NATIONAL PILOT COMMITTEE FOR DIGITAL ETHICS

OPINION 1

ETHICAL ISSUES ABOUT DIGITAL TOOLS FOR LIFTING OF LOCKDOWN

COMITÉ NATIONAL PILOTE D'ÉTHIQUE DU NUMÉRIQUE
sous l'égide du
COMITÉ CONSULTATIF NATIONAL D'ÉTHIQUE
POUR LES SCIENCES DE LA VIE ET DE LA SANTÉ

ETHICAL ISSUES ABOUT DIGITAL TOOLS FOR LIFTING OF LOCKDOWN

Response to the referral of

Mr. Olivier Véran	Mr. Cédric O
Minister of Health and Solidarity	Secretary of State for the Digital Economy

Opinion unanimously approved by the members present at the CNPEN plenary session of May 13, 2020.

Published on May 14, 2020

OPINION 1

CONTENTS

ETHICAL ISSUES ABOUT DIGITAL TOOLS FOR LIFTING OF LOCKDOWN

1. Introduction

On April 30, 2020, the French Minister of Health and Solidarity and the Secretary of State for the Digital Economy referred to the French National Pilot Committee for Digital Ethics (CNPEN) the question of ethical issues related to the design, implementation, and uses of digital tools in the different phases of lifting of lockdown, in particular concerning respect of privacy and protection of civil liberties and the structuring effects that these tools could have in the medium and long term, notably on citizens and society.

The response to this referral, which is the subject of this Opinion, has been drawn up within a very short time frame, given the context and the speed with which the government's decisions have to be implemented. However, the CNPEN had set up on March 19 a specific working group to review the ethical issues raised by the use of digital technology in the epidemic crisis. This led to the publication on April 7 of a first newsletter on Reflections and Warning Points on Digital Ethics Issues in Situations of Acute Health Crisis, with a particular emphasis on the monitoring of people using digital tools, followed by a press release on April 29 about Ethical Issues of Digital Epidemiological Surveillance on Lifting of Lockdown. The present Opinion is based in particular on these two documents, and was developed in cooperation with the CCNE (French National Consultative Ethics Committee for Life and Health Sciences), which was asked on May 4 by the COVID-19 Scientific Council to consider the ethical issues raised by the lifting of lockdown.

The crisis situation triggered by the COVID-19 pandemic has led to an unprecedented increase in the uses of digital technology as well as the creation of new tools that have become essential at all levels—societal, economic, health—and have led to a surge in attendant ethical issues.

In terms of health, digital tools can help identify possible transmission of the virus from carriers to people with whom they have been in close proximity, to facilitate the early warning of potential carriers. Collectively, these tools can in particular be used to study and model the evolution of the epidemic, to identify possible new outbreaks of infection, and to help assess population immunity in a context of partial understanding of the pandemic. These tools come into their own as part of an overall scheme that includes protection measures, tests, diagnosis, quarantine, support, treatment, and hospitalization.

However, the design, implementation, and use of these tools in the context of the pandemic bring into competition on the one hand health imperatives that respect fundamental freedoms—including protection of privacy and personal data—and on the other, an urgent need to deploy these tools, with the attendant questions of sovereignty, trials, control, and provision of fair information to the public.

In this Opinion, we first present an overview of digital tools that could be used in the different phases of the lifting of lockdown and beyond. We then focus on the specific analysis of ethical issues raised by digital tools made for tracing people who might spread the virus. As we explain in the appendix, this can be carried out in several complementary ways, relying both on contact tracing apps and on health teams that collect and exchange information about people and their social contacts. We therefore analyze the ethical issues relating to contact tracing apps, especially those based on the use of digital technologies like Bluetooth, and the ethical issues related to the use of these apps in combination with the SI-DEP information systems and Contact Covid, which are designed as supports for health teams, as described in Decree No. 2020-551 of May 12, 2020[1]. Following these analyses, we highlight some points requiring attention and formulate recommendations that shed light on the design, implementation, and uses of these digital tools.

2. Digital tools in the context of the COVID-19 crisis

The government's strategy for the lifting of lockdown is based on three pillars: protecting, testing, isolating. These require the implementation of specific short-, medium-, and long-term means, including various digital tools that could help to protect public transport users, for instance, by informing them about overcrowding in real time; to identify people to be tested as a result of close contact with infected persons; and to allow people likely to be infected to continue to communicate or to be medically monitored while remaining isolated. Digital tools, particularly in a research context, can also help to predict the evolution and consequences of this pandemic, and to improve prevention of future health crises.

The following table presents digital tools that are being used, or which could be used, during the various phases of lifting of lockdown and beyond, indicating their purposes to protect (P), test (T), isolate (I), and anticipate (A).

