

Development and governance of technology-based solutions for a health crisis exit strategy

Decision support for COVID-19 initiatives

INTRODUCTION

In a pandemic, a world of technology-based tools carries as much hope as risk

A host of digital projects is now underway across the world in an attempt to find an urgent solution to the dilemmas around SARS-COV-2 (COVID-19), involving tracking in order to contain infections, finding a way to get back to normal and avoiding an epidemic resurgence. The common challenge for these technology-based approaches is to provide “continuous control” of the global spread of the virus by leveraging the almost universal use of connected devices (smartphones, as well as the different prostheses and intelligent clothing) that have become extensions of the physical person.

A variety of sources have recently reported that over forty tracking applications for tracing contacts and monitoring people’s movement are being developed or deployed in more than twenty countries. Alternative measures for digitally tracking individuals (bracelets, cameras) and technologies for monitoring people’s movements were in use in some 30 countries. 28% of applications available to date were not subject to a stated privacy policy. About two-thirds use GPS technology to track people’s movements, while one-third uses Bluetooth technology. These developments are either the result of private initiatives, independent non-profit organizations, or initiatives actively supported by public authorities. All in all, techniques for managing and controlling the health crisis using digital tools are currently being developed in very different ways in well over fifty countries.

These developments are a source of hope, as no victory against disease in the history of mankind has ever been achieved without social and political action as well as innovative medical and public health tools and technologies to fight against germs (viruses, bacteria, etc.). But using today’s digital innovations is not without risks either. As the ancients have written, any tool is a pharmakon: it can kill or cure. The misuse of technology, the fascination it can hold or the ease with which it can be turned to covert purposes (economic, social or political) to control or manipulate individuals or populations, can profoundly affect the trust and social cooperation needed to fight a pandemic. The ambivalence of mankind’s relationship with technology raises practical questions that are by nature philosophical (what can we learn through technology?), ethics-related (what are the conditions for claiming certain property through the use of technology?) and political (how do we govern the deployment and use of technology in society?).

Decision-making, with ethics at the core

In a context of fear, uncertainty and sometimes even suspicion, all decision-makers now find themselves facing a flood of opinions that raise issues of ethics around the solutions they are weighing: governments over national measures, employers concerning solutions they could implement to protect employees, retailers and public transit for their customers, building owners for their tenants, etc.

Out this context emerge issues that could lead to the rejection of every solution put forward and thereby to paralysis: first of all, the ethical considerations and red lines in the sand imposed by those involved in the debate, and then moving on to technical and financial constraints.

And the polarizing debate around some of the most highly publicized aspects makes gaining a bird's eye view of the bigger picture difficult to say the least. For example, while the arguments put forward by defenders of individual freedoms and privacy are undeniably relevant and fundamental, the concept of "privacy by design" does not, on its own, fully address the ethical issues raised by the implementation of technology-based solutions. In a situation where preserving life and public health are the primary objective and are in themselves a human right, the issue is to find the right balance, among others, between freedom of movement — guaranteed by law but restricted by confinement — and digital freedom — also guaranteed to citizens but which could be compromised by certain uses that data might be put to.

Clearly, a broader view of ethics must be taken to benchmark the different measures being studied and explain them to the public — who must not be seen as mere users of digital tools. Ethics must not advocate any particular moral code, but be understood as a thoughtful and inclusive process based on a genuine discussion of the values we wish for our society.

Transitioning from disaster management to long-term risk management

The fierce debates around technology-based solutions developed in the heat of the health crisis highlight the real challenge for governance facing us over the long term.

On one hand, uncertainty remains high today for many reasons — will the virus mutate?, can actual immunity be acquired and for how long?, will seasonality affect the virus?, what is the potential for epidemic resurgence?, etc. And even once a vaccine does become available, we will inevitably face new pandemics that may take us just as much by surprise.

