INSTITUT
Thomas More

Key Points 23
April 2020

Digital tracking: Why it's no

Cyrille Dalmont

The French government is currently working on the creation of a digital tracking application, called StopCovid. On Tuesday, April 28, the National Assembly is expected to vote on the deconfine plan and its "digital innovations in the fight against the covid-19 epidemic." We call on MPs to vote overwhelmingly against and the French to take stock of the danger that such an initiative poses to our freedoms and rights. Definition, actors involved, effects on our lives, ethical risks, technical safeguards, institutional safeguards, preparation for the future: all aspects are reviewed. This note explains why we should say no to the government's plan.

> "Those who would give up essential liberty to purchase a little temporary safety, deserve neither liberty nor safety."
>
> **Benjamin Franklin**

Many voices have already been heard on the issue of digital tracking in the fight against the coronavirus epidemic. Population monitoring tools are already in place in China, Singapore or South Korea, but also in Europe, Poland and Italy recently.

Initially presented as *"contrary to French culture"* by the Minister of the Interior, the project of a tracking tool, called StopCovid, quickly imposed itself on the executive after the vote of the law of "health emergency" on March 23. It took shape thanks in particular to the contribution of Mounir Mahjoubi, MP (LREM) of Paris, former President of the National Digital Council and former Secretary of State for Digital Affairs who presented a very comprehensive action plan on April 6 in a parliamentary note entitled "Tracking Mobile Data in the fight *against Covid-19*". Since then, the project has become more real every day.

On Tuesday, April 29, the Prime Minister will present to the National Assembly a Government Declaration "on the national strategy of the deconfinement plan as well as digital innovations in the fight against the covid-19 epidemic", followed by a debate and a vote. We call on Members to vote overwhelmingly against it. We call on the French to speak out against an initiative which, in the name of fighting the virus, poses an unprecedented danger to individual freedoms and fundamental freedoms. In addition to the violations of our concrete freedoms (freedom of movement, privacy, data), the creation of such a tool poses too great ethical and political risks to the nation. The legal and technical safeguards put forward by the project's advocates (volunteering, Bluetooth and data anonymization) are largely inadequate. Institutional safeguards (e.g. Constitutional Council) no longer fulfil their traditional function because of the "state of emergency".

The speed with which France, like most European countries, has swung into this digital nightmare is extremely worrying. It justifies a clear and audible "no" to the executive's plan. It will call for massive and courageous initiatives to protect our digital freedoms in the second stage. Ten key points explanations.

1. What is digital tracking?

Digital *tracking* is a method used to track people's movements. "Backtracking" helps identifying the interpersonal relationships of individuals traced by the system. The term "digital trace" refers to all the information that a digital device records about the activity or identity of its user by means of tracers such as cookies, either automatically or through an intentional deposit. Search engines, blogs, social networks, e-commerce sites, but also smart cards, transport tickets, mobile phones: all systems that require identification or interaction are likely to capture information about the user - journeys, queries, preferences, purchases, connections, evaluations, contact information. Traces are not messages, but data that, taken in isolation, make little sense but which, grouped, processed and combined in important databases, can reveal meaningful, strategic or sensitive information.

Digital tracking technology is not new in France as it is already used for detainees who are offered, under certain conditions, the wearing of an "electronic bracelet" or Electronic Surveillance Placement (PES) **[1]**. It is a regime established by the Law of 12 December 2005 on the recidivism of criminal offences and extended to "security supervision" by the Detention Act No. 25, 2008. On 21 April, Ludovic Le Moan, president of Sigfox, a French specialist in very low-speed networks for connected objects, proposed the distribution of an electronic bracelet, as an alternative to a digital tracking application, to all French people in the run-up to deconfinement **[2]**. This is already the case in Hong Kong, where a wrist sensor has been imposed on people in quarantine, and tests are underway in Liechtenstein and South Korea for certain categories of people considered "at risk".

[1] French Ministry of Justice, "Le placement sous surveillance électronique", 10 May 2019, available here.
[2] Ludovic Le Moan, "On va dire que je vends ma soupe, mais un bracelet, c'est mieux qu'une appli de tracing", *Les Echos*, 21 April 2020, available here.

