Ethical Challenges in the Digital Age: The Case of Mobile Contact Tracing Applications

By Geneviève FIEUX-CASTAGNET and Gérald SANTUCCI

November 2020

Table of Contents

Personal data, privacy, ethics: what are we talking about?

"Ethics, unlike the law, is above all an interpersonal matter; it cannot be the subject of general rules without taking the path of tartuffery. In the face of any prohibition, let us ask ourselves a single question: to whom does such action directly harm? No one but the perpetrator? So, let it be done, let it live. If need be, let us be indignant: it is all the more legitimate to morally condemn what we have had the courage to tolerate legally."

Gaspard Koenig, philosopher and chairman of the GenerationLibre think tank, Les Echos, 16/09/2020

"The strength of morality is its internal coherence. It is also its weakness: because of its systematization, there is the risk of putting reality in brackets. But the risk of ethics is no less: if it is only an indefinitely open discussion about good and evil, it ends up dissolving these notions in the gossip and becoming, in the end, the register of pathos and opinion. Morality has the hardness of the law, but ethics has the softness of an infinite dialogue. Nowadays, morality has a lot of connotations. One hears "moralizing" behind the word "morality". A discourse that judges..."

Martin Steffens, "Éthique et morale, de quoi parle-t-on", Le Figaro, 28/09/2018

A bit of history...

Never before in the history of mankind have the questions of identification and surveillance of individuals been raised as acutely as they are today.

Europe gave *the green light in* 1995 with the Data Protection Directive, supplemented in 2002 by another directive on the processing of personal data and the protection of privacy in the electronic communications sector (e-privacy).

To be more complete, it should be remembered that Germany was the first country to turn its attention to *privacy*. In fact, it was the region of Hessen which, in 1970, introduced the first data protection law[1], soon followed by the other Länder and then by the federal level[2]. In 1983, the Constitutional Court of the Federal Republic of Germany established that the individual has a constitutional right to self-determination in matters of information. This decision prohibits the processing of personal data unless there is specific statutory authorization or consent from the person concerned. In 1990, a new Federal Data Protection Act incorporated these constitutional requirements.

Before the middle of the eighteenth century, the issue of personal data protection hardly ever arose. Then, over the course of two centuries, due to industrialization and punched cards, it gradually became a topic of discussion, albeit a very limited one. After 1945, the subject became a major topic of public debate with the arrival of large computers (from 1945 onwards), mini-computers (1975), personal computers (1980s) and then computer networks (1990s). This acceleration of change due to digital technologies continued with the nonstop increase in the power of computer systems, the growth in transmission bandwidths and data storage capacities, the permanent reduction in the size of components until they disappeared from the field of vision, the emergence of new concepts (biometrics, speech recognition, geolocation, Artificial

[1] Datenschutzgesetz [Data Protection Act], Oct. 7, 1970, HESSISCHES GESETZ-UND VERORDNUNGSBLATT I

[2] Act Concerning the Abuse of Personal Data in Data Processing, Jan. 27, 1977, BGBL I at 201

Intelligence, blockchain, etc.) and the appearance of ubiquitous data processing (pervasive computing, ubiquitous networks, Internet of Things, Cyber-Physical Systems, etc.).

The "right to privacy" was first established in the United States by Boston lawyers Samuel WARREN and Louis BRANDEIS[3] :

"That the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection. Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the new demands of society. Thus, in very early times, the law gave a remedy only for physical interference with life and property, for trespasses. Then the "right to life" served only to protect the subject from battery in its various forms; liberty meant freedom from actual restraint; and the right to property secured to the individual his lands and his cattle. Later, there came a recognition of man's spiritual nature, of his feelings and his intellect. Gradually the scope of these legal rights broadened; and now the right to life has come to mean the right to enjoy life, – the right to be let alone."

This "right to be let alone" constitutes the first legal loophole in the broad debate on privacy that followed. At the time, it was only an essentially *physical* right, i.e. a right to maintain a certain distance from others. It was in line with the American idea of the "pursuit of happiness" contained in the Declaration of Independence of 4 July 1776: "*We hold these truths to be self-evident, that all men are created equal, that they are endowed by their Creator with certain unalienable Rights, that among these are Life, Liberty and the pursuit of Happiness. – That to secure these rights, Governments are instituted among Men, deriving their just powers from the consent of the governed (...)*". The advent of information technology and the ensuing digital explosion have obviously shaken up the concept of privacy, provoking exciting and endless, and so far unsuccessful, debates on personal data, privacy and ethics.

[3] WARREN (Samuel D.) and BRANDEIS (Louis D.), "The Right to Privacy", Harvard Law Review, Vol. IV, December 15, 1890 No. 5

Evolution of data protection rules around the world

Year	Country	Title
1972	Germany (Hesse Region)	Data Protection Act
1974	United States	Federal Privacy Act
1977	Federal Germany	Data Protection Act
1980	OECD	Privacy Guidelines
1981	Council of Europe	Convention 108 for the protection of personal data
1995	European Union	Data Protection Directive 95/46/EC
2000	European Union	Protection of personal data in the Charter of Fundamental Rights of the European Union (Article 8)
2002	European Union	Directive on privacy and electronic communications (e-privacy)
2005 (updated in 2015)	APEC (Asia-Pacific Economic Cooperation)	Privacy Framework
2016	European Union	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

At the turn of the 21st century, new issues related to digital technologies and the "transformation" they bring with them have emerged, which raise the questions of personal data protection, privacy and ethics in a new way.

These technologies include the Internet of Things, Ambient Intelligence, RFID (radio frequency identification) and NFC (Near Field Communication), Affective Computing, Cloud Computing, Bioelectronics, Neuroelectronics, Artificial Intelligence, Human-Machine Symbiosis.

Let's take a few examples.

The Internet of Things (IoT), a concept that emerged in 1999, refers to the idea of objects "chatting" with each other and with humans. Digital systems are everywhere (notion of ubiquity) and they are invisible because of the increasingly small size of microprocessors, RFID (radio frequency identification) tags and other devices embedded in everyday objects. Threats are mainly:

- the sum of all the small traces of information that a person leaves behind unintentionally every time she takes part in daily activities using a digital service, such as the Internet or a mobile phone (*data shadows*), i.e. every click leaves a digital trace,
- behavioral profiling, and

- data manipulation.

The Internet of Things not only refers to the computer network that connects objects, it also refers to the concept of the *object*, which, as science fiction author Bruce Sterling[4] has shown, has metamorphosed over time. First an *artefact* (i.e. a rudimentary tool linked to hunting and agricultural civilizations), then a *machine (*i.e. a complex object based on an artificial energy source), and finally a *product* (i.e. a manufactured object reproduced in a large number of identical copies), the object in the digital age can also be a *gizmo* (i.e. a complex object, such as software, which is more difficult to simplify than to increase, which requires learning on the part of its users and which relies on other objects to exist) or a *spime (*i.e. an object that is traceable, identifiable, locatable, equipped with digital devices, e.g. RFID chips, and existing in a network). If we look further into a distant future (around 2060, according to Sterling), with in particular the Nano-Bio-Info-Cogno (NBIC) convergence, the object would become a *biot*, i.e. an entity that would be both an object and a human!

Nanotechnologies operate on a scale of 1 to 100 nanometers (nm) and make it possible to create and use structures, components and systems which, because of their small size, have new properties and functionalities that we are trying to transpose to the macroscopic scale in order to take advantage of them. These technologies are invisible to the naked eye, even with the help of a magnifying glass, and they make it possible to capture information such as temperature, voltage and pressure.

These technological advances refer to the image of the "digital dust", i.e. particles on a molecular scale capable of tracing and tracking individuals, without them being aware of it, thanks to various independent measurements whose data are transmitted and received through digital networks.

More recently, Artificial Intelligence and 5G have complemented the digital technologies already in deployment.

Personal data

The notion of "personal data" is not as easy to characterize as one might think. In Directive 95/46/EC its definition is worded as follows:

"any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."

The General Data Protection Regulation 2016/679 updated this definition by introducing the notion of "identifier" which complements the previous notion of "identification number" and by adding the "genetic" identity to the specific elements that may identify a natural person:

"any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

[4] STERLING, Bruce, *Shaping Things*, The MIT Press, October 2005

In a 2007 opinion, the Article 29 Data Protection Working Party had reviewed and analyzed the constituent elements of this definition[5]:

- "any information"
- "concerning"
- a "natural person"
- "identified or identifiable"

This long-standing opinion is still relevant to clarify the definition of "personal data" in the 2016 regulation.

The general observation is that the intention of the European legislator was to adopt a broad concept of personal data in order to ensure the protection of the fundamental rights and freedoms of natural persons, in particular their privacy, with regard to the processing of personal data. There was a consensus that the scope of the data protection rules should not be too broad but at the same time that undue restrictions on the interpretation of the concept of personal data should be avoided. Data protection authorities, such as CNIL in France, "play an essential role in achieving an appropriate balance in the scope of the Directive."

The respect of privacy

Although the concept of *privacy is an* old one[6], there has not been a broad consensus on its interpretation so far. Privacy is recognized as a fundamental human right in the Universal Declaration of Human Rights (Article 12), the International Covenant on Civil and Political Rights (Articles 14 and 17) and in many other international and regional human rights conventions. In particular, it reinforces the values of human dignity, freedom of association and freedom of speech. The appointment by the Human Rights Council in July 2015 of the first Special Rapporteur on the right to privacy[7] reflects the growing importance of this right in global digital policies.

The increasing sophistication of information and communication technologies, including the possibility to collect, analyze and disseminate personal data, has led to a need for legislation in many countries. Over the last thirty years, the level of information generated by each individual has reached new heights due to advances in health, telecommunications, transport systems and financial transfers. Computers, linked to broadband networks, generate records on each individual without the need for a single central computer system.

It is not easy to distinguish between the notions of "privacy" and "protection of personal data". Depending on the situation, one may be perceived as encompassing the other. However, lawyers agree that "data protection" refers to the legal mechanism for ensuring "privacy". The term *privacy* refers to the right of every citizen to control his or her personal information and

---

5 Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, 20 June 2007

6 The notion of the right to privacy can be traced back to the fourteenth century, particularly in England. See BANISAR, David, and DAVIES, Simon, "Privacy and Human Rights: An International Survey of Privacy Laws and Practice", The John Marshall journal of computer & information law, 1999, https://www.gilc.nl/privacy/survey/

7 https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx

to decide how it will be used (i.e. whether or not to reveal it). Specialists in these matters most often consider that the term *privacy* can refer to the following[8]:

1. privacy of the natural person
2. privacy of data and image
3. privacy of personal communication
4. privacy of behavior and action
5. privacy of location and space
6. privacy of thoughts and feelings
7. privacy of association, including group privacy

In the United States, the prevailing concept is the one of *privacy*, while in the European Union it is the one of "protection of personal data". It should be noted that the General Data Protection Regulation does not provide a definition of "privacy", nor does the old 1995 Directive. Thus, for example, in the United States the term "Privacy Impact Assessment" (PIA) is used, whereas in Europe the term "Data Protection Impact Assessment" (DPAI) is preferred, which is one of the most important concepts of the current European General Data Protection Regulation. The American and European conceptions are opposed in that Europe favors an overall legislative framework while the United States develops privacy regulations for each sector of the economy, for example for financial services (the Gramm-Leach-Bliley Act), children's privacy on the Internet (the Children's Online Privacy Protection Act) or the medical field (the Health Insurance Portability and Accountability Act).

Another important difference between the two regions of the world concerns the authority responsible for enforcing the rules: in Europe it is the public authorities, whereas in the United States it is businesses and individuals who decide for themselves, which puts the latter in a weak position since they are often little or poorly informed about the privacy implications of the options offered by the private sector. In 2016, the European Commission and the United States agreed on a legal framework for transatlantic data transfers: the "EU-US Privacy Shield" to protect the fundamental rights of EU citizens when their data is transferred to the US and to provide legal certainty for businesses[9]. But on 16 July 2020, the European Court of Justice (CJEU) ruled that this framework did not sufficiently protect European data and therefore risked infringing citizens' rights, in line with the GDPR: "*As regards a level of protection essentially equivalent to the fundamental rights and freedoms guaranteed within the EU, the Court finds that, under EU law, legislation is not limited to what is strictly necessary where it authorizes, on a generalized basis, storage of all the personal data of all the persons whose data is transferred from the EU to the United States without any differentiation, limitation or exception being made in the light of the objective pursued and without an objective criterion being laid down for determining the limits of the access of the public authorities to the data and of its subsequent use.*"

The CJEU ruling is obviously bad news for businesses, which still prefer to have reliable and stable mechanisms for sending data from the EU to the US. It creates an obstacle to e-commerce between the EU and the US at a time when global trade relations are increasingly strained. On

---

8 WRIGHT, David, and DE HERT, Paul (Eds.), Privacy Impact Assessments, Springer, Dordrecht, 2012

9 The "*EU-US* Privacy *Shield*" meets the requirements set out by the Court of Justice of the European Union in its ruling of 6 October 2015, which declared the former Safe Harbor regime invalid (Safe Harbor, 2000).

https://ec.europa.eu/commission/presscorner/detail/fr/IP_16_216

the other hand, it is a victory for privacy advocates who had rightly argued that the privacy shield did not sufficiently cover European data.