On the other hand, our ability to mobilize the power of technology and harness digital expertise to prevent epidemics or protect our populations is a new and major asset for our societies in facing health disasters. But the methods for deploying these solutions will also

come with their fair share of risk, particularly for geostrategic sovereignty and the protection of user interests and freedoms over the long term.

Through constant exposure to these types of risks, we must learn to govern how we develop and implement solutions.

That being said, the processes of engaging stakeholders, analyzing and deciding on the best solutions, and facilitating social acceptance that we develop to curb COVID-19 may offer the first outline of a governance model for a future in which technologies and algorithms along with extreme risks — health-related or not — will be determining factors and enable us to weigh our decisions against global ethics considerations.

AVOID PITFALLS

Two traps to avoid: reductionism and solutionism

Two common and opposing stumbling blocks around digital technology must be raised up front — reductionism and its corollary, solutionism. Reductionism is the reduction of phenomena and policy decisions to a base set of social factors. This very broad trend, considerably reinforced by big data and algorithmic processing, has advantages, but also carries significant risk: the familiar “can’t see the forest for the trees” syndrome, taking statistical correlations as proof and, as a result, confirming bias or painting a “virtual reality” disconnected from the truth. Without being overly simplistic in criticizing technology, we must also guard against a tendency towards techno-solutionism, which aims by solely technical means to resolve problems that are essentially social and political, such as those posed by a pandemic crisis situation, which is a public health issue involving national and international solidarity.

Finally, many recent studies have shown that systems portrayed as the successful outcome of automation made possible by artificial intelligence are in fact based on a host of mostly unseen human tasks. The factual clarity and nowness conjured by the very word “data” is deceptive and disguises the inherent nature of data as a construct. Far from being pure and simple “data” for digital processing, the quality of data depends on the set procedures and methods put in place to produce it, on human processes for field observation, on bringing observables together, on the basis of selection criteria chosen by humans (and therefore potentially questionable), on the more or less systematic collection of relevant information, etc. More broadly, the human operations of encoding, programming, maintaining, refining, evaluating and interpreting data are needed across all levels of the digital process chain.

Thus, the operational effectiveness and ethical acceptability of a digital application for combating COVID-19 cannot be analyzed in isolation from other health measures, or from

the social processes implemented to control, interpret and correct, whenever necessary, the shortcomings inherent in reductionism and techno-solutionism. In this respect, experience shows that the countries which pioneered the use of digital tools for combating COVID-19, such as China, Taiwan and South Korea, derive effectiveness from using technology only by carefully fitting it into a much broader global and multidimensional crisis governance policy, where social and political participation by communities and intermediary bodies, between the individual and the state, makes it possible to continuously monitor the digital tool's effectiveness and how it is adapted to human needs in fighting the pandemic.

Ethical vigilance at all times

Beyond the risks previously mentioned, the development of digital tools to combat COVID-19 also constitutes a major ethical challenge for Western democracies, given the obvious risks to fundamental rights and freedoms that would result from the uncontrolled deployment of digital tracking or tracing tools. From the moment the crisis began to spread around the world, numerous ethics, legal and social science experts flagged this risk and undertook to analyze the various problems raised by these latest innovations. To facilitate coherent analyses of the broad range of social, ethical, legal and political implications, different expert groups have in recent weeks proposed frameworks for assessing the ethical implications of the digital technologies developed to fight the pandemic. These include documents issued by the CCNE and the CNIL in France, and the CEST and the CRE in Québec (Canada).

Prepared primarily by independent, academic, public or private bodies, most of these ethics guidelines are lists of principles and criteria, and applying them should enable states, public institutions and private companies to build human rights protections into the design of the technology from the earliest stages of development (ethics by design). While not attempting a full summary here, we note with some comfort that, interestingly, these different initiatives all share similarities and focus on fundamental principles and values around respect for privacy, personal data protection and security, and the intrinsic nature of the technology they must accommodate such as necessity, proportionality, transparency, loyalty, etc.