2. What is the government's StopCovid application project?

It is an application project, using the Bluetooth system **(Point 6)**, "contact tracking", that is, tracking people and their interpersonal relationships through their smartphones in order to be able to track the sick and people they are likely to have infected during their daily movements. According to Cedric O, Secretary of State for Digital affairs and Olivier Véran, Minister of Health, *"the idea would be to warn people who have been in contact with a positive patient in order to be able to get tested, and if need to be taken care of very early, or to confine themselves"* **[1]**.

This type of device already exists in some countries. It can be mandatory (as in China, South Korea, Taiwan, Poland or Israel) or optional with varying degrees of incentive (as in Singapore). If the French government, which is currently working with other European governments **(Point 3)**, is reassuring in explaining that the scheme will be based on the volunteering of people, it should be remembered that these tools, from the softest to the most restrictive, are cumulative between them and are based on the same requirements: identifying people, following them in their movements and interpersonal relationships and possibly controlling their place of residence.

3. Who are the players involved in digital tracking?

In his note entitled "Tracking mobile data in the fight against Covid-19", Paris MP (LREM) Mounir Mahjoubi explains that data mapping collective mobility is already widely used, especially by local authorities who buy them from telephone operators (particularly to analyze tourist flows). It proposes to use the data mapping of individual mobility and states that "*many mobile operators and application providers say they are willing to work with health authorities."* He explains that *"to transmit or receive information, whether it is a call, an SMS or Internet access, mobile phones connect to the most powerful relay antenna being nearby. When data transfers, operators record login information and store it in memory for a year. It is then possible for them to attest to the presence of a telephone around a terminal, within a given perimeter, with a history of 12 months. Orange, Free, SFR and Bouygues Telecom share 40,000 relay pylons in France"* **[2]**.

In order to be able to set up a digital tracking system, the participation and agreement of several actors is indeed necessary: the European Union in the first place in order to deviate from the rules of personal data protection (RGPD), digital actors in order to reconcile the tracking tools created with the operating systems of smartphones, the European states to make the different systems compatible with each other in the event of allowing the free movement of people and finally operators to access their global population mapping data. A quick overview of the forces involved.

●

[1] Cédric O and Olivier Véran, "'L'application StopCovid retracera l'historique des relations sociales' : les pistes du gouvernement pour le traçage numérique des malades", *Le Monde*, 8 April 2020, available here.
[2] Mounir Mahjoubi, "Traçage des données mobiles dans la lutte contre le Covid-19. Analyse des potentiels et des limites", Parliamentary Note, 6 April 2020, available here.

The European Union • On March 20, the *European Data Protection Board* (EDPB) lifted the ban on the exchange and processing of the personal information of EU citizens, stating that *"the RGPD allows relevant health authorities to process personal data in the context of an epidemic, in accordance with national law and under the conditions set out in it"* **(1)**. On the 23rd, Thierry Breton, European Commissioner for internal market and digital, asked European mobile operators to provide Member States with their customers' geolocation data **(2)**.

Digital players • Apple and Google announced on April 10 a joint approach to establish a software infrastructure for "social tracking" applications as part of the fight against the Covid-19 epidemic **(3)**. It finally took less than twenty days between the decision of the EDPB and the announcement of the collaboration of the two digital giants. This announcement, however, lays the groundwork for a global system of tracking populations and sharing their data **(4)**.

States • A few days ago, Cédric O, Secretary of State for Digital Affairs, announced that Germany, France, Italy, Monaco, the United Kingdom and Switzerland were in talks to jointly develop a clean digital tracking system, not using the solution proposed by Apple and Google: *"It's a question of health and technological sovereignty",* he argued **(5)**. On April 26, Germany announced its exit from the consortium and its support for the two web giants' solution: *"Our aim is that the tracking application is ready to be used very soon and that it is widely accepted by the population",* said Jens Spahn, Minister of Health, and Helge Braun, Chief of Staff to Chancellor Angela Merkel **(6)**. While it was one of the first European countries to think about it, Belgium announced that it was abandoning its plans **(7)**.

Telecom Operators • On April 17, Orange CEO Stéphane Richard told France Inter radio: *"Today we have a prototype application that works"* **(8)**. He said he was ready to bring his group's expertise to the "StopCovid" application desired by the executive. The boss of Orange is campaigning for the use of Bluetooth **(Point 6)**.

4. Freedom of movement, privacy, data: what effects of digital tracking on our lives?

At the individual level, the potential effects of digital tracking on our lives are manifold. We will just synthesize them in four points.

