Commission de l'éthique en science et en technologie
Québec

Conditions for Ethical Acceptability

MILA Application – The COVI Project

1. CONDUCT A RIGOROUS AND ONGOING ASSESSMENT OF THE PROJECT'S **RELEVANCY**

2. BE VIGILANT AND TRANSPARENT ABOUT THE **TECHNICAL LIMITATIONS AND CONDITIONS FOR SUCCESS** OF THE APPLICATION AND ITS USE, TAKING ALL THE DETERMINANTS OF ITS RELIABILITY INTO ACCOUNT

3. RESPECT INDIVIDUALS' **AUTONOMY** AND **DIGNITY** WHILE TAKING ACTION APPROPRIATE TO A PUBLIC HEALTH CRISIS

4. ENSURE **PROTECTION OF PRIVACY**, STARTING IN THE DESIGN STAGE, BY TAKING INTO CONSIDERATION THE APPLICATION'S ENTIRE LIFE CYCLE AND DATA

5. ESTABLISH A CLEAR **GOVERNANCE** STRUCTURE WITH AMPLE ROOM FOR CONSULTATION WITH DIFFERENT EVALUATION AND MONITORING BODIES

This draft paper was prepared by an ad hoc working committee on the use of digital and artificial intelligence technologies for COVID-19 monitoring and tracking (the "Committee"). The Committee was established on April 1, 2020, by the Commission de l'éthique en science et en technologie, a Government of Québec agency.

It is not the intention of this paper to formulate the Committee's final conclusions. Rather, its objective is to describe the Committee's current thinking on the main conditions of ethical acceptability for the design and potential use of such technologies. Therefore, its content may change.

The Committee's approach is iterative and evolutionary, in that it relies on constant dialogue with public authorities and IT developers to feed and guide ethical reflection, so that this latter is an integral part of the design process ("ethics by design").

The contents of this document should not be interpreted as a position for or against any particular application or the use of technological solutions more generally. This document is not binding for the institutions with which the members of the Committee are associated.

1.

CONDUCT A RIGOROUS AND ONGOING ASSESSMENT OF THE PROJECT'S **RELEVANCY**

- The functionalities of the application must be anchored in **public health needs**, as expressed by the public health authorities currently involved in fighting the pandemic.
- The planned use of the application must occur at **the appropriate time** in the public health authorities' strategy.
- Use of the application should not come as an additional burden for health care workers, who are already heavily solicited (**do no harm**). Functionalities must be designed to fit into currently applied health processes and protocols, including the one requiring health professionals to provide a special code or token to confirm a positive diagnosis.
- The contact tracing and the algorithmic individual risk estimation functions must meet a **reliability** threshold. While the reliability of the algorithm cannot be assessed from the start, it must nevertheless be demonstrated as early on as possible in the process and be reassessed at each stage of development.
- There must be **proportionality** of expected benefits and possible risks, reflecting the state of research and international experience.

The state of emergency and the significant prejudice caused by social distancing measures, as well as by the closures of institutions and businesses, require multiple avenues to be explored to maximize health benefits while minimizing the psychological, social, economic, financial and moral impacts on the population. The MILA application–COVI Project is one possible technological solution among others that should be considered in this exploration.

Relevancy must be measurable and able to be reassessed at different stages of the project. Stated otherwise, it will be necessary to conduct an ongoing evaluation of at least some of its aspects. **An adequate governance structure must support ongoing monitoring and evaluation** (see point 5). In particular, a few indicators should be identified to measure the success of the use of the application's different functions. This also raises the question of a "control group", i.e., a point of comparison making it possible to assess the gains of using the application.

2.

BE VIGILANT AND TRANSPARENT ABOUT THE **TECHNICAL LIMITATIONS AND CONDITIONS FOR SUCCESS** OF THE APPLICATION AND ITS USE, TAKING ALL THE DETERMINANTS OF ITS RELIABILITY INTO ACCOUNT

- The minimum number of users required for the application to be sufficiently reliable must be achieved realistically and without resorting to coercion.