But concerns around ethics and the willingness to regulate digital technology had emerged before the current crisis highlighted so clearly the risks of rights infringement it involves. We note the influence of the GDPR, the European “privacy and electronic communications” directive, the OECD principles on Artificial Intelligence and the Montreal Declaration for the responsible development of AI on the frameworks currently being shared online for assessing issues of ethics around digital technology in a pandemic context.

While some might have thought briefly that the fight against the current pandemic would, under the guise of saving lives, erode the fabric of our democracies and usher in a new era of deregulated use, capture and commercialization of health data, or even widespread individual surveillance, we are happy to note that any such moves are meeting strong

resistance from civil society. Ethics benchmarks and safeguards are being effectively reinforced to meet the highest expectations of a broad cross-section of civil society actors. Saving lives doesn't mean trading off our deepest ethical aspirations, and using technology to achieve it is no reason to change our convictions.

Technology is only a tool for our collective intelligence and creativity to deploy in saving lives and we must adapt it to reflect the fundamental principles and values we hold dear. Ending the deadlock between upholding rights and freedoms and saving lives is a first win-win over chaos and unpunished unfair practices. There is no conflict between protecting data and combating the pandemic, or between the interests of the one and the interests of the many, as long as pursuing the common good does not exclude the use of personal data, provided that processing is carried out using responsible collective methods, and that measures to protect individuals are implemented.

FOR A NEW GOVERNANCE OF TECHNOLOGY

That being said, we need more than ever to put our creativity, governance and collective intelligence to use to preserve our deepest democratic convictions. But the risk of thought bias that pits individual rights and freedoms against public health and the protection of a collective remains real and constitutes a trap, particularly in modern Western culture which values the individual. Conversely, collectives – families, communities, institutions – always have the authority to restrict or even temporarily or permanently suspend their members' rights and freedoms (for example, by citing the common good, such as public health). Such political measures are routine in Asia, and particularly China, where curtailment of individual rights and freedoms is not rare. Across this dilemma-shaped landscape, the only path for public and collective intelligence can be a fine balance between the two extremes. In medio stat virtus. (Virtue lies in the middle.)

Most of the ethics assessment frameworks published in recent weeks clearly underline our need for collective governance of the current crisis, to which digital tools for tracing or monitoring individuals or populations must be subordinate.

Basing governance on key principles

The choices made by different states with regard to COVID-19 tracing applications are therefore not without significance and are based on policies and orientations around both technology governance and governance of the health crisis itself. Thus, an ethical viewpoint that highlights the values applied (voluntarily and explicitly or not) and their implications for the way these applications are designed, deployed and implemented can provide us with useful insights faced with the difficult choices that we, and our public decision-makers especially, must make in these times of crisis and, often, urgently.

To frame the collective crisis governance we are calling for, we would like to highlight some of the values that we believe are relevant to analyzing the various technological solutions, particularly those based on tracing:

- **Transparency.** Transparency is essential to debates around ethics. How do you discuss what might be right and good if you fail to understand the pros and cons involved in the discussions. In the case at hand, this means educating citizens, the public, around the issues in a debate that is certainly technical but ultimately political, involving citizen behaviour. What are the technology-based solutions? What are the alternatives? Who are the actors behind each solution? Who manages the system, with what data and how? So, in discussing a Bluetooth solution, it is important to know which population the solution is suitable for or which population will be excluded from it? With what risks of error? INRIA's efforts to give an open access description of the specifics of its technology system are commendable. It is the duty of the state, or rather of an independent commission of experts from various disciplines, to provide this information — not to make decisions but to respond to requests from all sides.

- **Added value.** Added value is beyond doubt the first criterion to be considered, although the meaning of the term covers a variety of ideas as to the expected benefit of the technology-based system. It is important not to favour one point of view over another, at least initially, but to consider all of them before taking any decision. Firstly, added value is measured in terms of public health and presupposes the comparison of various technology-based as well as non technology-based methods. Then, their contributions — separately or in combination — to combating new contaminations must be considered; added value is also assessed in economic terms in respect of the direct or indirect costs associated with implementing and operating tracing, as well as when calculating the impact of persistent pandemic on economic activity; added value is also assessed in terms of the population's psychological well-being.