Ethics

Ethics emerged in the public debate and on the political agenda of public authorities around the world when the Internet of Things (IoT) and Artificial Intelligence (AI) spread to almost every corner of the economy and society. Ethics raises a broader issue than the protection of personal data or privacy, even if it encompasses the latter.

Values and privacy

The word "ethics" is not new: Aristotle defined its contours in his "Nicomachean Ethics"[10] before many authors, from Spinoza to Wittgenstein, added their contribution to the edifice. Leaving aside the Aristotelian universe and its "virtues" (e.g., courage, temperance, generosity, greatness of soul, pride, healthy ambition, gentleness, truthfulness, humor, kindness, correctness), the design of an ethical system in the Machine Age should be based on positive values. But it is difficult to agree on what *value* is! Philosophers like Epicure and Jeremy Bentham recognize only one value: human happiness. But most other philosophers and psychologists believe that there are a large number of "intrinsic values" such as knowledge, beauty, health, truth, power or harmony, to which should be added "extrinsic values", i.e. instrumental values, which support the attainment of intrinsic values. The most important of these extrinsic values is, of course, privacy.

However, as Karl Popper, Martin Heidegger and other philosophers and epistemologists have shown, value does not exist *per se* if man does not act on it. Thus, for example, for transhumanists, humans can be seen as sub-optimal biological systems compared to machines with Artificial Intelligence. They place their ideal in machines considered superior to humans, which, no doubt, through manipulation by some malicious minds, could have deadly consequences for human societies.

Based on the work of the psychologist Abraham Maslow, the academic Sarah Spiekermann has grouped the eighteen intrinsic values of the former around only seven[11]:

- two prerequisites: knowledge (true opinion, understanding), freedom (independence, free choice);
- five basic needs: physiological needs (health and strength, prosperous life, activity), safety needs (peace, safety, security), belongingness and love needs (true friendship, cooperation, love), esteem needs (power, achievement, self-respect, reputation, honor, social recognition), the need for self-actualization.

Privacy is an extrinsic value that plays a key role in all these intrinsic values. The link between "values" and "privacy" is thus established. This is why it is important to ensure the protection of the above-mentioned values in current and future IT environments, especially with regard to Artificial Intelligence.

---

10 "Virtue is an acquired disposition of the will, consisting in a middle way relative to us, which is determined by the right rule and as a prudent man would determine."

11 SPIEKERMANN, Sarah, Ethical IT Innovation: A Value-Based System Design Approach, CRC Press, Taylor & Francis Group, 2016, chapter 4, pp.39-45.

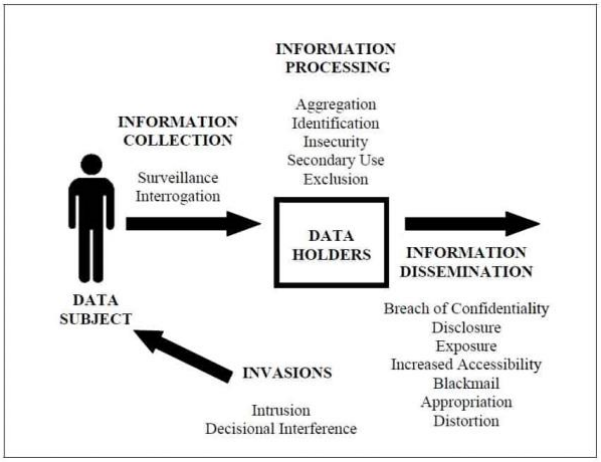
Daniel Solove, an American law professor at George Washington University Law School, proposed an interesting taxonomy of privacy in 2006, showing that most of the problems stem from the information generated about individuals.

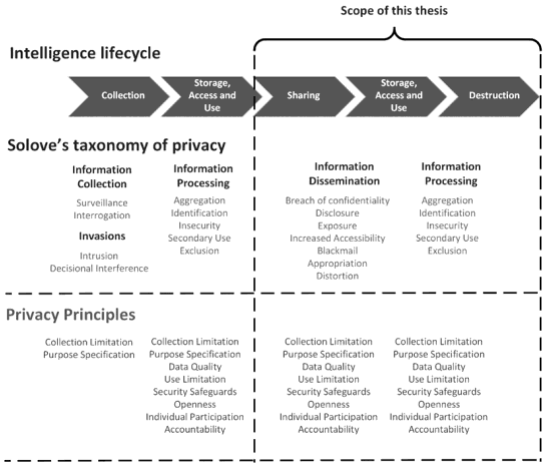
The collection of information raises two risks in relation to privacy:

- surveillance, which consists of surreptitiously spying, listening or recording a person's various activities;
- interrogation, which consists of putting pressure on a fully conscious person to disclose information about him or her.

The processing of information raises other risks:

- the aggregation of various pieces of information about an individual;
- the identification of a person on the basis of various information related to him/her;
- insecurity, which results from negligence in the protection of stored information, which may lead to possible leaks or unauthorized access;
- secondary use of stored information which, without a person's consent, is diverted from its original purpose.





The figure of man in the 21st century between the "intelligent machine" and the "augmented human"

By referring more or less explicitly to these values – intrinsic and extrinsic – ethical debates today are closely linked to two major revolutions that are unfolding in parallel at an ever-increasing pace.

Firstly, the *intelligent machine*, i.e. essentially robots and autonomous systems, to which should be added connected objects (or the Internet of Things). It is driven by a double revolution, that of Artificial Intelligence, which allows man to create a "non-biological intelligence" superior to human intelligence, and that of nanotechnology, which allows him to manipulate matter at the molecular and atomic levels. The machines of the future will thus be equipped with unprecedented capabilities: they will be able to gather resources far beyond what man is capable of; they will possess super-powerful memories; and they will be able to operate 24 hours a day, connected around the world, combining the best skills without ever leaving the level of

maximum performance. This raises the central question of the relationship between humans and machines. In what way could humans keep control of what the machine will do?

Perhaps the answer lies in the "*augmented human*", the second great revolution of our time. The augmented human is one whose various dimensions, particularly physical and cognitive, are "enhanced" by the new technologies evolving at the confluence of nanotechnologies, biotechnologies, information technologies and cognitive sciences (NBIC). The idea is not new, but it was presented in a detailed and coherent manner in 2002 in a visionary report by the National Science Foundation (NSF) and the American Department of Commerce (DOC). Only an "augmented man" would be able to compete with the growing capabilities of machines and a future Artificial General Intelligence (AGI).

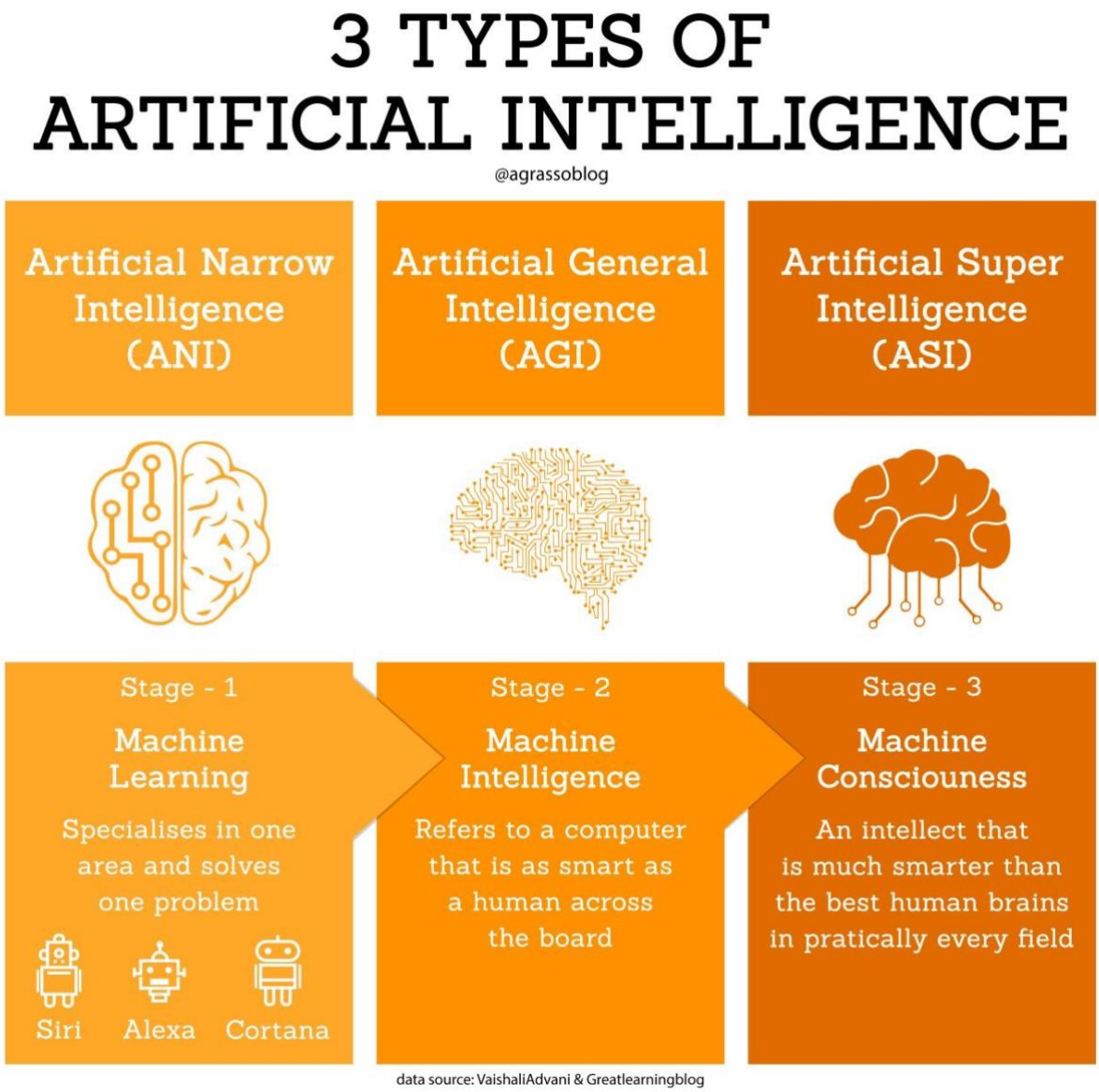
The NBIC convergence is today enriched by another revolution, that of genetics, which allows man to reprogram his own biology. Thus, the "human-machine", post-human, or even trans-human, is the one who, by possessing the codes of his own making, will be able to modify its structure, to endow it with superpowers that will free it from the physical, biological and cognitive limits to which humanity remains subject until now. The augmented human allows us to glimpse the realization of the dream of extreme longevity, of increased strength, resistance and intelligence, of a regained freedom of the body.

The sketch of such an improvement in performance was the subject of strong media recognition in France when in 2019 a young quadriplegic succeeded in controlling his exoskeleton thanks to electrodes implanted in his skull[12]. This revolution holds undeniable promise, but it also raises fundamental questions for the "future of the future" of human beings[13]. Will the augmented human have to rely at some point on other actors to activate, modify or maintain his "augmentation"? In this case, will these actors be able to take cognizance of the personal data of individuals, or even control them remotely? What risks would there be that augmented humans would come under the control of malicious people? What could be the impact of this augmented human on society itself, for example how will human relations evolve, in terms of emotional interactions and solidarity, and social relations, in terms of non-discriminatory access to work?

---

[12] "A tetraplegic patient managed to walk thanks to an exoskeleton connected to his brain", Le Monde, 4 June 2019.

