Ethical issues of pandemic applications

Centre de recherche en éthique, Montréal, le 1er juin 2020.

Martin Gibert, researcher in ethics, IVADO, CRE.
Contact: martin.gibert@umontreal.ca, Centre de recherche en éthique, 2910 boul. Edouard Montpetit, Montreal (QC) H3T 1J7.

Guillaume Chicoisne, Scientific Advisor, IVADO.
Ryoa Chung, Professor, Department of Philosophy, UdM.
Peter Dietsch, Professor, Department of Philosophy, UdM.
Sébastien Gambs, Professor, Department of Computer Science, UQAM.
Jocelyn Maclure, Professor, Department of Philosophy, U.Laval.
Dominic Martin, Professor, School of Management, UQAM.
Christine Tappolet, Professor, Department of Philosophy, UdM.
Daniel Weinstock, Professor, Faculty of Law, McGill.

Abstract

The coronavirus pandemic is spawning various projects mobilizing massive data and AI techniques. These seek to understand and reduce the impact of the virus using cell phone applications or directly from geolocation data collected by telecom operators. Among the objectives mentioned are contact tracing, risk evaluation of becoming infected oneself, the optimization of social distancing measures, the identification of population mobility behaviors, the control of the containment of infected persons and of the population in general, and a more precise understanding of the epidemic and its evolution.

Some of these projects could contribute to "flattening the curve" significantly. However, they also raise several important ethical issues. In particular, they may lead to the stigmatization of certain individuals or geographical areas and may lead to significant breaches of privacy because of the large amount of personal data collected. Such applications could even pave the way for a society of mass surveillance and control. The risk of error is also to be feared, as well as a false sense of security and the failure to respect the free and informed consent of users. Finally, it is important that these projects be carried out in close consultation with health and government authorities and be validated by an ethics committee.

Project proposals and applications

There are several projects and models of pandemic applications with various goals and objectives:

1- Collecting large-scale data on the pandemic including :

- Cases and contacts between infected and uninfected patients,
- Some epidemiological parameters of the pandemic such as the baseline reproduction rate (R0) of the virus, case-fatality rate, etc., to improve models.
- Spatial distribution of cases.
- Conditions that favour virus transmission (distance and duration of encounters, e.g. use or lack of masks, working conditions, etc.).

2- Inform government authorities about the evolution of the pandemic so that they can make the best decisions to minimize damage.

3- Inform users of the application :

- Of their degree of exposure to the virus or their risk of contracting the disease,
- The best behaviours to adopt, according to their level of risk,
- Spatial distribution of cases of the disease or density of people in different locations
- About the pandemic in general and about COVID-19.

4- Change the behaviour of the population by encouraging good isolation practices (e.g., nudge practices).

Different applications can be developed to achieve a few or many of these objectives. An important motivation behind the development of these applications is to reduce the number and severity of COVID-19 cases in the first instance, as well as to facilitate a return to normalcy and the resumption of economic activity later on.

Seven issues

1- Avoid the **stigmatization** of people at risk.

- Infected persons and persons at risk of being infected could easily be stigmatized and socially rejected, especially if the application shares the risk score with others. On the one hand, it is morally problematic to blame people for catching the virus. On the other hand, it can complicate the lives of those who are most vulnerable or who come into contact with sick people through their work.
- For example, an application that would make it possible to identify the level of risk of a person I come across in real time might reinforce stigmatization.
- Similarly, an application that would make it possible to indirectly deduce the level of risk of people I meet during the day or week would be problematic in this regard. This is particularly true in a context of social distancing where the number of people met each day is generally relatively low.
- It is crucial that the application not lead to irrational attitudes of mutual mistrust or paranoia.

- Stigmatization can also be spatial, so particular care and caution must be taken when distributing maps suggesting that shops or neighbourhoods are hot spots. Spatial stigmatization (e.g., a Jewish neighborhood) can easily lead to the stigmatization of groups that become scapegoats.
- Finally, stigmatization of people who do not want to use the application (e.g., people with mental disorders) or who cannot use it (e.g., due to the digital divide) should be avoided.

2- Do not create a precedent (ratchet effect) that would facilitate **monitoring and mass control**.

- There should be clear criteria for determining what kind of situation would warrant the adoption of this kind of technological measure: exceptional character, public health reasons, extreme economic consequences, etc.
- It should be borne in mind that the most vulnerable people are often the first victims of control and surveillance measures.
- Of course, an application can be uninstalled and its temporary or exceptional nature is reassuring. However, the question of the fate of the data collected and their potential use outside the original framework is a major risk.
- Moreover, to the extent that the threat of a new virus will always be present, these applications could become the norm and their (potentially mandatory) use could be easily reactivated. It is then important to be wary of the path dependencies that could be created with the first attempts.
- It is also noted that the use of such applications could later be generalized to follow other less invasive viruses, such as seasonal influenza - and raise the same hopes and reservations.