- **Autonomy.** Autonomy and, therefore, respect for personal choice must be affirmed. Expressed in law through the concept of privacy, this ethical value must not mean the single-minded pursuit of self-centred choice but rather the pursuit of the capacity for self development. A democratic society has a duty to guarantee this ability such that this development constitutes a guarantee for everyone of full participation in democratic life. This view of autonomy thus prohibits pitting individual and collective interests against each other, but sees each as linked to other, in a dynamic relationship. Autonomy underlies the responsibility of every individual to work for the common good. We might add that pursuit of the common good cannot stop at national borders but must extend into a global solidarity imposed by the disease.

- **Social justice.** Social justice must not be set aside at a time when, in the face of disease, vulnerability is not the same for everyone, demanding that technology be made accessible to all and, first and foremost, to the most disadvantaged. The use of predictive artificial intelligence systems can lead to the stigmatization of certain categories of people suspected

of having the virus or certain neighbourhoods where infected people live. The aim must not be simply to protect individuals' data but to avoid discrimination against groups of people. Finally, the value of dignity disallows constant surveillance and public targeting of people with the disease (the coloured QR codes used in China). These values must be taken into consideration from the outset in designing technology-based solutions and throughout their lives (ethics by design).

- **Assessment of the public interest.** Assessing what is in the public interest must be inclusive and involve all stakeholders. It is important that room should be made for public discussion in a forum that brings together all stakeholders: the medical profession, representatives of civil society (especially vulnerable groups), business, education, etc. Decisions around choosing one system over another cannot be left to experts alone, but rather choices must be open for discussion and the choices assessed at both the technical level (ethics by design) and other levels (psychological, socio-economic, etc.). In the end, it falls to the constitutionally designated competent political authority, after hearing the opinions of the required "independent" bodies, to determine and set the parameters and mode of operation of any technology-based tool. To achieve (and maintain) full transparency and gain public confidence, the public authority must explain, in accessible terms, the reasons behind the choices made and the details of the decisions, including any AI algorithm models used. In this regard, we must not accept technology choices dictated by actors who might not operate transparently and have no interest in assessing issues of ethics.

- **Proportionality of implemented systems.** The principle of system proportionality must guide the choice of technology-based systems, if that option is selected. We must emphasize the minimization of data collected as a principle to be applied across the content and quality of data collected and processed as well as the duration of the processing operations. The temptation to preserve the technology-based systems implemented to confront the urgency of the moment is great; the longevity of the solutions devised in the heat of crisis (the September 2001 terrorist attacks of may be cited here) is often justified in the interests of innovation and the considerable effectiveness that technology can offer legislation. The need for strict compliance with the purpose for which systems are set up must be guaranteed. This implies that the management of health crisis systems exploiting personal health data should be entrusted to bodies bringing together health professionals and stakeholders (e.g., patient groups). Compliance with these principles can be ensured only by giving citizens the right to verify compliance against them.

CONCLUSION: CRITERIA FOR THE CHOICE AND IMPLEMENTATION OF TECHNOLOGICAL SOLUTIONS FOR A WAY OUT OF THE HEALTH CRISIS

In view of the many unknowns surrounding the virus and the factors of contagion, our societies must prepare to live with the threat of resurgence. The end of the crisis expected by the population therefore **requires shifting from health disaster management mode to a medium-term risk management process.**

Technology-based solutions to assist with deconfinement and economic recovery may thus be studied only as part of a broader risk management process that includes health measures, support for potentially infected people, and oversight of different types of economic and social activities.

To avoid being trapped in a network of double constraints that would prevent any decision-making, **a trade-off between the values underlying choices and the prioritization of principles we collectively wish to see respected must be made**, avoiding focusing the debate solely on respect for privacy.