[13] Geneviève Fieux-Castagnet and Kamel Bentchikou, Les exosquelettes connectés et leurs enjeux éthiques, PromEthosIA, 12 December 2019, https://promethosia.com/intelligence-artificielle-un-defi-de-civilisation-un-devoir-de-generation/



The question also arises as to how the cohabitation will be exercised between, on the one hand, the augmented human, endowed with extraordinary capacities but also incited by regulation or by "soft manipulations" (*nudge*) to regulate his behavior on norms and codes, and, on the other hand, intelligent machines, perhaps soon to have their own "consciousness". On the one hand, we might have *subjects* transformed into quasi-objects because of their obligation to conform to behaviors deemed "normal" and, on the other hand, *objects* transformed into quasi-subjects thanks to autonomous and self-learning Artificial Intelligences capable of making decisions without human control. It would be very interesting for scientists and philosophers to study these questions, the former to understand the profound transformations that these developments will bring about in the human brain and biological behavior, the latter to reflect on the contours of the new relationships between human and the world around it.

The authors of the twentieth century set out to characterize the human figures of History, reviewing the Saint, the Hero, the Knight, the Wiseman, and finally the *honest man of the* seventeenth century. Paraphrasing Saint-Augustin, French philosopher Emmanuel Mounier wondered, not without cynicism, whether the twentieth century had not given birth to the

satisfied mediocre. Let's disregard all that. Isn't it now the *hyper-connected man* who becomes the new figure around whom society is reorganizing itself?

Psychologists warn us, however, that virtual sociability has only a relative significance: "virtual friends" are far removed from the model of Montaigne and La Boétie, exchanges on forums do not really erase the impression of being strangers to others, the feeling of loneliness or isolation does not disappear, on the contrary! New pathologies such as chronic fatigue, digital addiction, loss of concentration, burnout follow. Consequently, the proliferation of social interactions is at best a palliative to the feeling of abandonment and loss of control over their lives of the majority of human beings. Moreover, has not this hyper-connected human become above all an augmented consumer that is profiled thanks to the traces he/she leaves on websites and social networks, which encourage him/her to consume more? The risk is also that s/he loses control of his critical thinking, locked in an information bubble that makes him/her vulnerable to forms of intellectual and political manipulation. To what extent should we accept to let the technologies designed and implemented by a small number of giant, increasingly dominant technology companies ("big tech"), for the moment based in the United States and China, read our thoughts, decipher our emotions, guess our needs and desires, decide how the content of our thoughts will be protected?

Ethical principles in Artificial Intelligence

With a bit of humor, one could say that defining ethical principles for Artificial Intelligence is easy: haven't almost all countries and all types of organizations done it? More than for other disruptive digital technologies, such as the Internet of Things or 5G, the values and principles likely to guide the development and deployment of Artificial Intelligence in the economy and society mobilize the interest, commitment and participation of all stakeholders on all continents. There is no shortage of books, articles, reports, "declarations" and other written documents on the subject, and the ocean of contributions, in addition to highlighting the attractiveness of the subject, and underlining the concerns it generates, has continued to grow since the year 2017.

In order to tighten the analytical framework, we have chosen to refer to seven sources of information, the last of which, that of the European Commission, will be detailed in the following section:

1. The 23 Asilomar principles for the ethical development of Artificial Intelligence [14]
2. The Montreal Declaration for the Responsible Development of Artificial Intelligence [15]
3. The general principles set out in the IEEE Global Initiative [16]
4. The five principles making up the British House of Lords' "IA Code" [17]
5. The work of the Partnership on Artificial Intelligence, a multi-stakeholder body comprising academics, researchers, civil society organizations and companies that contribute to the development and use of Artificial Intelligence. [18]

---

[14] Future of Life Institute, "Asilomar AI principles", Conference Asilomar, January 2017, https://futureoflife.org/ai-principles/

[15] Montreal University, "The Montreal Declaration for a Responsible Development of Artificial Intelligence", November 3, 2017, https://recherche.umontreal.ca/english/strategic-initiatives/montreal-declaration-for-a-responsible-ai/

[16] The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems, 2020, https://standards.ieee.org/content/dam/ieee-standards/standards/web/governance/iccom/IC16-002-Global_Initiative_for_Ethical_Considerations_in_the_Design_of_Autonomous_Systems.pdf

[17] House of Lords, Select Committee on Artificial Intelligence, " AI in the UK: ready, willing and able?", 16 April 2018, https://publications.parliament.uk/pa/ld201719/ldselect/ldai/100/100.pdf

[18] Partnership on AI, 2018, https://www.partnershiponai.org

6. The ethical framework provided by AI4People[19], which is based on the four fundamental principles of bioethics (beneficence, non-maleficence, autonomy and respect for autonomy, justice) and adds a new one: explicability, which includes intelligibility and responsibility.

The good news is that if we sift through the different principles provided in the previous documents – some 50 in total – we find a strong coherence between them and therefore it is possible to group them into a few broad categories. This is what the European Commission has been able to do, and this is why we will rely heavily on the results of its work.

It should already be pointed out that the values and ethical principles concerning Artificial Intelligence (we could also have mentioned the Internet of Things or 5G) provide a robust basis for further examination of the particular case of mobile applications for contact tracing in the context of the Covid-19 pandemic, bearing in mind that each particular case raises specific questions that need to be recognized and taken into account.

Europe at the forefront of ethical thinking

The European Union is taking a global leadership role in the reflection on "trustworthy AI"[20]. In April 2019, the High-Level Expert Group (AI HLEG) that the European Commission had set up in June of the previous year published its guidelines on ethics in the field of Artificial Intelligence. According to European experts, seven principles are needed to achieve trustworthy Artificial Intelligence:

[19] AI4People's Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations", November 2018, https://www.eismd.eu/wp-content/uploads/2019/11/AI4People's-Ethical-Framework-for-a-Good-AI-Society_compressed.pdf

[20] European Commission, Shaping Europe's digital future, Report/Study, Ethics guidelines for trustworthy AI, 8 April 2019, https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

Human agency and oversight

AI systems should empower human beings, allowing them to make informed decisions and fostering their fundamental rights. At the same time, proper oversight mechanisms need to be ensured, which can be achieved through human-in-the-loop, human-on-the-loop, and human-in-command approaches.

Technical robustness and safety

AI systems need to be resilient and secure. They need to be safe, ensuring a fall back plan in case something goes wrong, as well as being accurate, reliable and reproducible. That is the only way to ensure that also unintentional harm can be minimized and prevented.

Privacy and data governance

Besides ensuring full respect for privacy and data protection, adequate data governance mechanisms must also be ensured, taking into account the quality and integrity of the data, and ensuring legitimized access to data.

Transparency

The data, system and AI business models should be transparent. Traceability mechanisms can help achieving this. Moreover, AI systems and their decisions should be explained in a manner adapted to the stakeholder concerned. Humans need to be aware that they are interacting with an AI system, and must be informed of the system's capabilities and limitations.

Diversity, non-discrimination and fairness

Unfair bias must be avoided, as it could have multiple negative implications, from the marginalization of vulnerable groups, to the exacerbation of prejudice and discrimination. Fostering diversity, AI systems should be accessible to all, regardless of any disability, and involve relevant stakeholders throughout their entire life circle.

Societal and environmental well-being

AI systems should benefit all human beings, including future generations. It must hence be ensured that they are sustainable and environmentally friendly. Moreover, they should take into account the environment, including other living beings, and their social and societal impact should be carefully considered.

Accountability

Mechanisms should be put in place to ensure responsibility and accountability for AI systems and their outcomes. Auditability, which enables the assessment of algorithms, data and design processes plays a key role therein, especially in critical applications. Moreover, adequate an accessible redress should be ensured.

On 17 July 2020, the AI HLEG presented the final Assessment List for Trustworthy Artificial Intelligence (ALTAI[21]). This accessible and dynamic assessment list is intended to enable developers and deployers in companies and other organizations to self-assess the reliability of their Artificial Intelligence (AI) systems under development.

[21] https://ec.europa.eu/digital-single-market/en/news/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment

The work of AI HLEG, which is enshrined in an overall strategy on Artificial Intelligence[22], will soon be complemented by new research and innovation (R&I) projects, namely those to be developed in the Horizon Europe 2021-2027 programme[23].

The commitment of the European Union, spurred on by the European Commission, on the theme of ethics, not only with regard to Artificial Intelligence, but also in other areas such as biomedical research, natural sciences and the humanities, should be highlighted. The Charter of Fundamental Rights of the European Union and the European Convention on Human Rights are the European Commission's main reference points. As a result, the most frequently addressed issues are: the involvement of children, patients and vulnerable persons; the use of human embryonic stem cells; privacy and protection of personal data; misuse or malicious use; environmental impact.

By affirming its determination on ethics, the European Union is continuing the process that led to the General Data Protection Regulation (GDPR) in 2016. In this regard, it should be noted that the European Data Protection Supervisor (EDPS) issued a statement on 19 March 2020 in which it states that "even in these exceptional times, the data controller must ensure the protection of the personal data of the data subjects."[24] This protection is indeed a fundamental dimension of privacy of individuals and, therefore, of ethical conduct in any digital contact tracing application.

---

22 https://ec.europa.eu/digital-single-market/en/artificial-intelligence

23 https://ec.europa.eu/info/horizon-europe-next-research-and-innovation-framework-programme_en

24 https://edpb.europa.eu/news/news/2020/statement-edpb-chair-processing-personal-data-context-covid-19-outbreak_en

Ethics and algorithms: can they converge?

The "values" that define ethics and the seven 'principles' that the European Commission has drawn from them with regard to 'Trustworthy Artificial Intelligence' may come up against algorithms that are neutral to them. It will be some years before we know whether Artificial Intelligence can be developed in an ethical way. For the time being, it must be borne in mind that Artificial Intelligence algorithms are amoral, as is the case, for example, when they commit racial discrimination. Therefore, the development of ethical Artificial Intelligence should not only be a matter for lawyers and regulators, but also for scientists[25]. Scientists are well aware that Artificial Intelligence is a "black box": the computer is able to distinguish a cat from a dog, but no one knows exactly how it arrived at the right conclusion! In order to obtain ethical Artificial Intelligence, it is essential to understand why algorithms make mistakes; this is how a new field of research in Artificial Intelligence, the "quantification of uncertainty", has recently emerged, with the aim of helping to develop a clear and accurate way of communicating the margin of error of an algorithm.

However, not all ethical challenges can be met with technical solutions alone. As we saw when we discussed the subject of "values" above, ethical dilemmas, by their nature, are subjective and, therefore, require individuals to resolve their conflicting priorities among themselves. The well-known example is that of the autonomous car which, in the event of an unavoidable accident in the city, would have to "choose" between swerving to spare the lives of its three passengers, among whom is a child, or causing the death of four elderly pedestrians. Depending on their cultures, individuals who are asked about this dilemma may respond differently: in China and Japan, where cultures attach greater weight to the community, the probability of sacrificing pedestrians is lower than elsewhere where cultures place greater importance on the individual. This case taken to its extreme raises a question that mathematics and technical advances cannot answer: if I buy an autonomous car that has been programmed in France and drive it in Asia, what ethics should it be subject to?

The conclusion to be drawn from this analysis is that the development of trustworthy Artificial Intelligence requires the commitment and participation of all actors: experts from all disciplines, social scientists, ethicists. This is why the European Commission should ensure that over the next few years AI HLEG will continue to work closely with scientists, engineers and other participants in future Horizon Europe R&I projects.

Contact tracing in the case of Covid-19: ethical issues between the health emergency and a mosaic of solutions

An outbreak of viral-like pneumonia of unknown etiology emerged in the city of Wuhan (Hubei province, China) in December 2019. On 9 January 2020, the discovery of a new coronavirus (called 2019-nCoV, then SARS-CoV-2) was officially announced by the Chinese health authorities and the World Health Organization (WHO). This coronavirus is the agent responsible for the new infectious respiratory disease called Covid-19 (for COronaVIrus Disease). SARS-Cov-2 is transmitted from person to person by air, forming a chain of contaminations: an infected person transmits the virus to another person who in turn infects another person, etc. The virus is then transmitted to the infected person by air. The fight against

[25] "Physicists Must Engage with AI Ethics, Now", Physics, 09/07/2020, https://physics.aps.org/articles/v13/107: "AI is shaping our world, our lives, our rights, and our futures every day. As scientists and citizens, we must actively engage to ensure AI develops and is utilized in an ethical and equitable manner."

the spread of the coronavirus therefore involves identifying and breaking the chains of contamination.