(1) CEPD, "Statement on the processing of personal data in the context of the COVID-19 outbreak", 20 March 2020, available here.

(2) "Coronavirus : la Commission européenne réclame des données d'opérateurs téléphoniques pour évaluer l'effet des mesures de confinement", *Le Monde*, 25 March 2020, available here.

(3) "COVID-19 : Apple et Google travaillent ensemble à une technologie de traçage des contacts", Apple, Press release, 10 April 2020, available here.

(4) Cyrille Dalmont, "Comment les Gafam veulent surfer sur la crise sanitaire mondiale", *Marianne*, 17 April 2020, available here.

(5) "Application StopCovid: le gouvernement n'utilisera pas la plateforme d'Apple et Google", BFM TV, 26 April 2020, available here.

(6) "Application de traçage : l'Allemagne mise finalement sur Apple et Google", *Le Point*, 26 April 2020, available here.

(7) "Le traçage via téléphone portable a du plomb dans l'aile", RTBF, 25 April 2020, available here.

(8) Stéphane Richard, "La question sera celle des garanties qu'on peut donner", France Inter, 17 April 2020, available here.

Digital tracking is an inherent major attack on the fundamental freedom to come and go. At this stage, it is certainly based on volunteerism **(Point 2)** but it is also presented as one of the necessary conditions for a successful deconfinement: there is therefore no guarantee that the use of this device will not become mandatory tomorrow, in the event of a second wave or a new epidemic.

This also represents an invasion of privacy since the user's interpersonal relationships and movements will be known through continuous exchanges between the user's smartphone and all the connected objects they will encounter in a day.

This will also allow multiple applications other than StopCovid to collect data in the event that the user's Bluetooth protocol is permanently activated **(Point 6)**. There is a concatenation risk of raw data collected by digital actors; this would allow them to establish future digital profiles and access health data, which they are particularly interested in **(Point 8)** when they were often out of reach until now.

Finally, there is a significant risk that the exception will become the rule and that this type of tools will in the future be used for multiple uses, always of course in the name of the safety of the participants and others: follow-up of street events, followed by supporters in sporting events, followed by participants in major cultural events such as festivals etc.

5. Designation of the "good citizen", risk of switching to a mandatory system and threats in the post-crisis: digital tracking raises serious ethical risks

Digital tracking technologies pose major ethical risks. In fact, this type of tool can be used to track people who have been in contact with a person carrying Covid-19 and to trace the Covid-19's movements. But for what purpose? Enforcing containment and automating and simplifying the controls that law enforcement refuses to do for lack of means and protective equipment **(1)**. Let's go to the end of the logic: isn't an automation of sanctions to be feared in case of prohibited travel?

This is where we reach the ethical tipping point. If the comparison with the Chinese "social credit" system still seems excessive to some **(2)**, it is clear that the logic of digital tracking brings us closer: there is certainly no notation of behaviors but this slope leads to the portrait of the "good citizen" and, by contrast, that of the "bad citizen". The authorities will naturally argue that their intention is a hundred miles away from that. But when it comes to freedoms, we do not judge intentions but deeds. Secondly, what guarantee is there that a first phase based on volunteerism will not succeed, if it does not achieve the expected objective, a second compulsory phase? The debate is already taking place in Italy, where some argue that the application of *Immuni* tracking should be mandatory as soon as it is put into service and that the wearing of the electronic bracelet should be imposed on the elderly **(3)**.

[1] "Coronavirus : les syndicats de policiers lancent le mot d'ordre 'pas de masque, pas de contrôle'", France Bleue, 26 March 2020, available here.
[2] Emmanuel Dubois de Prisque, *Le système de crédit social : comment la Chine évalue, récompense et punit sa population*, Institut Thomas More, Note 36, July 2019, available here.
[3] "Coronavirus, l'App (quasi) obbligatoria e l'ipotesi braccialetto per gli anziani", *Corriere della Sera*, 20 April 2020, available here.

But the most important ethical question is: once the Rubicon is crossed, what will happen? Who can honestly imagine that these technological tools will be stored in the Pandora's box that we have just opened because the health crisis will be over? In the pages of the *Financial Times* of March 19, Yuval Noah Harari warned that *"emergency measures have a bad habit of staying in place even after the emergency, especially since there are always new threats"* **(1)**. Unfortunately, recent history has proved him right: there will always be another crisis, another attack, another urgency to justify the use of these technologies. What happened with the anti-terrorism laws and the measures taken under the state of emergency in France between 2015 and 2017? They have been largely incorporated into the Homeland Security Code. The temporary one has become permanent.