In this exceptional situation, **assimilating data collected or used in managing pandemic risk with health data**, possibly placed through management agreements in the care of medical institutions, could offer satisfactory guarantees.

We believe the **principle of necessity**, stressed by the CCNE, should be favoured: if the usefulness of a technology-based solution is deemed too low in view of its implementation conditions (for example, an application that would require, in order to be effective, use by 60% of the population, but whose adoption would be voluntary), it would be advisable either to temporarily change the conditions of its deployment by adopting more directive measures, or to change strategy by deploying a different technology.

While tracking the trajectory of potentially infected people is the usual way of managing epidemics, and while one application may allow for its large-scale deployment, other approaches are emerging, such as **the use of predictive models of pandemic evolution, which make it possible to identify places and situations at risk**. Here again, ethical risks exist, such as seeing neighbourhoods or populations stigmatized, but they must be put into perspective in terms of the effectiveness of the solution in preserving public health. Thus, the debate cannot focus on the implementation modalities of a solution without questioning the appropriateness of the solution.

The implementation of measures allowing for medium-term management is a challenge in societies that have developed a strong aversion to risk. It requires careful support from public authorities. This support concerns, first of all, **the management and sharing of responsibility**: it cannot rest solely on the shoulders of the individual, at the risk of seeing infected people stigmatized; however, it cannot be borne solely by the collective, at the risk of seeing the least vulnerable people lose their sense of responsibility, to the detriment of social justice.

Any effective solution therefore requires solidarity among committed citizens. This assumes the following:

- **The role of the state coordinator** in determining public health priorities (for example, opening up sectors of the economy or not), promoting standards that facilitate national and international interoperability of digital devices, as well as in making resources available. In particular, business leaders, cannot be solely responsible for deciding on deconfinement measures amid a social situation that could become tense. The state will also have to define the adjustments for minimizing the discriminatory effects or harm suffered by certain categories of the population as a result of the use of such measures, for example, by introducing public policies to compensate for the loss of income for persons or communities who declare they are infected.
- The role of multidisciplinary “standard setting bodies” in the development of standards consolidating all the best practices for the responsible development and deployment of these new technologies and **facilitating their national and international interoperability.**
- **The role of the private sector** in the responsible development and deployment of these technologies and in the overall measures taken to ensure the health of employees and customers, as well as the responsible recovery of the economy.
- **The management role of communities** (municipalities, intermediary bodies) in the local application of measures, adapting them as much as possible to the realities on the ground and encouraging the population’s buy-in.
- **The role of each citizen** in the adoption of measures that are sometimes very restrictive, but which can effectively combat the pandemic, and the desire of the vast majority of citizens to avoid catching the virus and infecting their loved ones.

The governance of the selected technological solutions therefore appears to be the key factor conditioning their success or failure and must reflect the management of the responsibilities mentioned above. To do so, an appropriate body must be created, which must be:

- **Multipartite:** In addition to members of parliament and the government, who guarantee legitimate national representation, as well as experts, the specific body for governance and control of technological solution deployment must also include representatives of civil society and intermediary bodies, capable of inspiring trust and citizen commitment.
- **Agile:** As the situation and knowledge of the virus and its modes of propagation evolve, the chosen solution will have to be adapted in successive iterations.
- **Temporary:** If the risk of pandemic persists, the evolving and iterative nature of the proposed solutions should allow for their impact to be reduced and then discontinued as required, under the direct control of the governance body.



IN THE UPCOMING REPORT: A DECISION SUPPORT TOOL

In light of the close interplay between ethics, law and technology, a systemic and interdisciplinary approach is needed

Along with ethical questions, the deployment of technological applications to meet the challenges of the pandemic raises important legal issues. **All too often the debate focuses on privacy, even though many social values are involved.** In this context, we have designed an analytical method that goes beyond the scope of the Privacy Impact Assessment provided for in the GDPR to incorporate a more comprehensive set of factors. This approach, which is based on technical, legal and ethical issues, determines which values we as a society wish to collectively favour in the search for a way of living together that can create the conditions for promoting citizens' trust.