Digital tools	P	T	I	A
Contact tracing apps		X	X	X
Information systems for contact tracing by health teams (SI-DEP and Contact Covid)		X	X	X
Tools to facilitate provision of information to health teams and their interaction with people to be tested or monitored		X	X	
Self-diagnosis tools, tools for general practice, telemedicine	X	X	X	
Tools for informing the public and for citizen input	X	X	X	X
Modeling tools for monitoring and predicting epidemic spread	X			X
Research tools for statistical data analysis and long-term foresight	X			X

[1] Decree No. 2020-551 of May 12, 2020, relating to the information systems mentioned in Article 11 of Act No. 2020-546 of May 11, 2020, extending the state of health emergency and supplementing its provisions

Analysis and viewing tools for medical imaging		X		X
Tools for medical research (drug and vaccine research, etc.).	X			X
Robots for medical analysis		X		
Robots to assist in disinfection	X			
Robots to assist in the delivery of meals, drugs	X			
Information and guidance tools for users of public transport	X			
Automatic control of authorized access to public transport	X			
Closed-circuit television to check compliance with protection measures in public places and public transport	X			
Automated manufacture of critical products (masks, protective shields, respirator masks, etc.).	X			
Tools enabling the organization and pursuit of economic, social, educational, and cultural activities (teleworking, distance learning, etc.).	X		X	

Digital tools thus help to balance health, economic, and social objectives. However, their design, implementation, and use raise ethical tensions, which are considered in the following sections of this document with regard to apps and information systems used in contact tracing.

3. Ethical issues about contact tracing apps for epidemiological monitoring

3.1. Introduction to contact tracing apps for smartphones

In lifting of lockdown and more generally in an epidemic of a particularly contagious disease, it is of the utmost importance to reduce chains of infection. This is done first of all by prevention and protection, notably through protection measures. It also relies on identifying infected people and therefore on medical tests, and finally, on contacting potentially infected people as quickly and efficiently as possible.

The average number of people to whom a sick patient transmits the disease, called the transmission factor R0, must be less than 1 for the epidemic to decline. The value of this transmission factor is determined by several parameters, including prevention and protection, but also rapid identification of potentially infected people. This identification depends on the proximity of two people, one of whom is a symptomatic virus carrier. Contact tracing can be achieved either by the direct intervention of authorized persons or by using digital apps to automatically detect and memorize the proximity of two smartphones assumed to be carried by two people (see Appendix 1), or by combining both approaches.

Contact tracing apps can therefore help reduce R0, but also constitute a risk of leakage of the personal data of people using these apps. To reduce this risk, protocols preserving anonymity and enhancing the security of contact tracing apps have been designed, most of which belong to two main classes of protocols described as "centralized" and "decentralized". Appendix 1 states the main principles depending on whether the information is managed primarily by a centralized server or locally by smartphones.

In terms of cybersecurity, the risks concern data stored on smartphones or on a centralized server, and communications either between smartphones or between smartphones and a central server. The circulation of data on networks, including the internet, also presents a risk of leakage.

The hardware and software architecture of a contact tracing app must be taken into account in its implementation. The central server and networks will have to be configured to ensure the availability and reliability of the service and hence the security and reliability of the app. They could also incorporate learning tools regarding the duration and intensity of contact.

Analysis of the ethical tensions resulting from the choices made by designers of a contact tracing app requires an examination of the techniques currently available.

Proximity sensing can be carried out using location techniques—GPS, Wi-Fi, a cellular network or a combination thereof—or using a local communication protocol such as Bluetooth Low Energy between two digital devices. Most protocols available in Europe use this latter solution, sometimes combined with location. In making this technical choice, it is important to be aware of its consequences in terms of reliability of proximity detection. Notably, ignorance of protective barriers, such as a wall or a doctor's protective wear, would increase the number of false-positive subjects. Furthermore, the use of Bluetooth Low Energy by a contact tracing app may, for certain smartphone brands, be subject to restrictions on use imposed by the manufacturer and the owner of the operating system, who are then in a position to decide whether or not to promote implementation of this contact tracing app.

3.2. Analysis of ethical tensions specific to contact tracing apps

The technical and social choices made during the design, implementation, and use of a contact tracing app are likely to exacerbate tensions between different ethical principles and values that need to be identified, analyzed, and arbitrated.

Choice and uses of an app

By automating contact tracing, in particular in public places and public transport, the use of smartphone apps accelerates the reporting of new cases of potentially infected people. It thereby helps reduce R0 and slows the spread of the epidemic, thanks to self-isolation and medical monitoring offered to potentially infected people. In the longer term, it can also contribute to the development of statistical studies or predictive models nationally or internationally. Moreover, the use of similar apps for other health crises (seasonal influenza epidemics, for instance) may be considered. However, there may be concerns about the perpetuation of such contact tracing apps, their use for purposes other than health crisis management, or even habituation of the population to the use of such measures legitimized by the current pandemic.

In order to prevent the risk of privacy infringement that such perpetuation would constitute, guarantees would have to be given concerning the temporary and proportionate use of the data collected by the app. The activation of an app, its suspension or the adjustment of its parameters (distance measurement, alert level, etc.) will have to be decided by the competent public authorities on the basis of the evolution of the health situation.