In order to support this break, digital solutions for searching for infected people and identifying individuals with whom they have been in close and prolonged contact have been developed from the first weeks of the new coronavirus' spread. Initially used in Asia, notably in Singapore (*Trace Together*) and China (*Close Contact Detector*), contact tracing solutions were then developed in Western countries where they generated often heated debates concerning their effectiveness and respect for individual privacy (non-respect of medical secrecy or individual privacy, limitation of individual freedoms).

Almost everyone agrees that the digital tool must be integrated into a wider system. For the epidemic to be extinguished, it is not enough for individuals to use an application on their mobile phone; it is also necessary to involve people in the field to carry out the investigation work (*contact tracers*).

Digital solutions for contact search: a difficult to set up

"*A new Covid tracking application is launched in England and Wales*" (source: Financial Times, 24/09/2020), "*How Jean Castex killed StopCovid in one sentence*" (source: Le Figaro 25/07/2020). Nine months after the discovery of the new coronavirus, seven months after there was no longer any doubt that the new virus would lead to a pandemic, these two press headlines show just how difficult it was for the public authorities to set up independent contact tracing applications. The UK and France were the two main countries to reject the initial offer of technical assistance from Apple and Google, while the two "big tech" companies were at the same time working with medical authorities in several other European countries, including Germany and Italy, to introduce contact tracing technology into their mobile networks.

The chronology of events in the UK reveals some interesting lessons:

- 31 January: confirmation of the first two cases of coronavirus; the National Health Service (NHS) announces that it will track down all contacts of these patients;
- 29 February: Britain's health department announces a total of 10,483 people have been tested in the UK, of which 10,460 were confirmed negative and 23 positive, the department said in a statement;
- 12 March: the "containment" phase of the epidemic is replaced by a "delay" phase: from now on, efforts are no longer focused on seeking out contacts of known patients but on reducing the peak of infections to ensure that the sickest patients can receive the care they need (the so-called "flattening the curve" strategy);
- 23 March: The Prime Minister orders British people to stay at home and asks the police to impose this decision of national confinement[26];

[26] UK Prime Minister's statement on coronavirus, 23 April 2020: "*The coronavirus is the biggest threat this country has faced for decades – and this country is not alone. All over the world we are seeing the devastating impact of this invisible killer (…) Without a huge national effort to halt the growth of this virus, there will come a moment when no health service in the world could possibly cope; because there won't be enough ventilators, enough intensive care beds, enough doctors and nurses (…) To put it simply, if too many people become seriously unwell at one time, the NHS will be unable to handle it - meaning more people are likely to die, not just from Coronavirus but from other illnesses as well. So, it's vital to slow the spread of the disease (…) From this evening I must give the British people a very simple instruction - you must stay at home. Because the critical thing we must do is stop the disease spreading between households (…) If you don't follow the rules the police will have the powers to enforce them, including through fines and dispersing gatherings (…) No Prime Minister wants to enact measures like this. I know the damage that this disruption is doing and will*

- 12 April: The government announces that it will develop a contact tracking application[27];
- 17 April: The United Kingdom announces that it will rebuild teams of "contact tracers" as part of a new testing and tracing strategy;
- 5 May: The health secretary, Matt Hancock, announces the launch of a mobile phone contact tracing application, tested on the Isle of Wight, as part of the "Test, Track and Trace" strategy to track and isolate the virus in order to prevent it from reoccurring; the application uses Bluetooth signals to map contacts between users and alert those who have been close to an infected person;
- 8 May: In response to strong criticism following the first announcement, notably from privacy advocates concerned that anonymized data will be stored in a central database, the NHS announces that it is already working on a second version of the application incorporating technology provided by Google and Apple;
- 28 May: following the decision announced on 17 April, the manual search for contacts is resumed thanks to the recruitment and training of 25,000 people dedicated to this mission;
- 18 June: The United Kingdom turns around by abandoning the technology developed by its health services in favor of that of Apple and Google; during the pilot phase carried out on the Isle of Wight, the centralized application only recognized 4% of Apple's mobile phones and 75% of Google's Android devices;
- 13 August: Tests are announced for a new application based on a decentralized model;
- 24 September: the NHS launches the new application – called NHS Covid-19 – which immediately meets with considerable success (one million downloads on the first day).

do to people's lives, to their businesses and to their jobs. And that's why we have produced a huge and unprecedented programme of support both for workers and for business (…) And yet it is also true that there is a clear way through. Day by day we are strengthening our amazing NHS with 7500 former clinicians now coming back to the service. With the time you buy, by simply staying at home, we are increasing our stocks of equipment. We are accelerating our search for treatments. We are pioneering work on a vaccine. And we are buying millions of testing kits that will enable us to turn the tide on this invisible killer (…) Each and every one of us is now obliged to join together. To halt the spread of this disease. To protect our NHS and to save many many thousands of lives. And I know that as they have in the past so many times. The people of this country will rise to that challenge. And we will come through it stronger than ever. We will beat the coronavirus and we will beat it together. And therefore, I urge you at this moment of national emergency to stay at home, protect our NHS and save lives. Thank you."

[27] Health and Social Care Secretary Matt Hancock: "*If you become unwell with the symptoms of coronavirus, you can securely tell this new NHS app, and the app will then send an alert anonymously to other app users that you've been in significant contact with over the past few days, even before you had symptoms, so that they know and can act accordingly. All data will be handled according to the highest ethical and security standards and would only be used for NHS care and research and we won't hold it any longer than it's needed. And, as part of our commitment to transparency, we will be publishing the source code too. We're already testing this app and, as we do this, we're working closely with the world's leading tech companies and renowned experts in clinical safety and digital ethics so that we can get this right.*"

Source: Financial Times, 1/05/2020

In conclusion, it took the UK five months to bridge the gap between the decision to search for contacts using digital technology (April) and the actual launch of the application (September). In a tense context where public authorities had to deal with a sudden health threat of uncertain origin and unpredictable course, it was necessary to put in place an arsenal of emergency measures among which, in the absence of treatment and a vaccine, contact tracing appeared to be indispensable. This search had to be carried out in the traditional way with appropriately trained teams, but also thanks to the development of digital applications based on the high-performance and omnipresent technologies available to mankind today.

France found itself in a similar situation to the United Kingdom, but it seems that the objective of technological independence from the GAFA, in this case Google and Apple, has become at least as important to the authorities as that of privacy. The case of this country and its *TousAntiCovid* app will be examined in detail later. It is worth remembering that by the end of September 2020, the French application, launched four months earlier on 2 June, had been downloaded only about 3 million times, while the German application, launched on 16 June, had been downloaded 18 million times and the British application 12.4 million times in just four days. [28]

Beyond the technical, regulatory and societal vicissitudes of the year 2020, there is no doubt that if the pandemic persists, the need to use technology to search for contacts of people who are infected or who have been identified as having crossed paths with infected people will be greater than ever. Less than a year after the start of the pandemic, the development of contact tracing applications continues worldwide, but unevenly. In most countries, particularly in Europe, debates are heating up over the balance to be struck between privacy and efficiency. As a result, the deployment of applications is being slowed down, and in some countries, such as the United Kingdom, stopped and then resumed in other forms. The United States, for its part, has adopted a piecemeal approach insofar as states are allowed to build their own applications. Whatever the strategy followed by individual countries, what is certain is that high levels of adoption of digital contact tracing applications will have to be achieved if the effort is to be worthwhile in terms of effectiveness.

---

[28] The Guardian, "French ministers in spotlight over poor take-up of 'centralized' Covid app", 29 September 2020, https://www.theguardian.com/world/2020/sep/29/france-struggles-to-push-covid-app-as-neighbours-race-ahead

Privacy is a major challenge for the future of digital contact tracking solutions. A system used by tens of millions of individuals handling data as sensitive as contact history or even medical data requires a very high level of security. In Germany, the Chaos Computer Club (CCC), an association of computer experts that has been advising the Federal Government on privacy issues for 30 years, has made a useful contribution to the ethical debate by providing a list of 10 restrictive criteria for such solutions to take advantage of the epidemiological potential of contact tracing without posing a threat to privacy[29].

Incidentally, it's interesting to compare the ethical criteria of the European Commission experts (AI HLEG) and those of the CCC. The former criteria are broader as they apply to Artificial Intelligence, hence notions such as "human factor" or "societal well-being", but they correspond to a large extent, with a slightly different language, to those of the CCC, even if the latter criteria place the cursor on specific points such as "epidemiological purpose", "geo-localization" or "unobservability of communication". This shows that, beyond "values", ethical principles must be modulated according to the requirements of each particular field, depending on its size and specificities.

[29] https://www.ccc.de/en/updates/2020/contact-tracing-requirements

AI HLEG

- Human agency and oversight
- Technical robustness and safety
- Privacy and data governance
- Transparency
- Diversity, non-discrimination and fairness
- Societal and environmental well-being
- Accountability

CCC

- Epidemiological sense and purpose
- Voluntariness and freedom from discrimination
- Fundamental privacy
- Transparency and verifiability
- No central entity to trust
- Data economy
- Anonymity
- No creation of central movement or contact profiles
- Unlinkability
- Unobservability of communication

Digital contact tracing: centralized approach or decentralized approach?

The development of digital contact tracing solutions raises a number of fundamental questions before even addressing the ethical issues:

- Who commissioned the application and who developed it?
- What are its functionalities?
- When was it launched?
- What technologies does it use?
- Where is it available and on which platforms?
- What level of penetration has it achieved after one day/week or one month?

This paper will not elaborate on these different points. However, it is important to stress the importance of the choice of the basic technology used to search and identify contacts:

Basic technology	Comments	Country examples
Location	Some applications identify a person's contacts (a) by tracking their phone's movements (they use GPS or mobile phone networks, i.e. cellular triangulation of relay stations) and (b) by looking at which other phones have spent time in the same place.	Bulgaria, Cyprus, Iceland, Israel, Kuwait
Bluetooth [30]	Other applications use the "proximity tracking" method: phones exchange encrypted tokens with any other nearby phone using Bluetooth. Anonymization of the data is easier to achieve, making this method more advantageous than location tracking from a privacy perspective.	Australia, Austria, Canada, Croatia, Czech Republic, Denmark, Estonia, Finland, France, Germany, Hungary, Italy, Kenya, Northern Macedonia, Malaysia, Malta, Mexico, Netherlands, Norway, Poland, Portugal, Saudi Arabia, Slovakia, Singapore, South Africa, Spain, Switzerland, Tunisia, United Kingdom, Uruguay, Vietnam.

Around the world, and particularly in Europe, most countries have chosen short-range Bluetooth "handshakes" between mobile devices as the best way to record a potential contact, even if it does not provide location data.

Bluetooth technology, which is used in all contact tracking applications, was not designed to measure a distance, but only to transmit data. However, the strength of the signal received from a transmitter depends on the distance. Researchers must take into account the different models of phones, whose Bluetooth capabilities vary, as well as the countless situations in everyday life that induce a cascade of parasitic and a priori unknown factors, such as the transmission power (which the Apple-Google consortium is trying to specify) as well as the attenuation of the signal as it propagates through the environment (for example, depending on whether the

[30] Apple and Google have developed an API that allows iOS and Android phones to communicate with each other via Bluetooth. DP-3T is an open-source protocol for contact tracing, based on Bluetooth; the contact register of a person's phone is stored locally so that no central entity can know who has been exposed.

device is outdoors, in a densely populated environment or not, in a backpack, in a clothing pocket). Therefore, the ability of Bluetooth technology to achieve the necessary level of accuracy remains the big unknown in the equation. It is unclear whether the proximity settings of contact tracing applications that are deployed in many countries still match the contamination conditions as understood today. Indeed, studies have shown that the virus can be transmitted by aerosol effect, i.e. by air[31]. Proximity must certainly play a major role in transmission, but also other parameters, such as the nature of the space in which one is located (inside or outside), the conditions of aeration, the viral load of the aerosols.