  If the application were to be promoted by the government, further ethical analysis would be required.
- Issues related to the **reliability of data sources** must be recognized and taken into consideration by all stakeholders; for example, the underrepresentation of people with limited or no access to a mobile phone, and the risk of errors or lies in the self-reporting of medical history and symptoms.
- The vulnerable populations who are among those most likely to be affected by the pandemic may be left behind by the application: these people may not have access to technological devices, may not be able to fully understand the information being communicated to them or may not have the resources to further protect themselves against the risks of virus exposure in any case. At the strict minimum, **several approaches must be used simultaneously along with a technological solution.** In addition to the issue of reliability, major **inclusion** and **non-discrimination** issues have been raised.
- The actual effectiveness of Bluetooth technology for contact tracing is controversial. In particular, this use has been criticized for being inaccurate, generating false positives of contact, and consequently, either under- or overestimating exposure to the virus. An application that draws on GPS geolocation also raises privacy issues. Developers need to **better justify the choice of the adopted technology.**
- Widespread international screening campaigns seem to demonstrate that a high proportion of infected people are asymptomatic. **Measures, such as intensified screening, should be implemented to address this major limitation** in the assessment of individual risk.
- If a rigorous examination of the technical limitations of the application and the conditions for its successful use were to call into question its reliability, its relevancy would also be questioned.
- Limitations in regard to reliability should not become a pretext for expanding data collection, which would conflict with the principles of collection based on necessity, minimization and privacy.

A false sense of security among the general public or even among authorities must be avoided, as a result of a faulty assessment or a miscommunication to the user of the level of risk. For example, a user could construe a “green” rating as a stamp of immunity, which would be false and could lead them to engage in risky behaviour. Conversely, a “red” rating could cause a person additional anxiety that may not actually be warranted before a positive diagnosis is made.

3.

RESPECT INDIVIDUALS' **AUTONOMY** AND **DIGNITY** WHILE TAKING ACTION APPROPRIATE TO A PUBLIC HEALTH CRISIS

- In the context of the health crisis, the implemented measures are expected to curtail certain individual freedoms in the name of collective health benefits. Whether technological or otherwise, the measures that are selected must be those expected to bring the greatest benefits with the least harm and infringement of freedoms.
- Users who are over age 18 and sound of mind must be given the opportunity to formulate an **informed, voluntary and time-limited consent** for each of the project purposes and, in particular, for the data collection. To this end, accessible and understandable information that can be read in a reasonable amount of time must be provided at all appropriate moments. The adoption of the tool must also be free of undue coercion, which can be difficult in a context where social pressure is likely to be strong and potentially encouraged by governments. A government stance in favour of a technological solution must first and foremost be in keeping with the public health authorities' strategy and be accompanied by increased State responsibility in regard to protection from potential harm, as well as transparency and communication.
- Measures must be provided to **protect minors and incompetent adults** who might download and use the application.
- By categorizing users according to their level of risk, the application could lead to **stigmatization** and **discrimination** based on the rating. Individuals deemed to be at risk should not be subjected to prejudice as a result of this rating. If such prejudice is unavoidable, **compensation** measures must be foreseen.

  For example, if the risk score estimated by the application were to be used, as a necessary part of the public health strategy, to inform a gradual return to the workplace for low-risk employees, then protections and compensation would be necessary for employees said to be at higher risk and therefore unable to return to work.
- **The risk rating estimated by the application should not be used by individuals to manage access to public places and businesses** (coffee shops, stores, etc.).
- If the application is deployed, it is highly likely that such discrimination would occur. It would certainly be both easy and tempting (particularly for merchants and employers) to ask to see a consumer's or employee's risk rating as a condition for entry into their establishment, even if such a practice was prohibited. Special attention must be paid to this pitfall and a **discourse that discourages suspicion among citizens must be adopted**.