The proportionality criterion implies that applications minimize the volume of data collected and guarantee anonymity, so that neither the identity of the infected person nor his or her contacts are accessible, including to the app itself. However, this anonymization could make it harder for health professionals to provide the infected person with the care needed. Furthermore, if such tracing tools were to be insufficiently effective, other techniques such as geolocation could be considered, with possible risks of infringement of privacy.

In order to be able to control all these aspects, the public authorities must be able to make their own app choices. It is particularly important to use contact tracing devices designed and deployed with care and attention to interoperability, in Europe and internationally. The deployment of non-interoperable national apps and the proliferation of apps proposed by private and/or international actors likely to establish different contact lists could limit the effectiveness of contact tracing by digital means. This multiplicity could also limit freedom of movement, especially from one country to another.

Recommendations

3.1. Aim for interoperability of contact tracing apps in Europe, or even internationally, in compliance with the General Data Protection Regulation (GDPR).

3.2. Ensure there is no discrimination against people who do not use voluntary contact tracing apps, including in the context of travel in Europe and internationally.

3.3. Choose technical means of proximity detection that promote protection of both privacy and personal data.

3.4. Enable the competent public authorities to activate or deactivate contact tracing apps voluntarily downloaded and to inform the users.

3.5. Allow users who have voluntarily downloaded a contact tracing app on their smartphone to disable it temporarily or uninstall it permanently, at any time.

3.6. Provide for the automatic deactivation of contact tracing apps after expiration of their legal time limit and the means to report it publicly.

Transparency

The effectiveness of an app depends in particular on the public's support for its use, which is based on the trust placed in the whole prevention and care system put in place. This acceptance cannot be achieved without regular provision of freely accessible, fair and transparent information on the app's design, code, and code authors in addition to its purpose and the use made of the data it collects, so that everyone can rest assured that it only does what it is supposed to do. In particular, publication of the app's source code is an elementary condition of transparency. Fairness of information further requires that the terms employed to describe the technical aspects must be unambiguous and enable understanding by all users. For instance, use of the loaded terms "centralized" and "decentralized" may hinder understanding of technical devices.

This information, supplemented by data on the rate of dissemination of the apps in the population and by the results of national audits conducted by trusted third parties, should enable institutional and democratic control and foster public debate.

Recommendations

3.7. Ensure regular provision of freely accessible, fair, and transparent information on the design and code of contact tracing apps, their purpose, and on the use of the data they collect. Ensure that this information enables understanding by all users.

3.8. Provide a legislative and regulatory framework to organize institutional and democratic control of contact tracing apps, and to facilitate the public debate.

3.9. Subject contact tracing apps to audit by trusted third parties.

Consent

A contact tracing app is designed to inform users of contact with an infected person, thereby enabling them to be stakeholders in their own health and in the health of others. The voluntary and non-binding nature of its use can, however, reduce the app's effectiveness. It is also necessary to take into account the possible lack of reactivity of users or their potential reluctance to undergo medical testing. Despite its potentially negative impact on the effectiveness of an app, volunteering is essential and must be based on free and informed consent. This assumes that whoever refuses consent is not exposed to negative consequences of any kind.

Consent is based on transparency and requires the prior establishment of a policy of information and acculturation of citizens, despite the emergency context. This information must in particular set out the implications and limitations of the app, notably to avoid the illusion of being "protected" by a smartphone and the resulting risky behaviors. Besides, consent to the use of the app and the accountability of underage or vulnerable people must be considered and be the subject of support and of appropriate information. Particular attention must be paid to people in situations of social vulnerability, people who do not have a good command of the French language, and people unable to access this technology.

If policies to incentivize the use of contact tracing apps were to be put in place, they should exclude systems that may induce bias and cause discrimination against certain populations. This is particularly important in the case of those offering user rewards.

The possible stigmatization or pressuring of people who do not use an app cannot be discounted, particularly by employers or insurers. In no way do ownership of a smartphone and the use of an app constitute conditions for access to services or resources, in particular access to care and employment. Specific and free measures must be provided for people who do not have a smartphone, but who wish to participate in the contact tracing program.

Recommendations

3.10. Make clear and fair information available and accessible to all sectors of the public concerning the objectives, functioning, and limitations of contact tracing apps. This information should be provided on a national reference website, by phone, in the form of printed documents, and broadcast on radio and TV.

3.11. Educate the whole population about the technical and social challenges of contact tracing apps.

3.12. Ensure free and informed consent and the possibility of not giving consent, without pressure, constraint, or the implementation of a reward system.

3.13. Allow people to withdraw from their commitment at any time along with the deletion of the data collected.

3.14. Provide specific and free measures for people who do not have a smartphone and who wish to participate in the contact tracing program.

Point of attention

3.a. The use of a contact tracing app should be subject to a joint decision between the holders of parental authority and minors under 15 years of age.