While Bluetooth technology is favored by the vast majority of countries, they do not agree on whether contacts should be recorded on individual devices (the so-called "decentralized" approach) or on a central server (the "centralized" approach). The sensitive question is indeed to know where the decision is taken to trigger the sending of notifications to the contacts of a person who has just been diagnosed positive on Covid-19 – is it on a server controlled by a trusted health authority or on the telephone itself?[32]

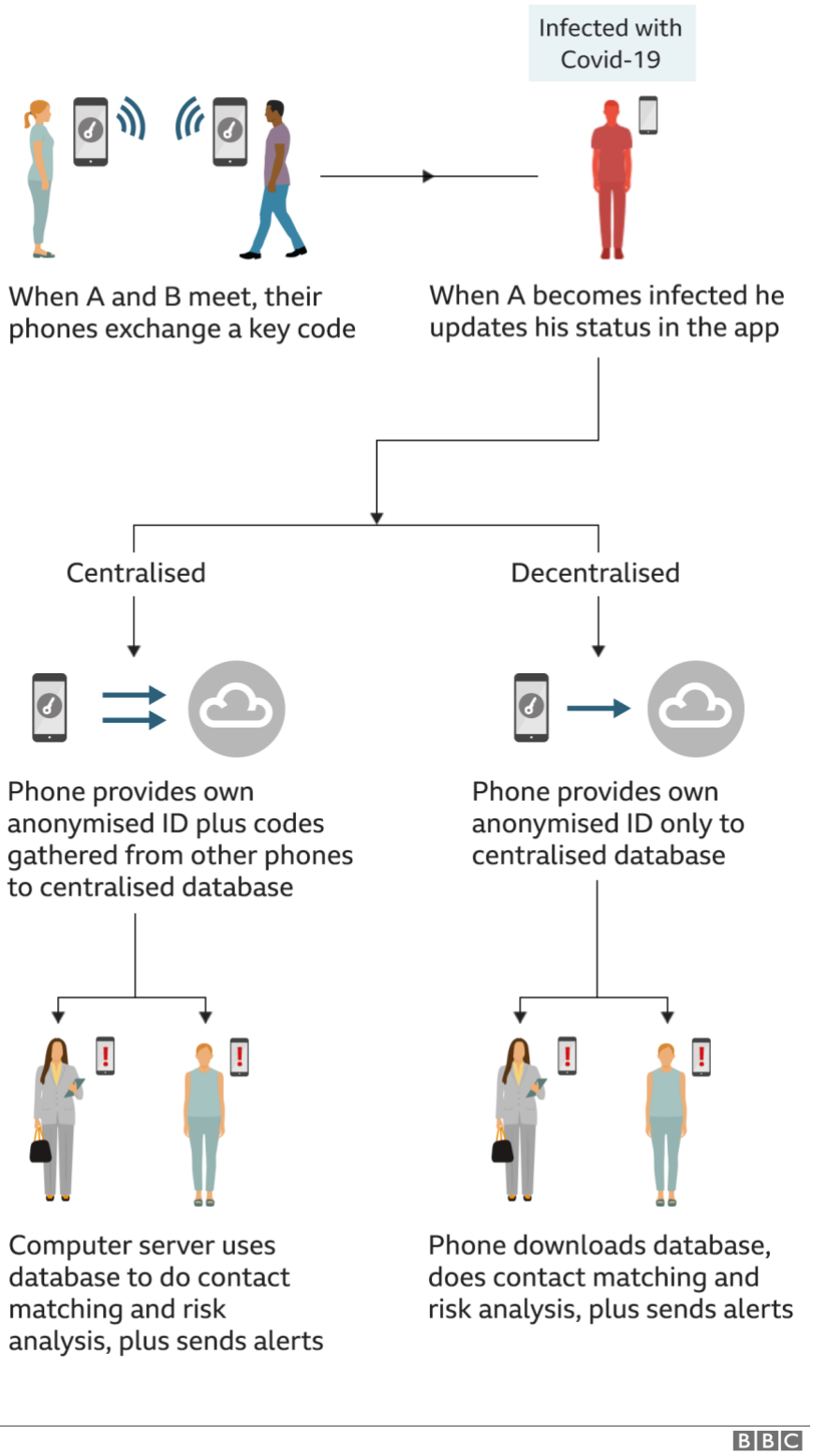
The centralized approach is theoretically more effective than its competitor, as it allows existing contact tracing teams to work directly on the phones and easily locate and warn individuals who may be at risk. In the decentralized approach, users can give their consent to share their telephone number or details of their symptoms, which then allows health authorities to contact them and advise on the best course of action in the event of a proven risk. However, this consent is given in the application and is not part of the central architecture of the system.

---

31 Cf. *Risk of airborne coronavirus spread being underplayed, say researchers*, New Scientist, 7 July 2020.

32 In the centralized approach, which was promoted by the European consortium PEPP-PT (Pan-European Privacy-Preserving Proximity Tracing) launched on 1 April 2020, the central server generates the crypto-identifiers assigned to users and then takes charge of collecting the crypto-identifiers of people who have been in contact with an infected person, calculating the probability of infection and notifying users, if necessary, of a probable infection. For its part, the decentralized approach is organized around a number of protocols, including DP3T, PACT (Private Automated Contact Tracing) and the TCN coalition. During the spring, these different consortia fought a fierce battle punctuated by betrayals and defections! With the decentralized approach, contact tracing operations are carried out on the user's device and the information transmitted to the central server is kept to a minimum. Thus, for example, in the case of a decentralized protocol such as DP3T the users themselves generate the crypto-identifiers on the telephones and exchange them via Bluetooth during prolonged interaction. When a user is infected, he declares to the central server the list of recently encountered identifiers. Other users will periodically download this list of identifiers that have encountered an infected person from the central server and compare it with the list stored on their device to tell the user whether or not they may have been exposed.

Centralized and decentralized models for contact tracing



Source: BBC News, *Coronavirus: The great contact-tracing apps mystery*, 21/07/2020

The European Union has shown that it is at the forefront on the ethical issues of digital technologies, particularly Artificial Intelligence. However, the question of the security of information exchange between national contact tracing applications based on a decentralized architecture has been acutely raised. It should be remembered that the Member States had initially embarked on purely national initiatives, most of which, after a shillyshallying, converged towards the decentralized approach proposed by the Google/Apple alliance. This raised the question of interoperability between the different national applications. As Thierry Breton, Internal Market Commissioner, pointed out, "*Many Member States have implemented national contact tracing and warning applications. It is now time to make them interact with each other. Travel and personal exchange are the core of the European project and the Single Market. The gateway will facilitate this in these times of pandemic and will save lives."* On 14 September 2020, the European Commission was able to announce the establishment of an interoperability gateway service linking national apps across the European Union, thus helping to break the chain of coronavirus infections and saving lives. After a successful pilot phase, the system went live one month later, on 19 October, with the first wave of national apps linked through this service: Germany's Corona-Warn-App, Ireland's COVID tracker, and Italy's immuni. Together, these apps were downloaded by around 30 million people, which corresponds to two-thirds of all app downloads in the EU[33].

Interoperability in Europe: how does it work?

The entry into service of the interoperability gateway highlights a certain isolation of France in the European Union. One country – Sweden – has certainly decided not to develop a contact

[33] https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1904

tracing application, others are considering it but have not yet launched it, but the important fact is that most countries have implemented an application by opting, sometimes after some procrastination, for a decentralized approach supported by Google and Apple.

How can ethical issues be taken into account in contact tracing applications?

From the very beginning of the pandemic, solutions were developed for *tracking* individuals to monitor compliance with the lockdowns and quarantines decided by governments. This was a logical, necessary and fairly simple approach to implement, provided that teams of "trackers" existed to carry out the work. Then quite quickly the idea sprang up among many governments to supplement the *tracking* solutions with solutions for *tracing* individuals, this time to identify and break the chains of transmission of the Covid-19. Thus, mobile solutions and applications were launched worldwide, first in Asia and then after a few weeks in Europe and elsewhere.

We saw that governments could adopt different technical protocols (Google/Apple, DP3T, etc.) as well as different technologies for data collection (Bluetooth, geolocation).

If Bluetooth has emerged as the largely preferred technological option despite uncertainties about the level of accuracy of transmissions, it's because the guarantees in terms of privacy are the best.

We have shown earlier that ethics is about values and that these values can be respected by following a number of principles, among which those advocated by the European Commission's expert group (AI HLEG) are almost unanimous. These principles should then be transformed into simple and clear questions so that they can be applied in specific cases, such as the tracking and tracing of contacts. These questions should at least be as follows:

- Is downloading and using the application voluntary (*opt-in*) or compulsory?
- Are there limits to the use of the data?
- Is the data intended to be destroyed after a certain period of time?
- Is data collection minimized?
- Is the underlying strategy transparent?
- Can children, the elderly and people with disabilities have access to the application? If so, how, and how are their data processed?

The two fundamental issues when considering privacy in the case of mobile contact tracing applications are, on the one hand, the identity of the users (Bluetooth connections allow an anonymous or pseudonymous approach to be implemented, whereas geolocation connections do not respect privacy) and, on the other hand, the structure and storage of data (centralized or decentralized model).

Not surprisingly, the way privacy is treated differs greatly between countries. In Singapore, the "Trace Together" application uses Bluetooth technology to track and identify people who have been in close and prolonged contact with other smartphone users who have tested positive for Covid-19 or are at high risk of carrying the virus, and then alerts them. In case of suspicion of an interaction between a confirmed case and an individual, the downloading of this data to a server becomes mandatory.

In China, where the place given to the individual in society is subject to the interest of the community, the search for contacts is done via the "Close Contact Detector" platform developed by China Electronics Technology Group Corporation (CETC), owned by the Chinese State. This platform, whose purpose is to notify people that they have been in close

contact with infected individuals, has been integrated into pre-existing popular applications such as Alipay, Wechat and QQ. It can be used by authorities, businesses, schools, employees in public spaces or representatives of residential neighborhoods. Users of the platform can access it by scanning a QR code and register with a phone number by providing their name and national identification number. Each account associated with a telephone number can request information on up to three people.

In Germany, the government-commissioned "Corona-Warn-App" application from SAP and T-Systems, developed by Google and Apple and inspired by the work of the European DP3T consortium, analyses Bluetooth signals from mobile phones to detect users who have been in close contact with each other. Individuals who have been in contact with an infected person are then warned. The identities of the users are not disclosed, the data is encrypted and deleted after 14 days.

In the United Kingdom, where as we have seen the implementation of the NHS Covid-19 application has given rise to heated debate, some now claim that the balance between privacy and efficiency excessively favors the former at the expense of the latter: the application provides details on the number of positive tests that have been recorded and the number of alerts that have been sent to users in order to isolate them, but does not reveal the identity of those who have tested positive or those who have been the source of their contamination[34]. In other words, the choices made by the government proved to be more conservative than those concerning the Apple-Google API. For example, users could have been asked when downloading the application whether they would be willing to provide a phone number so that they could be contacted when they were isolated. Instead, they only receive an alert, which they can follow instructions for, or not.

As we can see, the debate is not over, neither in the United Kingdom nor elsewhere in the Western world, where the comparisons that some people try to make sometimes with Asian countries, such as Vietnam or Taiwan, are not necessarily relevant.

The question of "control" is obviously essential. Some governments, such as in France, want to retain control of data and, as a result, have adopted a centralized model. But most governments, like in Germany or the UK, after erratic beginnings, have resigned themselves to relying on Google and Apple. It is rather curious to note that the two American Internet firms are ultimately perceived as offering a more reliable solution and guaranteeing greater security and privacy thanks to anonymization and a decentralized architecture. The interest of Google and Apple is obvious: rather than competing with governments, these companies intelligently prefer to offer each country the possibility of accessing their application programming interfaces (APIs), leaving it up to interested countries to configure these interfaces as they see fit, particularly with regard to privacy issues. Thus, on 10 April 2020, the two American companies announced that they were working together to develop a mobile application using the Bluetooth signals of a smartphone; no GPS location data or personal information would be recorded. "*Privacy, transparency, and consent are of utmost importance in this effort, and we look forward to building this functionality in consultation with interested stakeholders. We will openly publish information about our work for others to analyze*", Google and Apple said in a joint statement[35].

---

[34] Source: *Is the UK's NHS Covid-19 app too private*, BBC News, 30/10/2020.