Why not the political, economic and social emergency tomorrow justify the use of tracking in the areas of terrorism, money laundering, the fight against tax evasion, covert labour, prostitution or human trafficking, or even simply school absenteeism?

6. Bluetooth and data anonymization: the illusion of technical safeguards

Proponents of the project highlight two technical safeguards in response to ethical concerns **(Point 5)** and policies that are taking place against the Proposed StopCovid application: the use of Bluetooth technology and data anonymization.

Bluetooth is a communication standard that allows two-way data exchange at very short distances using UHF (ultra-high frequency) radio waves. It is used to simplify connections between electronic devices by removing wired links. The government's idea is to build on the Robert Protocol (for *ROBust and privacy-presERving proximity Tracing),* recently developed by INRIA (National Research Institute for Digital Science and Technology, France) and Fraunhofer AISEC (Germany) as part of the PAN-European Privacy-Preserving *Proximity.* According to its creators, this protocol *"can be used to build mobile contact tracking applications. It was designed to strictly respect the European data protection framework and be able to withstand credible attacks"* **(2)**. So, there would be no problem using Bluetooth. This is also the view of Mounir Mahjoubi, who in his parliamentary note states that *"Bluetooth contact tracking applications seem to create consensus because of their more protective aspect [than GPS] of individual freedoms"* **(3)**.

More protective than GPS but not very protective anyway! Everyone knows that Bluetooth is a permanent vacuum cleaner of raw data. Experts even talk about *"talkative protocol",* constantly seeking to be tamed with other tools with this protocol: this makes sense since it is its primary function **(4)**. This means that the connected device (here the smartphone) will interact with all other connected devices, not just those with the StopCovid app. Meanwhile, unlimited amounts of raw data will be collected by digital giants on our smartphones. The digital giants are already doing this in normal times but, with the obligation to keep Bluetooth on, the phenomenon will only increase. To be convinced, it is enough to

●

(1) Yuval Noah Harari, "The World after Coronavirus", *Financial Times*, 19 March 2020, available here.
(2) INRIA, "Publication du protocole ROBERT (*ROBust and privacy-presERving proximity Tracing*) ", 18 April 2020, available here.
(3) Mounir Mahjoubi, *op. cit.*
(4) Hervé Le Mar, "Connexion Bluetooth : comment ça marche ?", Échos du Net, 6 August 2019, available here.

remember some recent scandals: the one at Cambridge Analityca in 2018, in which Facebook was accused of recovering, without their consent, the personal data of fifty million users **(1)**; that of Google's impeachment with the Nightingale project that captured the health data of millions of Americans **(Point 8) (2)**; or that of Apple accused in a collective complaint of reselling the personal data of iTunes users **(3)**.

According to Strategy Analytics, there are 22 billion connected objects in the world (smartphones, speakers, televisions, watches, tablets, computers, game consoles, alarms, cameras, vending machines, public transport terminals, etc.) and there will be about 50 billion by 2030 **(4)**. Not all of them use the Bluetooth system, but in order to be compatible with smartphones, most are.

Last but not least, the Bluetooth system is hackable, as all other systems, and many security flaws are regularly discovered. The last one was a few weeks ago: in February 2020, Google released a fix for a critical flaw that affects Android's Bluetooth subsystem and potentially allows you to take control of any vulnerable device within range. Experts then advised Android users to turn off Bluetooth while waiting for the update **(5)**.

The same goes for data anonymization. It is a very fragile defence. The European shield of the RGPD – now suspended – was already a far-reaching line of defence since, while it guaranteed individuals against the arbitrariness of basic cases (sex, race, sexual orientation, political or trade union tendencies, etc.), it did not constitute an effective protection against the "concatenation" of non-personal raw data which, when aggregated and reconstructed, would achieve the same result **(6)**.

Indeed, by assembling a wealth of data concerning, for example, our travels (from our place of residence, work, vacation, etc.), our habits (types of products consumed, queries on search engines, etc.), the people we meet (data crossings of several users), the payments we make, our waking and bedtimes, all cross-referenced with the equivalent raw data of other occupants of our home or other employees of our company (also equipped with connected devices), digital giants can already obtain more efficient, accurate, non-personal profiling with a much greater market value than the few personal data protected by the RGPD.