The individualistic view of privacy has to be overcome

Privacy can be a misnomer — which can certainly be explained by the North American usage that too often leads to equating the notion of respect for privacy with that of protection of personal data — and thereby masks the other underlying societal issues. On the one hand, this conflation reduces the scope of the debate and on the other, distracts attention from the essential point, which is assessing the effectiveness of the contemplated mechanism with regard to all the individual and collective freedoms as well as the fundamental principles to which our society wishes to adhere.

Thus, it is useful to discuss as a society — without relying solely on the views of experts — the social values that we want to protect. Only a multidisciplinary or interdisciplinary approach, combining and also opposing technical, legal and ethical issues, will make it possible to create the conditions for promoting shared citizen trust in publicly acceptable mechanisms. In this respect, instead of focusing solely on the conditions of conformity of technological solutions to a given legislative framework, it would be useful to take a fresh look at the standards in question. In other words, the challenge is to transcend a simple compliance and enforcement approach and return to the essence of the law, i.e., the social values we wish to promote.

Introduction of multi-factor impact assessments

The inextricable link between the technical, legal and ethical dimensions obliges us to address the issue of deploying technology-based tools in a systemic way. This makes it **possible to consider not only the technology itself, but also its use and governance.** Accordingly, the study of purely legal criteria and strictly legal conditions must be completed, fine-tuned and deepened, in order to provide a complete vision of the consequences that these technology-based solutions may have on individuals, as well as on groups of individuals and the democratic organization of our rule of law.

Rather than evaluating technology-based tools using data protection impact assessments (known as PIAs for Privacy Impact Assessment), we propose to introduce multi-factor analyses. In this respect, the idea of introducing Discrimination Impact Assessments (DIAs) had already been proposed by the Villani report “AI for humanity”. Initiatives must now go further in this direction, taking into account the following seven main principles, which set out the ethical values mentioned above:

1. Ethics goals and benefits to society
2. Accountability
3. Transparency and explainability
4. Equity and non-discrimination
5. Safety and reliability
6. Open data and intellectual property
7. Personal data and privacy

Each of these seven principles is considered from numerous perspectives to assess not only the relevance of the proposed solution with regard to the imperative of satisfying the general interest, but also the absence of negative effects. These different levels of evaluation thus go beyond the mere consideration of the legal consequences for the individual (and their private life), including those affecting the group to which they belong, and society as a whole. The objective is simple: to force developers of technology-based solutions and all those responsible for their deployment to ask themselves the right questions beforehand.

An analysis that integrates all of the issues for the individual, the collective and society

Such an analysis begins by studying the **objectives** that a technology-based solution seeks to address: What is the purpose of the tool? Is it used to support other actions? How is the effectiveness of the tool measured? What decisions does the tool enable? Have the technologies deployed already been tested to achieve this result? Is the solution effective above a certain threshold of use?

Under this approach, the **technical characteristics** of the contemplated solutions are then analyzed: What technologies are used? Where is the data stored? Are the infrastructures centralized or decentralized? Is the code proprietary or open-source? Who has access to it? Can the application be temporarily deactivated? In the case of sub-contracting the development of such applications, what information will the service providers have access to? To what extent will the chosen systems depend on third parties or will they feed information (e.g., via APIs) to state or private systems? To what extent is the data truly anonymous?

The solutions currently proposed suggest that the determination of whether they are **voluntary or mandatory is a significant risk factor**. Therefore, legal issues will be addressed alongside ethical issues in order to tackle the challenges of social acceptability and the society we wish to build: What are the possible risks of circumvention or misuse of the

solution? Is there a risk of widening the digital divide? Are new forms of discrimination or bias being introduced? Is the creation of a new right — such as a “right to deactivate” the technology-based tool for tracking — appropriate? Is the solution interoperable with other systems? Is the sharing of data between actors, particularly in the context of monitoring inter-state, regional or international travel, possible/desirable?