[35] https://www.apple.com/cz/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/

Mobile contact tracing applications are expected to strike a balance, specific to each country's history, culture and current preferences, between the level of effectiveness that can be expected to control the spread of the epidemic and the potential risk to privacy. Fundamental rights advocates fear that while the tool may initially be used to trace the contacts of newly infected patients, it could later evolve into a "immunity passport" that must be presented systematically in order to use public transport or attend a football match. Especially in France, the debate remains intense between the supporters of a "modern" approach to contain the Covid-19 epidemic and the opponents of such an approach, who refuse to subscribe to a purely "technicist" approach that could call into question the fundamental rights of individuals[36]: "*Although new technologies are now indispensable to any public policy, placing at the centre of a state strategy an application whose effectiveness is more than doubtful, and above all inversely proportional to the ethical, political and health risks it entails, would be catastrophic for the evolution of our society. The exceptional moments we are living through should not lead us to deal with a technical response, as misleading as it is dangerous, nor should it make us deny our democratic requirements. On the contrary, they should encourage us to reaffirm the solidarity and trust that a society needs to continue to invent itself, by stimulating the social imagination that feeds it."*

The French solution: "TousAntiCovid".

France has developed its own application to help in the fight against the Covid-19 virus. This application, which until 22 October 2020 was called *StopCovid France*, is now called *TousAntiCovid*. France has chosen not to use geolocation, i.e. "tracking", which is similar to tracking movements via the GPS of smartphones and relay antennas. *TousAntiCovid* uses "tracing". This involves keeping track of contacts between people via Bluetooth technology. This technology is considered effective and less intrusive than geolocation. It is the position of the European Data Protection Board[37] that "*the use of contact tracing applications should be voluntary and should not rely on tracing individual movements but rather on proximity information regarding users.*"[38]. This is also the position of the European Commission, which favors the least intrusive though effective measures, including the use of proximity data, and avoiding the processing of data on the location or movement of people[39]).

To carry out the ethical analysis of the French application, we will rely on the ethical principles of the European Commission experts (HLEG) [40] mentioned above. These principles are shared by France, which contributed to their elaboration and which seem to us to be the most relevant

---

36 Op-Ed article from a group of academics in Libération, « StopCovid: une application inefficace et menaçante pour la démocratie », 27/04/2020

37 https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/enforcement-and-sanctions/enforcement/what-european-data-protection-board-edpb_en

38 European Data Protection Board: "Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak", 21/04/2020 https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf

39 Commission Recommendation (EU) 2020/518 of 8 April 2020 on a common Union toolbox for the use of technology and data to combat and exit from the COVID crisis, in particular concerning mobile applications and the use of anonymized mobility data https://op.europa.eu/fr/publication-detail/-/publication/1e8b1520-7e0c-11ea-aea8-01aa75ed71a1/language-en

40 Ethics guidelines for Trustworthy AI https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

to date for verifying whether the *TousAntiCovid* application is respectful of the fundamental rights and freedoms.

How does the TousAntiCovid application work?

As with all contact tracking applications, the application allows downloaders to be notified if they have been in the past in close proximity to people who have tested positive for Covid-19 and have the same application, as this proximity carries a risk of transmission of the virus.

In practice, once installed and features enabled, the application sends and receives specific Bluetooth messages from other smartphones where the *TousAntiCovid* application has been installed and enabled.

The device consists of a mobile application made available on mobile equipment (mobile phones and tablets) and a central server that stores and transmits a certain amount of data. If a user has been declared positive to Covid-19, s/he will be able to declare this state directly in the application not with his name but thanks to a code, the QR code provided by the laboratory or doctor. The use of this code by the user allows him/her to send his/her contact history to the central server which then processes each of the contacts in the history, in order to estimate the risk of contamination by the SARS-CoV-2 virus.

The application contacts the server once a day to check the user's exposure status. Users who have been in contact (within 1 meter for at least 15 minutes) with the person diagnosed or tested positive are notified by the server that they have been exposed to a risk of contamination with the SARS-CoV-2 virus within the last 15 days.

Privacy and data governance

What is the purpose of the treatment? Are there any limits to the use of the data?

The aim of the application was initially to facilitate the exit from the lockdown and to slow down the spread of the virus. According to article 1 of the decree, n° 2020-650 of 29 May 2020 relating to the processing of data called *StopCovid France*, newly named *TousAntiCovid*[41], the purpose of the processing is: a) to inform a person using the application of the fact that he or she has been in close contact with a user of the same application subsequently diagnosed positive for Covid-19, so that there is a risk that he or she may be contaminated in turn; b) to raise awareness of the symptoms of the disease, barrier gestures, the referral of contacts at risk to competent health actors, the use of anonymous statistical data at national level. European data protection recommended in its opinion of 25 May that contact between the user and the health professional be recommended but left to the user's discretion[42] to preserve his or her individual freedom, which was followed.

The following operations are expressly excluded from the purposes: the census of infected persons, the identification of the areas to which these persons have moved, the making of contact with the person alerted or the monitoring of compliance with lockdown measures or

---

[41] Decree No. 2020-650 of 29 May 2020 on data processing known as "StopCovid France" https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000041936881/

[42] Deliberation No. 2020-056 from 25 May 2020 delivering an opinion on a draft decree relating to the mobile application known as "StopCovid" (request for opinion No. 20008032) https://www.cnil.fr/sites/default/files/atoms/files/deliberation_ndeg_2020-056_from_25_may_2020_delivering_an_opinion_on_a_draft_decree_relating_to_the_mobile_application_known_as_stopcovid.pdf

any other health recommendations. Nor should the treatment allow monitoring of social interactions between people.

These restrictions on purposes rule out the risk that the *TousAntiCovid* application could be used as a tool for population surveillance or coercion, except in the case of misuse or piracy.

This complies with the applicable regulation recalled in the European Commission recommendation that "*purposes must be sufficiently specific so as to exclude further processing for purposes unrelated to the Covid-19 health crisis (e.g., commercial or law enforcement purposes). Subsequently, adequacy, necessity and proportionality of data must be ensured.*"[43]

Which data is processed and used? Is data collection minimized?

The aforementioned decree lists the categories of data processed: the authentication key shared between the application and the central server; a unique identifier associated with each downloaded application randomly generated by the central server and known only to the server where it is stored; country codes; random and temporary pseudonyms generated by the server; proximity history; periods of exposure of users to diagnosed or tested positive persons stored on the server; proximity history of contacts at risk "contacts at risk of contamination" status; date of last server queries.

There is no collection of names, phone numbers, or email addresses.

The data transmitted is only transmitted if the user of the application so decides, even if s/he is contaminated by the Covid-19 virus. The user is therefore under no obligation to transmit data and this transmission is not automatic.

If s/he decides to do so, the user will be able to transmit the proximity history of contacts at risk of contamination by the Covid-19 virus, the date of the onset of symptoms, and the QR code. Initially, the entire history of the user's contacts was sent to the server, if the user decided to send his contacts at risk. Following a formal notice from CNIL on 20 July 2020[44], the system was modified and now there is a pre-filtering of the user's contact history on the phone. It is therefore impossible for the user's entire contact history to be uploaded to the central server without pre-filtering at the telephone level. Only the contacts that are most likely to have been exposed to the virus are transmitted to the central server. The principle of minimizing data collection is therefore respected.

This minimization of data collection and use is in line with the data minimization principle of the GRDP[45] and recalled in the abovementioned European Data Protection Board guidelines according to which "*in the context of a contact tracing application, careful consideration should be given to the principle of data minimization and data protection by design and by default: (i) contact tracing apps do not require tracking the location of individual users. Instead, proximity data should be used; (ii) as contact tracing applications can function without*

---

[43] EU Commission's Guidance on apps to fight Covid-19: data protection and privacy Q&A, 20/04/2020 https://pierstone.com/eu-commissions-guidance-on-apps-to-fight-covid-19-data-protection-and-privacy-qa/

[44] https://www.cnil.fr/fr/application-stopcovid-cloture-de-la-mise-en-demeure-lencontre-du-ministere-solidarites-sante

[45] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=FR

direct identification of individuals, appropriate measures should be put in place to prevent re-identification; (iii) the collected information should reside on the terminal equipment of the user and only the relevant information should be collected when absolutely necessary."[46]

Is the data anonymized?

The data transmitted via *TousAntiCovid* is very sensitive since it is health data and allows contact histories to be created within one meter of people "crossed" for more than 15 minutes. In the absence of robust measures making it very difficult to re-identify users, the application would make it possible to know whether a particular individual has had the virus, particularly to the people with whom s/he has been in contact and who have downloaded the application, and to know the identity of these people, which would be a strong obstacle to privacy and individual freedoms.

This is why the European Commission, in its above-mentioned recommendation, states that the use of anonymized data should be respected, that safeguards should be put in place to prevent de-anonymization and to avoid re-identification of individuals, in particular through encryption. It refers to "*safeguards to be put in place to prevent de-anonymization and avoid re-identifications of individuals, including guarantees of adequate levels of data and IT security, and assessment of re-identification risks when correlating the anonymized data with other data*".[47]

The European Data Protection Board provides useful clarifications on the distinction between anonymization and pseudonymisation. For total anonymization to be real, it must meet three criteria: it must not be possible to identify an individual from a group; it must not be possible to link two files concerning the same individual; it must not be possible to deduce with significant probability information unknown to an individual. The Board adds that only groups of data (data sets) can be anonymized, and not individual data, and therefore encrypting data alone does not make it possible to anonymize it but only to pseudonymize it.

This distinction between anonymization and pseudonymization was recalled by CNIL in a summary article published on its website on 19 May 2020[48], according to which "anonymization is a processing that consists of using a set of techniques in such a way as to make it impossible, in practice, to identify the person by any means whatsoever and irreversibly" whereas "pseudonymization consists of replacing the directly identifying data in a data set (surname, first name, etc.) with indirectly identifying data (alias, sequential number, etc.)" Pseudonymization therefore makes it possible to trace the identity of the person concerned, which is why the use of pseudonymized data must comply with regulation on personal data, whereas the use of anonymized data is completely free.

The *TousAntiCovid* app does not guarantee the anonymization of data but only their pseudonymization. For this reason, *TousAntiCovid* must comply with the GRDP and the amended Loi Informatique et Libertés[49]. This was recalled by CNIL in its opinion of 24 April

---

[46] Guidelines 4/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, adopted on 21 April 2020, point 3.1.27 https://edpb.europa.eu/our-work-tools/our-documents/ohjeet/guidelines-042020-use-location-data-and-contact-tracing-tools_en

[47] Commission Recommendation (EU) 2020/518 of 08/04/2020, Use of mobility data to inform measures and exit strategy, (20) (3) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32020H0518&from=FR

[48] https://www.cnil.fr/fr/lanonymisation-de-donnees-personnelles

[49] https://www.cnil.fr/fr/la-loi-informatique-et-libertes

2020[50] according to which "there remains a link between pseudonyms and downloaded applications, each application being itself installed on a terminal, which generally corresponds to a specific individual". The fact that the application is downloaded onto a mobile phone with an IMEI (International Mobile Equipment Identity)[51] gives the possibility of tracing the user's identity.

In its guidelines, the European Data Protection Board recommends certain measures for contact tracing applications: pseudonymous identifiers should be exchanged between the mobile phones of users of equipment (computers, tablets, connected watches, etc.) and the mobile phone of the user.); identifiers should be generated using state-of-the-art cryptographic processes; identifiers should be renewed regularly to reduce the risk of physical tracking and link attacks; the application should not transmit information to users that would allow them to deduce the identity or diagnosis of others; and the central server should neither identify users nor deduce information about them.

What about the pseudonymization of personal data in *TousAntiCovid*? Are these measures respected?

As already mentioned, downloading the application does not require the provision of directly identifying data such as name, telephone number, e-mail address. The aforementioned decree states that "data allowing the identification of the mobile phone, its holder or user cannot be collected or recorded for processing purposes". Downloading to the mobile phone does not save the name but a permanent pseudonym. The decree does indeed mention that a unique identifier associated with each application downloaded by a user is randomly generated by the central server and is only known by the server where it is stored.

The decree indicates that there is an authentication key shared between the application and the central server, generated by the central server when the application is downloaded, which is used to authenticate messages from the application.

The application states that the data exchanged between two phones via Bluetooth are pseudo-identifiers that are automatically renewed every 15 minutes. They are therefore temporary. It is for example a sequence of numbers, letters or signs, which does not by itself identify a person. If you come across a person who has *TousAntiCovid*, the phones exchange the two pseudonyms with each other. Each records the other in its history of crossed people in an encrypted way. In principle, the crossed persons do not know the identity of the infected person who made the alert.

However, we can point out the caution of the drafting in the application. The "by itself" which indicates in hollow that there is indeed a possibility to identify the person with a cross-reference of other data.