But beyond that, with permanent Bluetooth interactions, it will be extremely simple to identify an individual. Luke Rocher, a researcher at the Institute *of Information and Communication Technologies, Electronics and Applied Mathematics* at the Catholic University of Leuven, says that "*in the USA, we have worked on US data, fifteen demographic information (age, sex, etc.) is sufficient for re-identification to be possible in 99.98% of cases",* based on raw, non-personal and anonymized data (**7**). Fifteen pieces of information? The StopCovid app, with the constant activation of Bluetooth, will collect hundreds or even thousands of them a day.

●

(1) Julia Carrie Wong, "The Cambridge Analytica scandal changed the world – but it didn't change Facebook", *The Guardian*, 18 March 2019, available here.
(2) Rob Copeland, "Google's 'Project Nightingale' Gathers Personal Health Data on Millions of Americans", *Wall Street Journal*, 11 November 2019, available here.
(3) "Surprise, Apple vendrait aussi nos données personnelles", *Capital*, 27 May 2019, available here.
(4) Strategy Analytics, "Global Connected and IoT Device Forecast Update", 19 May 2019, available here.
(5) "Android : grosse faille de sécurité sur le Bluetooth", Futura Tech, 10 February 2020, available here.
(6) Cyrille Dalmont, "Données personnelles : pourquoi le RGPD est déjà dépassé", *Les Echos*, 22 November 2019, available here.
(7) Luc Rocher, "Des données anonymes…ou pas !", ICTEAM, Université catholique de Louvain, 18 September 2019, available here.

7. CNIL, Council of State and Constitutional Council: institutional safeguards look elsewhere

Faced with the executive's initiative, one would expect certain institutions or authorities to rise in the name of preserving our freedoms and fundamental rights. This would probably be the case in normal times – at least we must hope so... In a "health state of emergency", unfortunately, the situation is different.

The National Commission on Information Technology and Freedoms (CNIL) • At its Senate hearing on April 16, Marie-Laure Denis, President of the CNIL, called for the focus on *"least intrusive solutions"*, stressed the *"temporary nature"* of the StopCovid application and called for *"data suppression"* after the crisis. She also highlighted the limitations of the tool in relation to the digital white areas and the lack of equipment for some people (especially the elderly). But it was not particularly offensive in defending citizens' freedoms and did not for a moment discuss the very principle of digital tracking.

This reluctance is in line with the evolution of the CNIL doctrine (which has changed considerably since the great founding law of 6 January 1978 on computers, files and freedoms) and its missions under the influence of European Union legislation, which has gradually imposed a logic of commercial law over the protection of civil liberties. Since the emergence of the RGPD and its system of economic sanctions against companies, the CNIL has moved from being a guardian of civil liberties to a guarantor of competition law. Marie-Laure Denis's words simply confirm this evolution.

Under the weight of criticism, the CNIL nuanced its president's position ten days later by formally calling for *"vigilance"* and stressing *that "the application can only be deployed if its usefulness is sufficiently proven and if it is integrated into a comprehensive health strategy. It asks for some additional guarantees."* It asks *"to be able to vote again after the debate in Parliament, in order to examine the final modalities for the implementation of the scheme, should it be decided to use it"* **(1)**.

The Council of State • On 18 March, the Council of State gave its opinion on the draft law and the emergency organic bill to deal with the Covid-19 epidemic, presented by the government. Unsurprisingly, the Council approved them **(2)**. It applied its classic jurisprudence in the case of "exceptional circumstances", namely that *"the existence of exceptional circumstances is such as to justify measures which would, under normal circumstances, be considered illegal"* **(3)***.* It should be remembered, however, that this case law was developed to respond to the emergency during the First World War **(4)**. It is therefore surprising to apply to a health crisis.