The essential question of **temporality** will also be taken into account. Indeed, any impact analysis will have to be continuously adapted as the scientific community confirms the characteristics of the virus. Moreover, determining whether or not a technology-based solution is temporary appears to be a prerequisite for the preservation of rights and freedoms, particularly as the limitation of these rights and freedoms cannot be justified outside the context of a state of public health emergency (provided that this is also defined and regulated). Finally, particular attention will also be paid to **the possibility for private companies to replicate these government initiatives**, initially intended for the public space, in the management of their private spaces, given that the state/citizen relationship has characteristics of a different nature to the employer/employee relationship.

For further information please email us :
contact@human-technology-foundation.org

CONTRIBUTORS TO “DEVELOPMENT AND GOVERNANCE OF TECHNOLOGY-BASED SOLUTIONS FOR A HEALTH CRISIS EXIT STRATEGY”

Name	Organisation	Capacity	Location
Comité de Pilotage			
Jean-Louis Davet	Denos Health Management	President	Paris
David Doat	Université catholique de Lille (ETHICS)	Lecturer in philosophy - director of the Ethics, Technology and Transhumanism Chair (ETH+)	Lille
Marie Éline Farley	Chambre de la Sécurité Financière du Québec	CEO	Montréal
Anne-Marie Hubert	EY	Associate Director	Montréal
Nathalie de Marcellis-Warin	CIRANO Polytechnique Montréal / OBVIA	CEO Full Professor	Montréal
Charles S. Morgan	McCarthy Tétraut	Partner	Montréal
Eric Salobir	Human Technology Foundation	President	Paris
Coordination du projet			
Chefs de projet			
Adrien Basdevant	Basdevant Avocats	Founding Lawyer	Paris
Caroline Leroy-Blanvillain	Basdevant Avocats	Lawyer	Paris
Analyste			
Pierre Gueydier	Human Technology Foundation	Research Director	Paris
Communication			
Antoine Glauzy	Institut de la technologie pour l'humain	Director	Montréal
Equipe éthique			
Maxime Allard	Collège Dominicain d'Ottawa	President	Ottawa
Allison Marchildon	Université de Sherbrooke / OBVIA	Associate Professor	Montréal
Manuel Morales	Université de Montréal / Fin-ML Network / OBVIA	Associate Professor	Montréal
Yves Poulet	Université de Namur / Université Catholique de Lille (ETHICS)	Honorary Rector of the University of Namur, Visiting Professor at the Catholic University of Lille	Namur

Bryn Williams-Jones	Ecole de Santé Publique de l'Université de Montréal / OBVIA	Full Professor	Montréal
Equipe juridique			
Edoardo Bardelli	Gattai, Minoli, Agostinelli & Partners	Trainee Lawyer	Milan
John Buyers	Osborne Clarke	Partner	Londres
Philip Catania	Corrs Chambers Westgarth	Partner	Melbourne
Massimo Donna	Paradigma Law	Managing Partner	Milan
Marco Galli	Gattai, Minoli, Agostinelli & Partners	Lawyer	Milan
Nikhil Narendran	Trilegal	Partner	Bangalore
Smriti Parsheera	National Institute of Public Finance & Policy		New Delhi
Patricia Shaw	Beyond Reach	CEO	Londres
Alexander Tribess	Weitnauer	Lawyer Partner	Hambourg
Padraig Walsh	Tanner De Witt	Partner	Hong Kong
Equipe technique			
Victor de Castro	Philips Health Systems	Chief Medical Officer	Paris
Maxime Fudym	Waxym	Developer	Paris
Roberto Mauro	Samsung Electronics	Managing Director Europe, Strategy & Innovation Center	
Gilles Mazars	Samsung Electronics	Director of Engineering – Advanced Innovation Lab	Paris
Pascal Voitot	Samsung Electronics	Applied Research Scientist in Deep/Machine Learning – Advanced Innovation Lab	Paris
Jean-Jacques Wacksman	Waxym	Developer	Paris