---

[50] Deliberation No. 2020-046 of 24 April 2020 giving its opinion on a project for a mobile application called "StopCovid" (request for opinion No. 20006919) https://www.cnil.fr/sites/default/files/atoms/files/deliberation_du_24_avril_2020_portant_avis_sur_un_projet_dapplication_mobile_stopcovid.pdf

[51] The IMEI code uniquely identifies each mobile phone terminal.

If the user of the application has been diagnosed positive for the virus, s/he will not send his/her name to the server but the QR code which is random and therefore does not identify the person concerned[52].

In conclusion, it seems that many precautions have been taken to avoid the re-identification of individuals and that the recommendations of the European Data Protection Board have been heard on this point. Regular checks should be carried out to ensure that this is indeed the case.

To whom is this data transmitted?

The data stored on the mobile phone is only shared by the application with the server managed by the Ministry of Solidarity and Health and its subcontractor INRIA if the user has been diagnosed as a Covid-19 case and with his/her consent. The transmission is therefore not automatic: the user is not obliged to declare that he or she is positive for the new coronavirus and he or she will only transmit the limited history of his or her contacts to the server if he or she so wishes.

When data is shared with the server, the application specifies that this allows other users' applications to query the server to find out if they have been in close proximity to the relevant application. If this is the case, users will be alerted that they have been exposed to a risk of contamination.

The fact that such sensitive data is centralized on a state server has been the subject of many comments, with some fearing misuse, such as the introduction of population surveillance or hacking.

Is the data intended to be destroyed after a certain period of time?

The application mentions that the data, i.e. in particular all pseudonyms and exchanges of pseudonyms, are kept for fourteen days and automatically deleted on the telephone and server. This data retention period corresponds to health recommendations and makes it possible to keep the data only for a limited period of time.

In addition, the user can at any time request the deletion of his data from his smartphone and the central server database before uninstalling the application.

Robustness and safety

According to the AI HLEG's work mentioned above, the robustness of a system is assessed on the basis of several criteria including resilience to attack and security, fallback plan and general safety, accuracy, reliability and reproducibility.

What is the technology used? Is it accurate and reliable?

The technology used is Bluetooth and not geolocation. As Bluetooth is only effective over very short distances, only very close contacts (one meter) are recorded. In the FAQ on the application site, it is stated that "the development of such an application is technically complicated" and that "*the work of the teams led by INRIA has removed most of the technological barriers. In particular, the issue of calibrating Bluetooth and its ability to estimate distances between two phones has been largely resolved, in cooperation with Germany, which has carried out tests on the subject.*" This question of the reliability and accuracy of the system is essential to ensure

[52] A QR code does not contain any information identifying the person concerned; it is randomly generated, affixed to the result of a test for the Covi-19 virus, and then sent to the person who carried out the test, in the event of a positive result.

that there will be no errors in the alerts made, at the risk of seeing erroneous alerts result in physical harm (no alert from contact with a person declared positive for the virus) or psychological harm (alert made when no person crossed is contaminated by the virus). Checks on these points must be carried out regularly.

Following the opinion of CNIL, it is no longer envisaged to intentionally introduce false positives in notifications sent to individuals, in order to limit the risks of re-identification in certain types of attacks.

CNIL had raised in its aforementioned opinion of 25 May that the failure to take into account the context of the contacts (doctors, persons protected by separating walls, etc.) was likely to generate false positives and that a button should be provided in the future to temporarily deactivate the application; this has been done. In addition, the second version of the application provides that it is no longer activated once and for all; the user must activate it when he is in a busy place, in a shopping centre, in his company, in a restaurant, etc.

Is the system safe? Have effective measures been taken to prevent and combat cyber-attacks (security) and accidents or incidents (safety)?

The French government has chosen to use the centralized architecture, i.e. only proximity histories are exchanged between the user and the server on the grounds that "the centralized architecture offers more guarantees and security. It prevents a server from collecting the list of people who have tested positive for coronavirus (even anonymously) and prevents this list from circulating or being stored on a server or on telephones". There is therefore no creation of a file of contaminated persons but simply a list of contacts, for whom all data is pseudonymized.

CNIL insisted in its opinion of 24 April on the need to take very high-level security measures to offset the risk of misappropriation of the data on the central server. It indicated that the 3DES encryption algorithm should no longer be used, which was followed.

Here again, it is in line with the European Commission's recommendations mentioned above, according to which "advanced cryptographic techniques must be implemented to secure data stored in servers and applications, and exchanges between applications and the remote server".

Concerning the reliability and security of the application's computer system, the content of the *TousAntiCovid* application indicates that the publication of the source code allows the application to be compared with the scientific community to identify possible flaws.

The fact that the National Agency for the Security of Information Systems (ANSSI) is a member of the *TousAntiCovid* team is a guarantee that these issues are taken up seriously.

The application states that "geolocation data is neither recorded nor exchanged". The wording here again seems cautious. Does this mean that it would finally be possible to reconstruct movements?

The captcha authentication method (which makes it possible to check during the initial activation of the application that it is used by a human being), which was based on Google's reCaptcha technology, used at the beginning, has now been replaced by the captcha technology developed by Orange. Google's reCaptcha web service is no longer used in the *TousAntiCovid* application.

This is a breakthrough as Orange's technology is limited to security purposes, unlike reCaptcha technology which was 'based on the collection of hardware and software information (such as device and application data), which is sent to Google for analysis'[53]. As a result, the information provided by Google to the developers was not only used to secure the application, but also to enable Google to carry out analysis. CNIL had indicated that the use of this Google service was likely to result in the collection of personal data not provided for in the decree, and also in data transfers outside the European Union. These two risks are now in principle ruled out.

How will the algorithms, data and the application in general be controlled, especially in terms of reliability, security and safety?

In the above-mentioned guidelines the European Data Protection Board states that "in order to ensure their fairness, accountability and, more broadly, compliance with the law, algorithms must be verifiable and must be regularly reviewed by independent experts". Regular monitoring of algorithms and application security systems is a key point to check that they are working properly for the desired purposes and that the system is not being biased or hacked. This must be done by independent experts.

It will also be necessary to check that the data has not been altered or hacked.

Security audits are planned by ANSSI throughout the development of the application and carried out by third parties. These audits should then continue throughout the use of the application.

CNIL is in favor of an evaluation of the application after experimentation. A specialized liaison and monitoring committee will therefore assess the application to check whether the state is doing what it says it is doing.

The aforementioned decree provides that the data controller shall make a public report on the operation of *TousAntiCovid* within thirty days of the end of the implementation of the application, and no later than 30 January 2021.

Human factor and human control

Is downloading and using the application voluntary (opt-in) or compulsory?

The European Data Protection Board has already taken a position that the use of contact tracing requests should be voluntary (guidelines mentioned above).

The *TousAntiCovid* system is based on the voluntary participation of users. The application is installed freely and free of charge by the users, who also have the option of activating or not activating the application's functionality to build up the proximity history. It is also possible not to communicate about the fact that one has had the virus and not to transmit the proximity history to the server. The application can be uninstalled at any time. Individual freedom is respected at every step of the process. The user who downloads the application is not engaged in an obligatory process of which he would lose control. He or she remains in total control of whether or not to declare his or her illness.

Moreover, in its opinion of 24 April 2020, CNIL stressed that volunteering should not only mean that the user chooses to download and then implement the application, but also that access to tests, treatments, release from confinement, use of transport, return to work should not be

[53] https://www.google.com/recaptcha/admin/create?pli=1

conditioned by the downloading and use of the application. No access to any place or service should be conditioned on it. This would constitute discrimination for CNIL. Thus, the installation of the application does not give access to any specific right or benefit. This information is provided in the content of the application.

CNIL complies in this respect with the position of the European Data Protection Board, according to which "persons who decide not to be able to use these applications should not suffer any disadvantage." (guidelines cited above). To date, there is no reason to believe that the application should become mandatory directly or indirectly through a restriction on services that would result from the absence of downloading. To date, CNIL's opinions regarding *TousAntiCovid* have always been followed (which moreover allowed CNIL to lift its formal notice on 3 September 2020) and it is certain that it will ensure that this point is respected. The *TousAntiCovid* website indicates that this is a "public freedom issue".

Transparency

According to the above-mentioned HLEG guidelines, transparency consists of three elements: traceability[54], explainability[55] and communication about the limits of the system.

What is the transparency attached to TousAntiCovid?

The source code implemented as part of *TousAntiCovid* is made public and is accessible from the websites of the Government (https://www.gouvernement.fr/info-coronavirus/tousanticovid), the Ministry of Solidarity and Health (https://solidarites-sante.gouv.fr/soins-et-maladies/maladies/maladies-infectieuses/coronavirus/tousanticovid), the Ministry of Economy, Finance and Recovery (https://www.economie.gouv.fr/tousanticovid), and the application itself. CNIL welcomed the free access to the protocols used and the source code. We did not find on the application's web site any information for those who were not aware whether the algorithms used were supervised or unsupervised. It would be useful to know who is the human at the joysticks and when there is human intervention or with which tools[56] . It would also be interesting for users to understand, through simple explanations, how the algorithms of the application work.

Another area for improvement would be to clearly explain to the uninformed user that the application does not allow anonymization of data but only pseudonymization, and that it is therefore possible to trace the user's identity, even if many precautions are taken to minimize the risk of re-identification.

Following the recommendations of CNIL on 25 May, the users' rights to erasure and opposition provided for in the GRDP were introduced to comply with the legal obligation.

Data subjects are informed of the main features of the processing and their rights, in accordance with the provisions of Articles 13 and 14 of the aforementioned Regulation (EU) of 27 April 2016, when the *TousAntiCovid* application is installed. They are further warned that in the event of sharing their proximity history on the central server, persons identified as their contacts at

---

[54] Ability to follow the path of a captured data through all stages of sampling, labelling, processing and decision making.

[55] Characteristic of an AI system that is intelligible to non-experts. An AI system is intelligible if its functionality and operation can be explained in a non-technical manner to a person who is not a specialist in the field.

[56] The human is in the loop: the system can perform a task and then stop to wait for human commands before continuing; the human is on the loop: the system operates completely autonomously, but a human can have a supervisory role if the system breaks down; the human is in control: it supervises the overall activity of the system and can decide not to use it.

risk of contamination will be informed that they have been in the vicinity of at least one other user diagnosed or tested positive for the Covid-19 virus during the last fifteen days and of the limited possibility of indirect identification that may result when these persons have had a very small number of contacts during this period.

The application provides a link to the site of the Ministry of the Economy, Finance and Recovery where there is a *TousAntiCovid* portal on which it is possible to find a wealth of documentation, including a practical guide, very simple and educational, on the application, detailed instructions for use, a guide to support carers, parliamentary debates and the various opinions of the expert committees. It is possible to ask questions about the application directly and a list of answers is then sent via an FAQ before any personalized response. A link is created to a free online test to find out whether you are likely to be infected with the virus or not and whether you should be tested, with of course the usual reservations about the reliability of the test. Since the new version of the application was released on 22 October, it is also possible to obtain data on the epidemiological situation, to have access to a map of testing centres, advice on Covid-19, and easier access to the dispensation certificate for areas affected by the curfew. This very substantial transparency and information effort is to be welcomed.

Many measures have been adopted to ensure data traceability and make the application intelligible, but there is little communication about the limits of the application and its risks of error. Educational efforts could be made on the latter point.

Societal and environmental well-being

Protection of public health and general interest

The application contributes to the fight against the Covid-19 pandemic and thus serves the general public health interest.

In accordance with the opinion of CNIL, the French government has decided to base the *TousAntiCovid* treatment on the legal basis of the public interest mission to combat the Covid-19 epidemic, and not on the legal basis of consent. For this reason, the government issued Decree No. 2020-650 of 29 May 2020 on data processing known as "StopCovid"[57] in accordance with Article 9-2-1 of the General Regulation on Data Protection (GRDP).

National sovereignty

As indicated on the application, *TousAntiCovid* was created under the supervision of the Ministry of Solidarity and Health and the Secretary of State for Digital Affairs. The team that developed *TousAntiCovid* is composed of INRIA, ANSSI, Capgemini, Dassault Systèmes, Inserm, Lunabee Studio, Ministry of Solidarity and Health, Orange, Santé Publique France (i.e. the national public health agency), and Withings.