The Constitutional Council • The Constitutional Council was referred five days later. In its decision, it validates the position of the Council of State: *"In order to deal with the consequences of the outbreak of the covid-19 virus on the functioning of the courts, the single article of this organic law merely suspends until 30 June 2020 the period within which the Council of State or the Court of Cassation must decide*

●

(1) CNIL, "Publication de l'avis de la CNIL sur le projet d'application mobile 'StopCovid'", 26 April 2020, available here.
(2) Conseil d'État, "Avis sur un projet de loi et un projet de loi organique d'urgence pour faire face à l'épidémie de COVID-19", 18 March 2020, available here.
(3) Paris Bar Association, "Circonstance exceptionnelle en droit administratif", La Grande Bibliothèque du droit, available here.
(4) Jean Massot, "Le Conseil d'État face aux circonstances exceptionnelles", *Les Cahiers de la Justice*, vol. 2, n°2, 2013, pp. 27-39, available here.

on the reference of a priority question of constitutionality to the Constitutional Council and the one in which the Latter must rule on such an issue. It does not call into question the exercise of this remedy or prohibit the decision on a priority issue of constitutionality during this period" (1). "*This is the first time that the Council has adopted the so-called 'Theory of the Council of State', without adding anything to it*", said Paul Alliès, professor emeritus at the Faculty of Law in Montpellier (2).

8. Digital tracking is a first step towards commodification of health data at European level

An insufficiently raised point in the debate on digital tracking is the very real issue of the health data market. To fully understand the ambition of digital players who are positioning themselves on digital tracking (particularly through the unprecedented rapprochement between Google and Apple), some figures are illuminating: in October 2019, Frost and Sullivan has estimated the value of the global digital health market at $234.5 billion by 2023 (up 160% from 2019), in a broader health market (digital, diagnostic, estimated at $6,500 billion to $7 trillion, which equates to about 8.5 to 9.3% of global GDP (3). To this must be added the market of the Internet of Things (IoT) which, according to a Fortune Business Insight study, could reach more than 1,100 billion dollars by 2026 (4).

What is the relationship between health data and digital tracking? It began ten years ago through various buyouts and takeovers in a multitude of health start-ups, with the very clear goal of becoming "third parties of trust" between the user and his caregiver through the Internet of Things (5). To do this, the digital giants have embarked on the massive collection of data, however insignificant it may seem at first glance, and their processing through algorithms or Artificial Intelligence in order to know us better than our own doctor, sometimes better than ourselves. Google was pinned a few months ago by the Wall Street *Journal* about its Project Nightingale, which allowed it to collect personal data on the health of millions of Americans through a partnership with Ascension, the second largest U.S. health network (6).

Through digital tracking, interpersonal interactions and data exchanges between connected objects, digital actors will be able to easily establish the digital profiles of sick people and their care (therapists, hospitals, treatments, etc.) – this in the long run in order to be able to offer them their future health solutions with an extremely precise customer targeting.

[1] Conseil constitutionnel, Décision n° 2020-799 DC du 26 mars 2020, available here.
[2] Paul Alliès, *Crise sanitaire et crise démocratique. La normalisation de l'exception (2/5)*, Mediapart, 11 April 2020, available here.
[3] BPI, "E-santé : vers un marché de 234,5 milliards de dollars", 31 October 2019, available here.
[4] Fortune Business Insight, "IoT Connected Machines Market Size", October 2019 available here.
[5] "Les 'Gafam' s'intéressent de plus en plus à notre santé", France Info, 4 May 2016, available here.
[6] Rob Copeland, "Google's 'Project Nightingale' Gathers Personal Health Data on Millions of Americans", *Wall Street Journal*, 11 November 2019, available here.

9. Why should MPs vote against the government's plan?

For all the reasons we have just mentioned, MPs must vote against the Government Declaration to be submitted to them on Tuesday 28 April. If they do not convince them, one last should suffice: they are asked to approve an extremely sensitive tool whose operation is not yet known since, by the admission of Cédric O, Secretary of State for Digital, the development of the StopCovid application will not be completed by that date [1].

But the *"concern for freedom"* dear to Camus, the most basic morality, the most banal prudence, Montesquieu's recommendation to legislators of all time that *"we must touch laws only with a trembling hand"* are clearly no longer guides for our politicians. The creation of a digital tracking instrument for the French population, even on the basis of volunteerism, even with the so-called safeguards announced, is a real catastrophe – from the Greek wordστροφή *"katastrophê",* which means "reversal". How do you explain such a setback, such a shift?

The exceptionality of the situation is not enough. It comes from afar. The evolution that began in the 1990s, which saw an increase in the number of ever more restrictive security policies of fundamental freedoms, with no real safeguards and no conclusive results, contributing significantly to this result. More than fifty such laws have been passed in the last thirty years. The example, cited above, of the measures taken during the state of emergency between 2015 and 2017 and incorporated into the Homeland Security Code **(Point 5)** illustrates this sad state of affairs. With the exception becoming the norm through successive "states of emergency", Parliament has become, each time a little more, a mere sluggish observer of the government's action [2].

At the same time, the derogatory prerogatives of the common law of the administration have increased by the same amount. The technological hubris is no longer the preserve of GAFAM but becomes that of the Minister of the Interior (and the policeman) or the Minister of Finance (and the official of Bercy). The widespread use of video surveillance, biometrics and the monitoring of social networks offer the state unprecedented instruments of control over our lives, which contribute to creating a new relationship of power to the citizen. Yet this patient nibbling of civil liberties never seems sufficient to a hypercentralized, hyper-administered state and, despite this, a rare inefficiency in a crisis like the one we are going through [3].

For all these reasons, when they vote, MPs must bear in mind the words that their illustrious predecessors engraved in the preamble to the Declaration of Human and Citizen Rights: *"The representatives of the French people, constituted in the National Assembly, considering that ignorance, oblivion or disregard for human rights are the only causes of public misfortune and corruption of governments [...]".* Civil liberties and fundamental rights are never definitively acquired, but always the stakes of power struggles and the result of precarious balances.

[1] "Coronavirus : l'application StopCovid 'ne sera pas prête' avant le débat parlementaire qui lui sera consacré", *Le Monde*, 17 April 2020, available here.

[2] Paris Bar Association, "L'état d'urgence dans le droit commun : quand l'exception devient la règle au mépris des libertés", 30 October 2017, available here.

[3] We reference masks, tests, resuscitative equipments, lab coats, etc. Here is a distressing illustration: "Dépistage du coronavirus : les raisons du fiasco français sur les tests", *Le Monde*, 24 April 2020, available here.

10. Preparing for post-covid19: civil liberties and fundamental rights are not only for happy days?

One crisis replaces another, one emergency gives way to the next. There will always be good reasons to postpone the fundamental reflection that is essential on our digital freedoms. Yet civil liberties and fundamental rights cannot be seen as subjects of fine discourse, which may one day be addressed if happy days return.

We cannot save ourselves from a deep and comprehensive reflection aimed at guaranteeing civil liberties and fundamental rights in the face of the increasingly systematic abuses of digital actors and, henceforth, of States, or sometimes even of collaboration with each other (it is indeed worth remembering that in our own country, officials have been working with Facebook for more than a year to develop a common strategy to "combat hateful content" without overly being moved).

This reflection will have to lead to a revision of our legal system and the creation of new tools to slow down these security excesses and the shift of our Western democracies towards the generalization of the identification and monitoring of people. The Thomas More Institute is currently working on such a solution.

Our publications

🟦 Live Europe
🟨 International Issues
🟪 Immigration & Integration
🟧 Society & Culture
🟩 Economy & Competitiveness
🟥 Institutions & Political Life

- 🟨 **Pourquoi faut-il soutenir l'île-État de Taïwan**, Jean-Sylvestre Mongrenier and Laurent Amelot, April 2020
- 🟨 **La planète à l'heure du coronavirus : un monde affolé qui bascule dans l'inconnu**, Jean-Sylvestre Mongrenier, March 2020
- 🟥 **Municipales 2020 : propositions pour la revitalisation des centres-villes et des centres-bourgs**, Édouard Guillot, February 2020
- 🟥 **Municipales 2020 : propositions pour la famille et les solidarités de proximité**, Elizabeth Montfort, February 2020
- 🟥 **Municipales 2020 : propositions pour la sécurité**, Édouard Guillot, February 2020
- 🟥 **Municipales 2020 : propositions pour l'écologie locale**, Jean-Thomas Lesueur and Édouard Guillot, February 2020
- 🟥 **Municipales 2020 : propositions pour le développement économique local**, Sébastien Laye, February 2020
- 🟨 **De l'« OTAN arabe » à l'« OTAN Moyen-Orient » : quels enjeux pour les puissances occidentales ?**, Jean-Sylvestre Mongrenier, January 2020
- 🟦 **Conférence sur l'avenir de l'Europe : beaucoup de bruit pour rien ?**, Jérôme Soibinet, December 2019
- 🟨 **Nation et religion : l'expérience marocaine**, Sophie de Peyret, December 2019
- 🟩 **Les causes monétaires de l'échec économique français**, Sébastien Laye and Didier Long, December 2019
- 🟦 **Macron, l'OTAN et la défense de l'Europe : un président ne devrait pas dire ça**, Jean-Sylvestre Mongrenier, November 2019
- 🟪 **L'islam en France, le temps des solutions : 35 propositions pour agir maintenant**, Sophie de Peyret, November 2019
- 🟦 **Emmanuel Macron au piège de la « souveraineté européenne »**, Jérôme Soibinet, October 2019
- 🟨 **L'opération turque dans le Nord-Est syrien, sa portée militaire et ses perspectives géopolitiques**, Jean-Sylvestre Mongrenier, October 2019
- 🟨 **Is It About the Money? Insights About Terrorism and Terror-Financing in West-Africa**, Antonin Tisseron, September 2019
- 🟨 **Libertés religieuses : le Parti communiste chinois contre les religions**, E. Dubois de Prisque and J.-S. Mongrenier, September 2019
- 🟧 **Familles monoparentales et PMA : quand la loi fabrique de la fragilité sociale**, Elizabeth Montfort, September 2019
- 🟥 **Projet de loi « engagement et proximité » : un geste pour les communes modeste et technocratique**, Jean-Thomas Lesueur, July 2019
- 🟨 **Le système de crédit social : comment la Chine évalue, récompense et punit sa population**, Emmanuel Dubois de Prisque, July 2019
- 🟧 **PMA, filiation, transmission : quels sont les besoins de l'enfant ?**, E. Montfort, M. Fontanon-Missenard, Ch. Flavigny and Ch. Delsol, June 2019
- 🟨 **Géopolitique et ambitions militaires de la France : l'Europe ne suffit pas**, Jean-Sylvestre Mongrenier, Jun 2019
- 🟦 **Après les élections du 26 mai, la « doctrine Macron » à l'assaut de l'Europe**, Jean-Thomas Lesueur and Jérôme Soibinet, May 2019
- 🟦 **L'« armée européenne », la défense de l'Europe et les enjeux géopolitiques occidentaux**, Jean-Sylvestre Mongrenier, May 2019
- 🟦 **Principes, institutions, compétences : recentrer l'Union européenne**, Report, May 2019
- 🟦 **Pour une autre politique monétaire. Flexibiliser l'euro et réformer la BCE**, Sébastien Laye, May 2019
- 🟦 **Quelle contribution européenne face aux nouveaux défis de l'immigration ?**, Report, April 2019
- 🟩 **Les origines économiques du mouvement des « gilets jaunes »**, Sébastien Laye, March 2019
- 🟨 **Usage et force des symboles dans la stratégie de Daesh. L'exemple du drapeau**, Sophie de Peyret, March 2019
- 🟨 **Politique française dans le golfe Arabo-persique : une nécessaire clarification**, Jean-Sylvestre Mongrenier, March 2019
- 🟨 **Jihadist Threat : the Gulf of Guinea States up against the wall**, Antonin Tisseron, March 2019
- 🟧 **Pour une école de la liberté et des responsabilités**, Report, February 2019
- 🟥 **La démocratie en circuit court. Plaidoyer pour la réforme de l'État, la décentralisation et le RIP local**, Jean-Thomas Lesueur, February 2019
- 🟨 **La Chine e(s)t le monde. Essai sur la sino-mondialisation**, Book of E. Dubois de Prisque and S. Boisseau du Rocher, éditions Odile Jacob, 2019
- 🟪 **Les migrations de masse, le droit international et le « Pacte mondial » de l'ONU**, Jean-Thomas Lesueur, December 2018
- 🟧 **Intelligence artificielle et santé : 10 propositions anti-brouillard pour régulation éclairée**, Cyrille Dalmont, November 2018
- 🟨 **Chine-Afrique : au-delà des intérêts économiques, l'indifférence réciproque**, Emmanuel Dubois de Prisque, September 2018
- 🟩 **2008-2018 : a-t-on retenu les leçons de la crise financière ?**, Sébastien Laye, September 2018
- 🟨 **Stabilising the Middle East : Stakeholders, Threats, Strategies**, Jean-Sylvestre Mongrenier, July 2018
- 🟦 **La Pologne, acteur géostratégique émergent et puissance européenne**, Jean-Sylvestre Mongrenier, June 2018
- 🟨 **L'accord nucléaire iranien, la stratégie américaine et les illusions européennes**, Jean-Sylvestre Mongrenier, May 2018
- 🟪 **Quelle politique migratoire pour la France ?**, