru; farinamirko@gmail.com
http://mirkofarina.weebly.com/

Andrea Lavazza
lavazza67@gmail.com
https://www.cui.org/andrea-lavazza/

[1] Institute for Humanities and Social Sciences, Universitetskaya St, 1, Innopolis, Republic of Tatarstan, Russian Federation 420500

[2] Centro Universitario Internazionale, Via Antonio Garbasso 42, 52100 Arezzo, AR, Italy

citizens and their communities, sometimes to the detriment of other goals and values (Lavazza and Farina 2020; Farina and Lavazza 2020). Biopolitics—in the sense of a control that is made on bodies through the categories of science and medicine—has become central in the political sphere as society is confronted with an unknown threat (Foucault et al. 2008). It may hence be useful to reflect on how the debate surrounding the adoption of digital contact tracing apps (DCT henceforth) bears on our conception of privacy and freedom in function of the objective of achieving immunity from contagion. As we start reflecting on this issue an important question arises: is it right to sacrifice citizens' rights in favour of immunity?

Immunity is the body's ability to prevent the invasion of pathogens and typically refers to communicable diseases that can be of different severity and to which one can be exposed with different degrees of risk. Naturally, not all pathologies and not all risks are the same and not always the search for immunity can justify a trade-off against other equally cherished values. In this sense, the mandatory subscription to a DCT app that uses data sharing (deemed as one of the best tools for addressing the threat to immunity) is a measure that should be calibrated in the face of the degree of urgency corresponding to the need for immunity concerning the emergency in progress.

The task of a philosophical and ethical reflection is then to identify a correct balance between the degree of immunity that is thought to be necessary and the respective reduction of other inalienable values and rights. Biopolitical decisions that put immunity first as a synonym of security run into the risk of sacrificing privacy and basic freedoms, by using technical tools that promise highly effective control over the spread of the virus. This has become a particularly pressing concern given the recent deluge of DCT apps aimed at monitoring Covid-19 exposure (Floridi 2020; Ienca and Vayena 2020).

DCT apps have become a critical tool in the arsenals of governments for fighting the pandemic and hence for achieving immunity (Stevens and Haines 2020). In truth, though, contact tracing is not an entirely new technique. Public health officials have long used it to break the chain of transmission of infectious diseases (think about the plague); however, given the technological and infrastructural connectiveness of the world and of the societies in which we live, this practice—that once had logistical and technical limitations—has the potential of becoming quickly pervasive, creating dangerous vulnera in the rule of law and threatening many acquired fundamental civil liberties with the justification of the search for immunity as a more important value.

At the most basic level, Covid-tracing apps are designed to automatically notify users of potential exposure to Covid-19, by tracking their phone's location. Therefore—prima facie—they seem pretty helpful tools, which a citizen—in performing her civil duties and in the interest of public health—should download and actively use. However, the landscape of these apps is so varied that if not properly standardised their effectiveness may be significantly reduced and the justification of their use be challenged (see Morley et al. 2020; Whitelaw et al. 2020 for interesting analyses of these points).

Furthermore, there are a series of fundamental ethical questions underlying DCT apps' usage that deserve much attention. For instance: who is producing a given

app? How the producer of that given app is related to the national government? On which technology does the app rely? What is its level of privacy? What will happen with the data collected and how such information will be treated in the future?

Besides these crucial social and political concerns, there are also important legal aspects underlying DCT apps' usage that need to be better analysed when planning large-scale rollouts. For instance, oversight bodies should test the robustness of adopted privacy-preserving measures and possibly produce legal definitions for the roles of all the actors involved in DCT apps' development and implementation. In addition, ad hoc legislation may be required to specify rules that can safeguard citizens against possible misuses. Furthermore, sanctions for unlawful handling of personal data ought to be implemented (Blasimme and Vayena 2020). And yet, while these are all important issues to consider, we believe that they do not address the fundamental problem at stake; the problem of mass surveillance.

Since 2013 we have become increasingly aware of government's data breaches. Tech companies, often on behalf of governments, actively profile their customers through social media (Cambridge Analytica, for instance: Isaak and Hanna 2018). Moreover, government agencies routinely carry out mass surveillance activity by accessing our inboxes, listening to our conversations, keeping track of the videos and of the websites we open, or by following the transactions we make online (Snowden 2019; Bernal 2016). An increasing number of laptops each year is found with hidden keyloggers;[1] motherboards with spying chips inbuilt in them. Some agencies even developed programs (like the Brutal Kangaroo[2]) to infiltrate a close network or air-gapped computer without requiring internet access.

This means that people's metadata is constantly under scrutiny and at the risk of being exposed, even if some of us are still not fully aware of the pervasiveness of this sophisticated system of espionage.[3] In this sense then, by using DCT apps—which due to their publicity must necessarily be subject to independent scrutiny by free and rational moral agents and abide to specific national regulations—people won't be doing more harm to their privacy and constitutional rights than what they already caused to themselves. People, over the last two decades, have been giving up their privacy sometimes willingly (for instance, by accepting Facebook, Google or Instagram's terms and conditions of usage). They have also been tolerating the constant violations of their digital freedoms, often silently. Thus, during the pandemic, privacy could paradoxically be protected more than usual. However, the point to be emphasised here is the potential role of a Trojan horse that the combination of biopolitical justification (immunity) and mass surveillance (to get that goal) could play in the future. Societies need to be aware of this risk and think about possible countermeasures.