Trials

In order to have a robust and functional tracing app, it is necessary to conduct trials openly beforehand. For this, it is better to investigate first on a small scale, in a sample population, before general deployment. Insufficient validation or hasty trialing of the app could impair its effectiveness. For example, this could lead to unwanted overloading of the medical testing system with false positives (notified but subsequently tested negative). If a tracing app malfunctions or proves ineffective, the responsibility and reputation of the those who sponsored, designed, or implemented it may be compromised, thus reducing confidence in management of the crisis.

These trials face two limits: first, the choice and size of the sample population, and second, the time needed to conduct the trials. If an app is deployed, it is advisable to continue the trials during deployment in order to correct and improve it, and to take the results into account, along with the feedback from this deployment.

Recommendation

3.15. If a contact tracing app is deployed, conduct trials even if rapid implementation is necessary. Pursue these trials in parallel with deployment.

4. Ethical issues regarding interactions between digital contact tracing and the SI-DEP and Contact Covid information systems for contact tracing

The National Lockdown Exit Strategy is currently based on two digital tools[2]: SI-DEP, an automated information and screening system that collects diagnostic testing results (RT-PCR) in order to identify positive cases, and Contact Covid, a specific database that records all patients who tested positive and their close contacts for monitoring purposes[3].

We analyze here the actual or potential links between the three information systems constituted by SI-DEP, Contact Covid, and a possible application of digital contact tracing. First, it should be noted that SI-DEP data, including the identity of people who test positive, are taken into account by Contact Covid[4]. Also, a contact tracing app records all contacts independently of their significance, whereas SI-DEP and Contact Covid only record suspicious contacts, as the process is triggered by a doctor considering medical test results or the presence of symptoms. This changes the evaluation of proportionality and, as a result, the anonymity requirements we address below.

Uses of information systems

Members of the health teams using SI-DEP and Contact Covid can both interpret the data collected in context and explain health measures recommended to the person concerned and his or her contacts. This is, however, conditional upon the users of the information systems being certified and competent.

Deliberations on the lifting of lockdown measures should weigh the effectiveness of a contact tracing app against that of actions carried out by human beings, especially by health teams. This contrast often leads to the fear of actions performed by machines, even if they are minimally intrusive, and to a preference for human actions, even if they are more intrusive. On the one hand, a database managed by human operators can have as many, if not more, risks of a breach of confidentiality as the data collected by a digital application. On the other hand, anonymity—which is the aim of a contact tracing app—does not allow professionals to provide support to people notified by the app as having been in contact with people who have tested positive, at least before they report it to their doctor or a health authority.

Other digital tools could also be used to support human intervention for tracing purposes. For example, in the Contact Covid approach, people asked to report their contacts could receive support where appropriate on the basis of their phone's geolocation history, or could even authorize the official asking for these contacts to access their history or organizer. Other digital means could, in support of human intervention, help to prioritize calls by frequency of contact or by most affected areas, or to provide tools for interaction,

[2] Act No. 2020-546 of May 11, 2020, extending the state of health emergency and supplementing its provisions

[3] See the website of the Ministry of Health and Solidarity, consulted on May 11, 2020, at 11 am.

[4] Decree No. 2020-551 of May 12, 2020, relating to the information systems mentioned in Article 11 of Act No. 2020-546 of May 11, 2020, extending the state of health emergency and supplementing its provisions

including telemedicine diagnosis. These tools also raise issues of confidentiality of personal data.

In addition, Contact Covid's multi-stage procedure involves potential weaknesses. It relies first on telephone calls, with the risk of failure to reach those concerned. It is then based on interviewing these people, whose memory is uncertain or who may not wish to divulge some information. As a consequence, the Contact Covid database is potentially incomplete and incorrect. Moreover, it may be biased by malicious acts, such as a false declaration of contacts. Conversely, an automated protocol could quickly give the complete list of contacts of someone who tests positive. With regard to these matters, the use of a contact tracing app could complement and usefully reinforce the Contact Covid procedure.

Complementarity between a contact tracing app and the SI-DEP and Contact Covid information systems could therefore allow faster, more accurate, and more robust detection of contact cases. Linking them together could expand the possibility of individual follow-up of potentially infected people. However, the combination of these two types of approaches runs two major risks. First, the cross-referencing of two databases, one with anonymous data (that of the app) and the other not (that of the SI-DEP and Contact Covid systems), may lead to loss of anonymity for the former. Besides, the sovereign character[5] of digital tools such as SI-DEP and Contact Covid could be compromised by their combination with a tracing app not controlled by the national authorities.

Recommendations

4.1. Ensure the anonymity of a contact database created automatically by a digital application when the app is linked to information systems managed by certified professionals in which the information is not anonymized.

4.2. Ensure that any combination of the SI-DEP and Contact Covid systems with a contact tracing app is subject to control by the national authorities.