3- Establish **free and informed consent** of users.

- This is a morally and legally necessary condition for the deployment of the application.
- Also, social pressure may push people to install the application. We can imagine cases where this becomes problematic, for example if an employer asks his or her employees to download the application and always carry their phones with them, or if a law makes it mandatory to install the application on people who are part of vulnerable populations.
- The design of the system should take into account the fact that a significant portion of the population may have difficulty understanding statistics, probabilities, uncertainty or nuance. Therefore, care should be taken to ensure that information is presented in a way that is understandable to the greatest number of people.

4- Ensure a high level of **privacy by design**.

- The collection and processing of large amounts of data such as citizens' movements or contacts over a long period of time creates significant privacy risks, for example in the case of a potential data leakage such as we have experienced in recent years.
- The data collected by the application should be those that are necessary for the chosen purpose and no more should be sought (the concept of data minimisation).

- It should be transparent to the user what data are collected, what processing is carried out on those data and what the final purpose is, and the application should offer the user maximum control over the use and dissemination of those data.
- By default the privacy settings should be set to a high level of protection for the user (notion of privacy-by-default).
- In order to minimise privacy risks, some application proposals propose to operate on the basis of a decentralised architecture, where data would, for example, be stored locally on individuals' devices in an encrypted manner and would be retrieved only when a case of COVID is detected prior to the user's consent.
- Finally, the application should be secured as much as possible with state of the art best practices in order to be safe from malicious hijacking by hackers.
- The protection of privacy is a relatively cross-cutting issue that also ties in with other issues such as point 2 (surveillance) and point 3 (informed consent).

5- Ensure the **reliability** of the predictions and recommendations, as well as the scientific conclusions that are inferred from the collected data.

- Several factors should make us particularly vigilant: the pressure for rapid development and deployment, the lack of scientific certainty about the spread of the virus or the scientific data needed to model it, the complexity of epidemiological models and the simplifications chosen (often based on encounters and proximity or geolocation, independent of individual protective measures, for example).
- By way of concrete example, a protected nurse who sees 1000 patients per day might be less at risk than a cashier who meets 100 clients without keeping the distance or washing his or her hands during the day.
- In any case, the discrepancy between the system's predictions and reality can have deleterious effects. It should also be kept in mind that the system can be wrong in two ways, with false positives (i.e., people who are at risk think they are safe) and false negatives (i.e., people who are safe think they are at risk). The impact of these two errors will surely be very different and should be taken into account before the deployment of a technical solution is sought at any cost.
- One must also be careful about the risks of self-fulfilling prophecies and feedback loops that could be generated by the deployment and use of the application, which could indirectly serve to justify its success a posteriori.
- In the first instance, when the reliability of the system is poorly known, transparency with users should be ensured, with special warnings about measurement uncertainty. Thus, the default setting should take into account this uncertainty. It might also be appropriate to start with an application with deliberately reduced functionality.

6- Prevent the **false sense of security** that could be created by the application.

- In a context of turbulence and uncertainty, the application could suggest that everything is under control and that the AI is watching over us. This could, for example, lead some individuals to become disempowered if they rely primarily on the application's advice, rather than their common sense, to know how to behave in relation to COVID-19.

- Also be careful about backlash if you become infected when the application predicted low or no risk. Thus, "code green" should not be understood as "no risk", but rather as a lower risk (we could also avoid a code green, or make it very rare).
- Conversely, the application should not unnecessarily increase anxiety, especially for people with mental disorders. In particular, it should not cause panic.

7- Ensure close **consultation with government and health authorities**.

- Because of its intrusive nature and its many ethical issues, an anti-pandemic application should be validated on an ongoing basis by a legitimate government authority, under the supervision and control of other bodies that can play the role of safeguards, such as a data protection authority like the Commission d'Accès à l'Information in Quebec, or even associations representing civil society.
- Teams developing anti-pandemic applications should be able to place themselves at the disposal of this governmental authority and answer its questions and queries.
- Can this type of application be deployed by governments that do not have the necessary democratic legitimacy? How to proceed in non-legitimate states?

Finally, it should be noted that the value of such an application depends largely on the comparison with a situation without it. It is advisable to define a priori the criteria that will make it possible to quantify its success, rather than seeking to justify it a posteriori by defining these metrics after the end of the project. In this way, we can avoid giving in too easily to the sirens of technological solutionism.

This document is a follow-up to the zoom meeting of March 29, 2020.
Published by the Ethics Research Centre, Montreal in French, April 8, 2020.