It is certain that in response to the pandemic, a number of governments will overstep their constitutional boundaries and try to seize the opportunity to strengthen the

[1] https://www.bbc.com/news/technology-42309371.

[2] https://thehackernews.com/2017/06/wikileaks-Brutal-Kangaroo-airgap-malware.html.

[3] One of us is working in an Informatics Department and is therefore quite familiar with issues of cybersecurity and data breaches.

system of comprehensive mass surveillance that has been created and implemented in the last two decades. For this reason, it might be argued that the answer to the problem of freedom after COVID-19 should not exclusively lie in the formulation of legal and ethical frameworks for DCT apps' usage (even though this latter attempt can be much praised); rather it ought to involve (if we are really serious about it) a paradigmatic change.

Such a change should encompass a cultural strategy to reduce the strength of the biopolitical appeal to immunity and make it proportional to the real danger (for example, not all threat to immunity needs to be addressed with drastic measures). It should also include the adoption of a number of technical solutions (such as end-to-end encryption and anonymization) as well as a radical departure from the current political landscape, focusing—for example—on the development of policies addressing software and hardware vulnerabilities and weaknesses of the Internet architecture. The former is certainly more feasible to achieve than the latter, at least in the short-term (Schuster et al. 2017), on the condition that people start using advanced anonymized encryption technology on a large scale (Schneier 2007).

In the framework of a bio-political quest for perfect immunity from contagion, our basic freedoms might be significantly eroded if we do not introduce a principle of proportionality among different values. Crucially, such a principle should help us attaining the legitimate objectives of preserving citizens and communities' immunity without exceeding the limits of what is appropriate and necessary in order to achieve those objectives (for example, one should not undermine basic civil liberties).

In order to regulate the proliferation and usage of DCT apps, oversight bodies should thus adapt technological design to socially perceived risks or expectations, take into account ethical and legal considerations, and introduce checks and balances to prevent abuses. However, this is unlikely to suffice to fully preserve our civil freedoms, as they ultimately depend on wider and more encompassing strategies that we ought to take collectively in order to defends our rights from the abuses that governments might conduct with the aim (or the excuse) of defending immunity. In this vein, the experts' task should be the assessment of real threats to immunity, so as to avoid the unjustified use of tools that can unjustifiably limit the rights of citizens as it might happen with DCTs.

References

Bernal, P. (2016). Data gathering, surveillance and human rights: Recasting the debate. *Journal of Cyber Policy, 1*(2), 243–264.

Blasimme, A., & Vayena, E. (2020). What's next for COVID-19 apps? Governance and oversight. *Science, 370*(6518), 760–762.

Farina, M., & Lavazza, A. (2020). Lessons from Italy's and Sweden's policies in fighting COVID-19: The contribution of biomedical and social competences. *Frontiers in Public Health*. https://doi.org/10.3389/fpubh.2020.563397.

Floridi, L. (2020). The fight for digital sovereignty: What it is, and why it matters, especially for the EU. *Philosophy and Technology, 33, 369–378*

Foucault, M., Davidson, A. I., & Burchell, G. (2008). *The birth of biopolitics: Lectures at the Collège de France, 1978–1979*. Springer, Berlin.

Ienca, M., & Vayena, E. (2020). On the responsible use of digital data to tackle the COVID-19 pandemic. *Nature Medicine, 26*(4), 463–464.

Isaak, J., & Hanna, M. J. (2018). User data privacy: Facebook, Cambridge Analytica, and privacy protection. *Computer*, *51*(8), 56–59.

Lavazza, A., & Farina, M. (2020). The role of experts in the Covid-19 pandemic and the limits of their epistemic authority in democracy. *Frontiers in Public Health*, *8*. https://doi.org/10.3389/fpubh.2020.00356.

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

Schneier, B. (2007). *Applied cryptography: Protocols, algorithms, and source code in C*. London: Wiley.

Schuster, S., Van Den Berg, M., Larrucea, X., Slewe, T., & Ide-Kostic, P. (2017). Mass surveillance and technological policy options: Improving security of private communications. *Computer Standards and Interfaces, 50,* 76–82.

Snowden, E. (2019). *Permanent record*. NYC, NY: Metropolitan Books.

Stevens, H., & Haines, M. B. (2020). Trace together: Pandemic response, democracy, and technology. *East Asian Science, Technology and Society: An International Journal, 14*(3), 523–532.

Whitelaw, S., Mamas, M. A., Topol, E., & Van Spall, H. G. (2020). Applications of digital technology in COVID-19 pandemic planning and response. *The Lancet Digital Health*, *2*, e435. https://doi.org/10.1016/S2589-7500(20)30142-4.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.