Point of attention

4.a. Cross-referencing the SI-DEP and Contact Covid databases makes the health information highly identifiable.

The use of new rapidly trained employees and the possible opening of a company's sensitive medical data (person's state of health, health history, possible treatments) to stakeholders who do not normally have access to them, are likely to increase the risk of breaches of medical confidentiality. The responsibility of the state and of all stakeholders involved would be incurred in the event of data leakage or misuse.

[5] Sovereignty allows one to be responsible for one's ethical choices; see CERNA report, Sovereignty in the Digital Age - Remaining Masters of our Choices and Values, Allistene, Oct.2018. http://cerna-ethics-allistene.org/digitalAssets/55/55708_AvisSouverainete-CERNA-2018.pdf

Recommendation

4.3. Train health team members and raise their awareness of the issues related to personal data protection, notably in the context of the use of digital tools. In particular, ensure the protection of medical confidentiality.

Anonymization and pseudonymization

Personal health data gathered by the SI-DEP and Contact Covid systems are pseudonymized for their use in epidemiological and research studies.

Numerous computer studies have shown that the removal of identifying data, in particular surnames and forenames, possibly replaced by pseudonyms, is not anonymization within the meaning of the GDPR. Indeed, there is a risk of re-identification through cross-referencing with other databases where personal information figures explicitly. We should therefore be careful to distinguish between "pseudonymized" data and “anonymized” data.

Point of attention

4.b. "Pseudonymized" health data are not "anonymized" data and should therefore be considered as personal and as such protected according to the principles of the GDPR.

Protection without discrimination

Data collected by health teams or by a digital application are sensitive data that could be used for discriminatory purposes. The Council of Europe underlines that "*profiling should not lead to discriminatory measures of any kind*," in particular with regard to political, social, economic, sexual or religious aspects[6]. Similarly, the WHO warns of the risk of stigmatization of people showing characteristics that could be perceived as being related to the disease[7].

Recommendation

4.4. Ensure there is no discrimination against people who test positive, or against groups that could be identified in the epidemiological analyses, while applying the isolation measures required to limit the spread of the epidemic.

[6] Council of Europe "The Convention for the protection of individuals with regard to automatic processing of personal data”, European Treaty Series No. 108, 1981

[7] Article 3 of the WHO International Health Regulations (2005)

5. General recommendations regarding contact tracing tools

For design

5.1. Organize checks and technical tests throughout the life cycle of contact tracing tools to evaluate their robustness and security.

5.2. Have the effectiveness of contact tracing tools evaluated by an independent body.

Point of attention

5.a. At all design stages and for all technical components, ensure compliance with French and European regulations, notably the GDPR.

For implementation

5.3. For each contact tracing tool, define and announce the legal duration of its use and of the storage of processed data, which should be limited and proportionate to the duration of the pandemic. Document the conditions for reversibility of implementation of these tools.

5.4. Provide the appropriate technical and legal means to ensure the cybersecurity of contact tracing tools given their intrusive nature and massive use.

5.5. Establish a single, operational monitoring committee to identify and address ethical, legal, and social issues created by contact tracing tools in the context of the lockdown exit strategy. This committee will include, among others, digital, health, social sciences, and humanities professionals, as well as parliamentarians and representatives of civil society. This committee should join up with the COVID-19 supervisory and liaison committee, introduced by the Act of May 11, 2020 (Art 11 VIII), which is tasked with linking civil society and Parliament in the fight against the spread of the epidemic by tracing contacts and by monitoring the deployment of information systems for this purpose.

For uses

5.6. Allow individuals to access their personal data, report an error, require changes, receive a reply to their request within a specified time limit, and initiate an appeal in the event of harm suffered.

6. Summary of general and specific recommendations

For design

3.1. Aim for interoperability of contact tracing apps in Europe, or even internationally, in compliance with the GDPR.

3.3. Choose technical means of proximity detection that promote protection of both privacy and personal data.

3.4. Enable the competent public authorities to activate or deactivate contact tracing apps voluntarily downloaded and to inform the users.

3.5. Allow users who have voluntarily downloaded a contact tracing app on their smartphone to disable it temporarily or uninstall it permanently, at any time.

3.6 . Provide for the automatic deactivation of contact tracing apps after expiration of their legal time limit and the means to report it publicly.

3.7 . Ensure regular provision of freely accessible, fair, and transparent information on the design and code of contact tracing apps, their purpose, and on the use of the data they collect. Ensure that this information enables understanding by all users.

3.9. Subject contact tracing apps to audit by trusted third parties.

3.15. If a contact tracing app is deployed, conduct trials even if rapid implementation is necessary. Pursue these trials in parallel with deployment.

5.1. Organize checks and technical tests throughout the life cycle of contact tracing tools to evaluate their robustness and security.

5.2. Have the effectiveness of contact tracing tools evaluated by an independent body.

Point of attention

5.a. At all design stages and for all technical components, ensure compliance with French and European regulations, notably the GDPR.