It is expected, in the context of a pandemic, for public health authorities to impose measures that significantly restrict individual freedoms, with detrimental social, economic and psychological consequences for many. The application is therefore being evaluated at a time that is not "normal," when our reasonable expectation of autonomy may differ from our expectations in a non-crisis context. The solution chosen should be one that, in the circumstances, best achieves a balance between respecting autonomy, minimizing harm, maximizing health benefits and distributing these equitably throughout the population.

4.

ENSURE **PROTECTION OF PRIVACY**, STARTING IN THE DESIGN STAGE, BY TAKING INTO CONSIDERATION THE APPLICATION'S ENTIRE LIFE CYCLE AND DATA

- Privacy by design requires developers to **work closely** with independent bodies to assess impacts on privacy and take the necessary steps to meet legal obligations and eliminate or mitigate risks, from early on in the design process.
- The data collected should be tagged, especially with regard to sensitive data and data with a **high potential for inference** (i.e. data from which sensitive or intrusive information, such as geolocation data, can be inferred).
- Principles of **necessity**, **minimization** and **proportionality** of data collection: The nature and quantity of the data collected must not exceed what is necessary to achieve the **stated**, **validated** and **legitimate** purposes (social acceptability, response to a legitimate public health need), and must be proportionate to the importance of the end objectives and reasonably expected benefits.
- The design should minimize potential privacy risks through the use of well-identified and proven-effective infrastructures and protocols.
- Users of legal age and competence should be given the opportunity to **provide clear, voluntary, informed and time-limited consent** for each of the purposes of the project. Consent must be solicited again if new purposes are pursued or new data, collected. Consent may also be withdrawn at any time. The terms and conditions of the right to withdrawal must be defined immediately.
- As a large amount of personal data (de-identified but not anonymized) will be centralized at MILA to train the learning algorithm, **the responsibility of those who will have access to these data must be defined now.**
- The following actions are also necessary: determine the rules for aggregating the data provided to public authorities; provide a framework for data sharing with third parties; and restrict possible uses of the application and the data in the future.
- The personal data collected should be destroyed within a reasonable amount of time once the purpose of the application has been achieved. Mechanisms for data destruction and deletion of the application ("self-destruction") should be well defined now and accompanied by guarantees for their implementation. As personal information can be generated and inferred from the risk estimation algorithm or classifiers, specific measures must be provided to ensure privacy protection even after the data has been deleted.

It is understood that the development of the algorithm is iterative and that it is difficult to determine completely and in advance which data are most relevant and therefore necessary to achieve the stated purposes. This may justify ongoing assessments throughout the development and deployment phases of the application.

5.

ESTABLISH A CLEAR **GOVERNANCE** STRUCTURE WITH AMPLE ROOM FOR CONSULTATION WITH DIFFERENT EVALUATION AND MONITORING BODIES

- The project must be closely coordinated with public health authorities at all stages to ensure the **relevance** of the application and the **consistency** of communications.
- Several public authorities (INESSS, INSPQ, CEST, CAI, etc.) should be drawn into the project, in a concerted manner and according to their respective expertise, to carry out an adequate follow-up of the project's multiple dimensions (assessment of health technologies and intervention methods, public health, ethics, protection of privacy, etc.).

  In particular, such organizations must be involved to ensure that citizen voices are heard in the decision-making process, for example by involving public representatives who are already sitting on ethics committees.
- "Ethics-by-design": An ethics-by-design approach requires developers to work closely with independent authorities, from the early design stage, to identify the ethical risks as well as the measures to be adopted to eliminate, mitigate or compensate such risks. The project should also be subject to ongoing and iterative evaluation of its deployment, for future use. An ad hoc ethics committee may be mandated to ensure compliance with the conditions of ethical acceptability.
- Research ethics: It is the working committee's opinion that a portion of the project may be considered research and thus subject to the normative frameworks of the granting agencies and the relevant articles of the Civil Code of Québec. MILA should contact the responsible authority at the Université de Montréal and the other universities involved to determine whether a portion of the project, such as training the algorithm using data collected from users or using it to develop epidemiological models, should be subject to review by a research ethics board.

Commission de l'éthique en science et en technologie
Québec