The French system deliberately aims to be independent of the most powerful companies on the Internet (the so-called GAFA). This makes it possible to greatly limit the risks of data transfer and cross-referencing which, as explained above, allow the re-identification of individuals. It is therefore a choice for enhanced protection of personal data. The content of the TousAntiCovid application states that "the solutions proposed by Apple and Google are based on the transmission in all smartphones of pseudonyms for people who have been diagnosed positive. This means that a medical diagnosis, even in encrypted form, circulates in all

[57] https://www.legifrance.gouv.fr/download/file/XflPtkDVNIUQvmjG_P47zuwD-lQnj8EG78BD08U7ANE=/JOE_TEXTE

applications. The risks of vulnerabilities are high and models of computer attacks are already available on the web."

It is also a means of asserting national sovereignty and developing national excellence. This is how the government presents it on its website: "protecting the health of French citizens is a mission that is the exclusive responsibility of the State and not of private international players... It is a question of health and technological sovereignty".

However, this national sovereignty must not be an obstacle to the interoperability of the solutions adopted within the European Union. It is essential and required by the above-mentioned European Commission Recommendation 2020/518 that this application is part of a European approach and that it is coordinated at EU level. In its opinion of 25 May 2020, CNIL noted that "changes to the application and the protocol for monitoring contacts, particularly in order to enable interoperability on the scale of the European Union, are likely to be developed in the medium term". Unfortunately, being based on the same infrastructure as *StopCovid*, the *TousAntiCovid* application still has the disadvantage of not being interoperable with other applications available in neighboring countries.

Democratic process

Many organizations were consulted for the implementation of the *TousAntiCovid* app:

- CNIL issued two opinions, a formal notice and a decision;
- the National Digital Council (CNNum), the Scientific Council, the National Academy of Medicine, the European Centre for Disease Prevention and Control, the National Digital Ethics Steering Committee, the French Medical Association, the National Consultative Commission for Human Rights, the Higher Commission for Digital and Postal Services have issued opinions and recommendations.

Democratic debates were held in the National Assembly on 28 May 2020 and in the Senate on 27 May, which voted in favor of implementation. A decree was then issued to authorize the creation of the application.

Diversity, non-discrimination and equity

Downloading the application is free of charge.

The free application and its ease of use make it accessible to anyone with a mobile phone or tablet.

Can children, the elderly and people with disabilities have access to the application?

The application is accessible to minors. In its opinion of 25 May 2020, CNIL invited the Ministry to incorporate specific developments both for the minors themselves and for their parents. The application invites minors under the age of 15 to discuss with their parents or legal guardians the opportunity to install the application.

Since elderly people are generally distant from the digital world, it has been imperative to establish parallel and effective systems enabling them to be effectively alerted to the fact that they have been in contact with an infected person, so that the very existence of the application does not discriminate against them in terms of care and support. We have already pointed out that it is possible to download from the application a complete, educational and simple guide to help carers get to grips with the application.

Moreover, the application is very simple to use and in principle accessible to people with disabilities.

Accountability

Who is the controller?

The controller is the Ministry in charge of health policy, which subcontracts the processing to INRIA.

CNIL welcomed the fact that the cloud computing service provider hosting the application infrastructure as a subcontractor has data centres in France and that personal data is not transferred outside the European Union.

What are the recourses?

The application provides for the possibility of referring the matter to CNIL if it is deemed that the processing of its data does not comply with the regulations in force on personal data.

It also provides for the possibility of asking questions.

However, we have not identified a mechanism for users to report problems related to bias, discrimination or poor performance of the application.

CNIL is the guardian of compliance with the regulations on personal data.

The scheme must therefore meet the conditions laid down in the European Convention for the Protection of Human Rights and Fundamental Freedoms, the Charter of Fundamental Rights of the European Union and the specific guarantees of the GRDP. It must therefore be necessary, proportionate to the objective pursued and must not lead to the disappearance of privacy and protection of personal data.

This explains why CNIL reserves the right to regularly assess the effectiveness of the system, which will make it possible to say whether it is still necessary over time. Doubts about this effectiveness have been widely expressed in the press due to its low download rate in relation to the overall population. What the *TousAntiCovid* website says on this point is that the application is useful from the very first downloads because it saves time and precious hours by alerting people who have been in contact with a sick person, thus speeding up the taking of health measures. Another limitation raised is that elderly people, who are at high risk, probably have little reflex to download the application. CNIL's effectiveness monitoring will therefore be valuable to see whether it is useful to maintain the application over time.

At the end of November, the *TousAntiCovid* app had more than 10 million downloads, which is by all standards a success.

CNIL insists that in order to be useful and necessary, the application must be part of an overall plan to combat the epidemic, which includes "the mobilization of health professionals and health investigators, the availability of tests and masks, the management of screening, support measures, information and service provided to people who have received the alert, the ability to isolate them in suitable places, etc.". (Opinion of 24 April mentioned above). In other words, the application should be presented as an additional tool for dealing with the Covid-19 pandemic, in no way as a device that would replace the mask, barrier gestures and social distancing which are means within everyone's reach, low tech and very effective in limiting contamination.

In order to respect the principle of proportionality, it is foreseen that the *TousAntiCovid* app will disappear six months after the end of the state of health emergency.

CNIL validated in its opinion of 25 May 2020 that the app provides neither a right of access to data, nor a right of rectification and limitation, as the data is pseudonymized and the exercise of these rights would require identification of the person concerned, which would weaken the security of the entire app. On the other hand, it considered that the right of objection materialized by the possibility for the user to stop using the app at any time and the right of deletion were applicable to the device.

CNIL has, of course, reiterated the need to carry out an impact analysis, which has been done.

To conclude on the French application, its ethical assessment appears positive because most of the criteria set by the experts of the European Commission (HLEG) or the Chaos Computer Club mentioned above are well met. This app represents a truly ethical alternative to the use of much more intrusive technologies such as facial recognition or geolocation, which infringe on individual freedoms and privacy.

The most difficult criteria for ethicists to evaluate, yet decisive, are the robustness of the application and its safety and effectiveness. We will still have to wait for the opinion of CNIL and the evaluation of technical experts in IT and public health to find out what it really is.

One identifiable area for improvement today is, as we have already had occasion to mention, the interoperability of the *TousAntiCovid* application with other European applications to facilitate intra-European trade and the free movement of people and services, the pillars of the European Union.

Conclusion

We have outlined the differences and interrelationships between the concepts of “privacy”, “personal data protection” and “ethics”, showing that in the literature these concepts are often mixed up with the result that there is some confusion. It is important to re-establish the respective nature, scope and challenges of these three concepts which, although complementary, refer to different histories and public policy objectives.

We then chose to apply these concepts, and in particular that of ethics which has recently positioned itself at the heart of Artificial Intelligence and Internet of Things human challenges, to the particular, but very important, case of contact tracing in the context of the Covid-19 outbreak. We have stressed that digital technologies play an essential role today in the capacity that nations may have to limit the risks of transmission of Covid-19 and therefore of contamination. If the Asian countries have been undeniable leaders in the design and implementation of contact tracing applications, with successes that should be recognized, linked in particular to the greater discipline of the populations compared to those of the Western world, but also and above all to the good integration of these applications into the general arsenal of public strategies for responding to the pandemic (testing, tracing, isolation), it must be agreed that the European countries, more than the United States, were able to find relevant responses without delay despite, here and there, hesitations and changes in strategy. We have shown that the main difficulties consisted, on the one hand, in positioning the cursor between “effectiveness” and “privacy” (a choice that was above all political) and, on the other hand, in choosing between a centralized approach and a decentralized approach (a choice that was above all technical).

Although the European Union seemed slow to fully appreciate the seriousness of the outbreak at the outset, it did, however, prove effective in designing and deploying a so-called “interoperability gateway”, i.e. an infrastructure enabling several European tracing apps to be connected to each other to prevent the spread of Covid-19.

France, for its part, has shown stability in its approach, maintaining over the period its initial choice of a centralized approach based on Bluetooth technology. However, this choice did not enable it to join the group of European countries capable of making their systems interoperable.

The ethical assessment of the French app appears positive. This app represents an ethical alternative to the use of much more intrusive technologies such as facial recognition or geolocalization, which infringe on individual freedoms and privacy.

Appendix: some examples of mobile applications

Country	Name of the application (Developer)	Start date	Protocol / Mode of data collection	Website
Australia	COVIDSafe App	13/05/2020	Bluetooth	https://www.health.gov.au/resources/apps-and-tools/covidsafe-app
Austria	Stopp Corona (Red Cross, Accenture)	25/03/2020	Google / Apple Bluetooth	https://www.stopp-corona.at
Belgium	Coronalert (Belgian authorities)	30/09/2020	Bluetooth	https://coronalert.be/fr/
Canada	COVID Alert	31/07/2020	Google / Apple Bluetooth	https://www.canada.ca/en/public-health/services/diseases/coronavirus-disease-covid-19/covid-alert.html
China	Close Contact Detector (National Health Commission, CETC)	10/02/2020	QR code, mobile apps (Alipay, WeChat)	http://en.nhc.gov.cn/2020-02/10/c_76416.htm
Denmark	smittestop	18/06/2020	Google / Apple Bluetooth	https://smittestop.dk
France	StopCovid (Inria)	02/06/2020	RoBERT Bluetooth	https://www.economie.gouv.fr/stopcovid
Germany	Corona-Warn-App (SAP, Deutsche Telekom)	16/06/2020	Google / Apple Bluetooth	https://www.coronawarn.app/en/
Hungary	VirusRadar (Nextsense)	13/05/2020	Google / Apple Bluetooth	https://virusradar.hu
Israel	HaMagen Hamagen 2.0	29/03/2020 27/07/2020	GPS GPS, Bluetooth	https://govextra.gov.il/ministry-of-health/hamagen-app/download-en/
Italy	Immuni	01/06/2020	Google / Apple	https://www.immuni.italia.it/faq.html

			Bluetooth	
Japan	COCOA (Microsoft Corp.)	19/06/2020	Google / Apple Bluetooth	https://play.google.com/store/apps/details?id=jp.go.mhlw.covid19radar
Malaysia	MyTrace	03/07/2020	Google / Apple Bluetooth	https://www.mosti.gov.my/web/en/mytrace/
New Zealand	NZ COVID Tracer App (Rush Digital)	20/05/2020	Bluetooth	https://www.health.govt.nz/our-work/diseases-and-conditions/covid-19-novel-coronavirus/covid-19-resources-and-tools/nz-covid-tracer-app
Norway	Smittestopp (Local design)	16/04/2020 (application suspended on 15/06)	GPS, Bluetooth	https://www.helsenorge.no/coronavirus/smittestopp
Poland	ProteGO Safe	20/04/2020, revised 09/06/2020	Google / Apple Bluetooth	https://www.gov.pl/web/protegosafe
Portugal	STAYAWAY COVID	01/09/2020	Google / Apple Bluetooth	https://stayawaycovid.pt/landing-page/
Saudi Arabia	Tabaud (Saudi Data and Artificial Intelligence Authority (SDAIA))	14/06/2020	Google / Apple Bluetooth	https://tabaud.sdaia.gov.sa/IndexEn
Singapore	TraceTogether Ministry of Health (MOH), GovTech	20/03/2020	BlueTrace Bluetooth	https://www.tracetogether.gov.sg
South Africa	Covid Alert SA App	01/09/2020	Google / Apple Bluetooth	https://sacoronavirus.co.za/covidalert/
Spain	Covid Radar (Secretary of State for Digitisation and Artificial Intelligence)	15/09/2020	Google / Apple Bluetooth	https://www.abc.es/tecnologia/moviles/aplicaciones/abci-radar-covid-todo-tienes-saber-sobre-aplicacion-rastreo-coronavirus-gomera-202006301129_noticia.html
Sweden	Sweden has no plans to introduce an application at the moment.			

Switzerland	Swiss Covid (Swiss Federal Institutes of Technology in Lausanne and Zurich)	25/06/2020	Google / Apple Bluetooth	https://www.bag.admin.ch/bag/en/home/krankheiten/ausbrueche-epidemien-pandemien/aktuelle-ausbrueche-epidemien/novel-cov/swisscovid-app-und-contact-tracing.html
The Netherlands	CoronaMelder Application	18/08/2020	Google / Apple Bluetooth	https://github.com/minvws/nl-covid19-notification-app-android
United Kingdom	NHS Covid-19 App	24/09/2020	Google / Apple Bluetooth, QR code	https://www.covid19.nhs.uk
United States	Many, but not all, states have launched or are currently developing an application using the Google/Apple protocol and collecting data via Bluetooth.			