For implementation

3.8. Provide a legislative and regulatory framework to organize institutional and democratic control of contact tracing apps, and to facilitate the public debate.

3.10. Make clear and fair information available and accessible to all sectors of the public concerning the objectives, functioning, and limitations of contact tracing apps. This information should be provided on a national reference website, by phone, in the form of printed documents, and broadcast on radio and TV.

3.11. Educate the whole population about the technical and social challenges of contact tracing apps.

3.12. Ensure free and informed consent and the possibility of not giving consent, without pressure, constraint, or the implementation of a reward system.

4.1. Ensure the anonymity of a contact database created automatically by a digital application when the app is linked to information systems managed by certified professionals in which the information is not anonymized.

4.2. Ensure that any combination of the SI-DEP and Contact Covid systems with a contact tracing app is subject to control by the national authorities.

4.4. Ensure there is no discrimination against people who test positive, or against groups that could be identified in the epidemiological analyses, while applying the isolation measures required to limit the spread of the epidemic.

5.3. For each contact tracing tool, define and announce the legal duration of its use and of the storage of processed data, which should be limited and proportionate to the duration of the pandemic. Document the conditions for reversibility of implementation of these tools.

5.4. Provide the appropriate technical and legal means to ensure the cybersecurity of contact tracing tools given their intrusive nature and massive use.

5.5. Establish a single, operational monitoring committee to identify and address ethical, legal, and social issues created by contact tracing tools in the context of the lockdown exit strategy. This committee will include, among others, digital, health, social sciences, and humanities professionals, as well as parliamentarians and representatives of civil society. This committee should join up with the COVID-19 supervisory and liaison committee, introduced by the Act of May 11, 2020 (Art 11 VIII), which is tasked with linking civil society and Parliament in the fight against the spread of the epidemic by tracing contacts and by deploying information systems for this purpose.

Points of attention

4.a. Cross-referencing the SI-DEP and Contact Covid databases makes the health information highly identifiable.

4.b. "Pseudonymized" health data are not "anonymized" data and should therefore be considered as personal and as such protected according to the principles of the GDPR.

For uses

3.2. Ensure there is no discrimination against people who do not use voluntary contact tracing apps, including in the context of travel in Europe and internationally.

3.13. Allow people to withdraw from their commitment at any time along with deletion of the data collected.

3.14. Provide specific and free measures for people who do not have a smartphone and who wish to participate in the contact tracing program.

4.3. Train health team members and raise their awareness of the issues related to personal data protection, notably in the context of the use of digital tools. In particular, ensure the protection of medical confidentiality.

5.6. Allow individuals to access their personal data, report an error, require changes, receive a reply to their request within a specified time limit, and initiate an appeal in the event of harm suffered.

Point of attention

3.a. The use of a contact tracing app should be subject to a joint decision between the holders of parental authority and minors under 15 years of age.

Appendices

Appendix 1: The different methods of contact tracing[8]

In the context of an epidemic, let us imagine that Alice and Bob meet and three days later it turns out that Alice is sick. How can she warn Bob so that he self-isolates, gets tested, and thus breaks the chain of infection?

For Alice, a first algorithm consists in writing down in a notebook Bob's phone number, along with the phone numbers of all the people she has met, to be able to warn them if she ever gets sick. However, Bob doesn't necessarily want to give his number to Alice, who might use it in a way that Bob doesn't agree with. If he refuses to give it to her, or if he has no telephone, he will not be notified if Alice becomes sick. This method—that we'll call the Contact Book protocol—forces you to declare your identity to everyone you meet. It is an intrusive method, and potentially ineffective because Bob may not wish to give Alice his contact information. The principle of this method is used by doctors to avoid violent epidemics, as of meningitis: when someone becomes sick, a professional investigator tries to identify all the people with whom the person has been in contact, to diagnose them and offer them treatment if needed. In the context of the COVID-19 health crisis, this is the principle of the protocol behind the Contact Covid information system[9].

To avoid this algorithm, which is intrusive because of its access to people's identity, programmers have invented others that are more respectful of privacy and personal data. For example, when Alice and Bob meet, they are designated by pseudonyms, such as "Xlthlx" and "Qfwfq". A third person, Zoe, then receives the information that Xlthlx and Qfwfq have met. When Alice gets sick, she tells Zoe that person "Xlthlx" is sick; Zoe deduces that person "Qfwfq" has been in contact with an infected person. Bob asks Zoe every day if person "Qfwfq" has been in contact with an infected person; on the third day, Zoe answers in the affirmative. He concludes that there is a risk to himself. This method, in which Zoe records all pairs of pseudonyms nationally or by continent, is called "centralized." It is the basis of the ROBERT protocol[10], which is used in particular in the StopCovid tracing app.

However, it is also possible to proceed differently. For example, another method based on the DP3T protocol[11], is used in contact tracing apps preferred by operating system owners. This method will be deployed notably in Germany and Switzerland. It works on the following principle: Bob notes in his phone that he has been in contact with a person whose pseudonym is “Xlthlx”. Alice then warns all phones using this protocol that person "Xlthlx"

[8] According to an article published in *Pour la Science* in July 2020 : https://www.pourlascience.fr/sr/homo-sapiens-informaticus/stopcovid-communiquer-tout-en-restant-masque-19568.php

[9] See the website of the French Ministry of Solidarity and Health

[10] https://github.com/ROBERT-proximity-tracing/

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

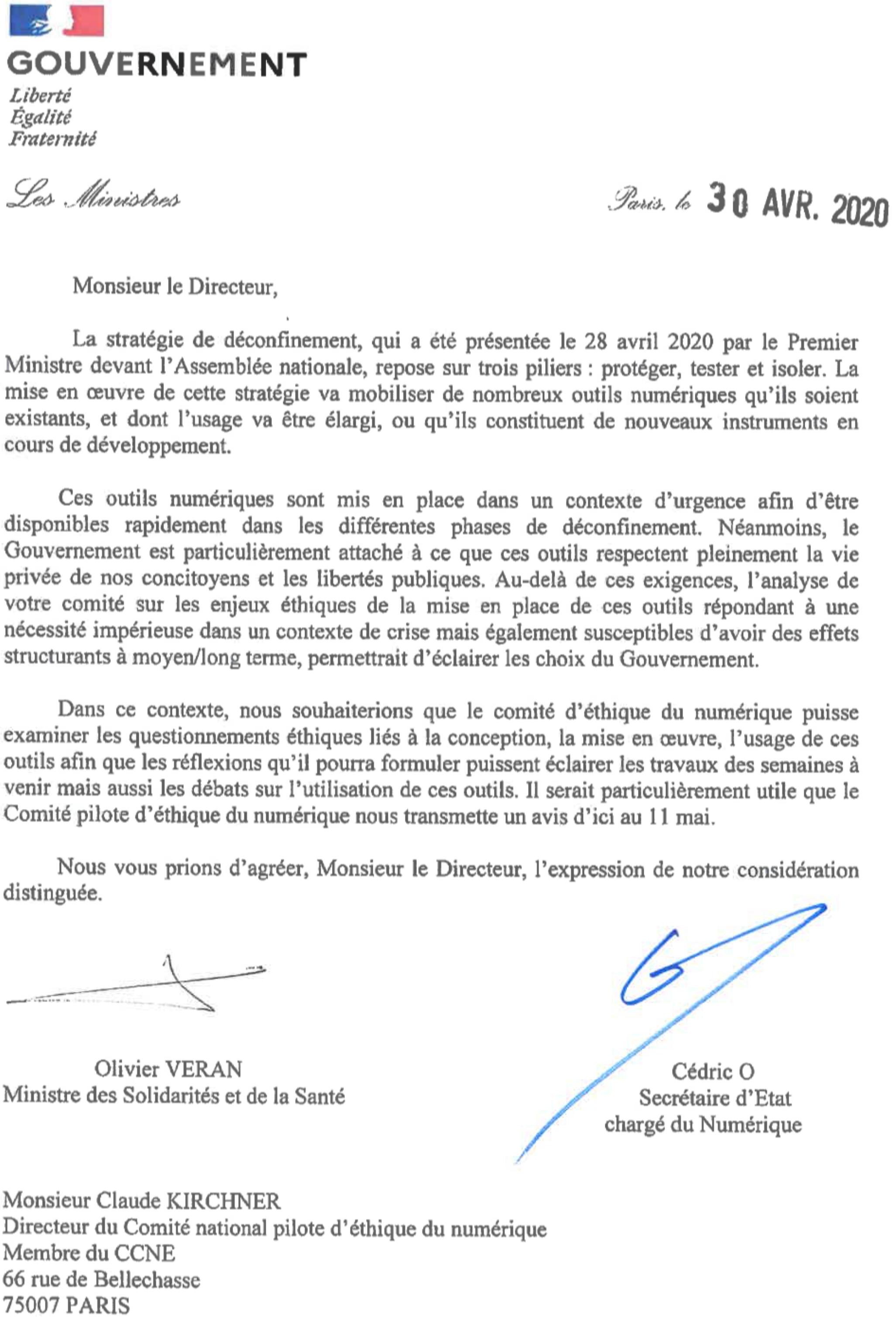
is sick, so that Bob, among others, knows that he has been in contact with an infected person. This method, known as "decentralized" since Zoe no longer plays any role in it, requires a lot of information to be made public. In fact, all the telephones that use it contain the information that person "Xlthlx" is infected, whereas this information is only known to Alice and Zoe in the "centralized" algorithm.

In both "centralized" or "decentralized" protocols, Alice can tell Bob that she has become sick since they met, without Bob having to give Alice—or anyone else—his phone number or name. These protocols are therefore less intrusive than the Contact Book one. It should also be noted that attacks are possible in all cases, for example by stealing Alice's address book in the case of the Contact Book protocol, or by conducting a cyberattack in the case of the two other types of protocols.

A third type of protocol associating unique encrypted identifiers with each encounter and not with each phone, is under development. It could open up a third approach that would not limit the choice to either centralized or decentralized protocols[12].

[12] https://github.com/3rd-ways-for-EU-exposure-notification/project-DESIRE, put online May 9, 2020

Appendix 2: Referral of the Ministers



GOUVERNEMENT
Liberté
Égalité
Fraternité

Les Ministres

Paris, le 30 AVR. 2020

Monsieur le Directeur,

La stratégie de déconfinement, qui a été présentée le 28 avril 2020 par le Premier Ministre devant l'Assemblée nationale, repose sur trois piliers : protéger, tester et isoler. La mise en œuvre de cette stratégie va mobiliser de nombreux outils numériques qu'ils soient existants, et dont l'usage va être élargi, ou qu'ils constituent de nouveaux instruments en cours de développement.

Ces outils numériques sont mis en place dans un contexte d'urgence afin d'être disponibles rapidement dans les différentes phases de déconfinement. Néanmoins, le Gouvernement est particulièrement attaché à ce que ces outils respectent pleinement la vie privée de nos concitoyens et les libertés publiques. Au-delà de ces exigences, l'analyse de votre comité sur les enjeux éthiques de la mise en place de ces outils répondant à une nécessité impérieuse dans un contexte de crise mais également susceptibles d'avoir des effets structurants à moyen/long terme, permettrait d'éclairer les choix du Gouvernement.

Dans ce contexte, nous souhaiterions que le comité d'éthique du numérique puisse examiner les questionnements éthiques liés à la conception, la mise en œuvre, l'usage de ces outils afin que les réflexions qu'il pourra formuler puissent éclairer les travaux des semaines à venir mais aussi les débats sur l'utilisation de ces outils. Il serait particulièrement utile que le Comité pilote d'éthique du numérique nous transmette un avis d'ici au 11 mai.

Nous vous prions d'agréer, Monsieur le Directeur, l'expression de notre considération distinguée.

Olivier VERAN
Ministre des Solidarités et de la Santé

Cédric O
Secrétaire d'Etat
chargé du Numérique

Monsieur Claude KIRCHNER
Directeur du Comité national pilote d'éthique du numérique
Membre du CCNE
66 rue de Bellechasse
75007 PARIS

Hearings held by the working group

Franck Chauvin, Chair of the French High Council for Public Health and member of the COVID-19 Scientific Council

Marc Debrincat, Bruno Gazeau, Anne-Marie Ghermard of the French National Federation of Transport Users Associations

Luciano Floridi, Professor at Oxford University, Member of the Ethics Advisory Board for the NHS COVID-19 app

Hélène Gebel, coordinator of the Space for Ethical Reflection of the Grand Est Region and of the French National Conference of Regional Spaces for Ethical Reflection

Bruno Sportisse, Chairman and Chief Executive Officer of Inria

Composition of the working group that contributed to the preparation of this document

Gilles Adda

Raja Chatila

Theodore Christakis

Laure Coulombel

Camile Darche – editor

Laurence Devillers

Emmanuel Didier

Karine Dognin-Sauze

Gilles Dowek

Valeria Faure-Muntian

Christine Froidevaux – co-rapporteur

Jean-Gabriel Ganascia

Eric Germain

Alexei Grinbaum

David Gruson

Jeany Jean-Baptiste

Claude Kirchner

Caroline Martin

Tristan Nitot

Jérôme Perrin

Catherine Tessier – co-rapporteur

Serena Villata

Célia Zolynski

This text has been translated from its French version with the assistance of David Marsh and the company Coup de Puce Expansion.

Members of the National Pilot Committee for Digital Ethics (CNPEN)

Gilles Adda
Raja Chatila
Theodore Christakis
Laure Coulombel
Jean-François Delfraissy
Laurence Devillers
Karine Dognin-Sauze
Gilles Dowek
Valeria Faure-Muntian
Christine Froidevaux
Jean-Gabriel Ganascia
Eric Germain
Alexei Grinbaum
David Gruson
Emmanuel Hirsch
Jeany Jean-Baptiste
Claude Kirchner - Director
Augustin Landler
Christophe Lazaro
Gwendal Le Grand
Claire Levallois-Barth
Caroline Martin
Tristan Nitot
Jérôme Perrin
Catherine Tessier
Serena Villata
Célia Zolynski

Press contact: communication@comite-ethique.fr

NATIONAL PILOT COMMITTEE FOR DIGITAL ETHICS

COMITÉ NATIONAL PILOTE D'ÉTHIQUE DU NUMÉRIQUE

sous l'égide du

COMITÉ CONSULTATIF NATIONAL D'ÉTHIQUE
POUR LES SCIENCES DE LA VIE ET DE LA SANTÉ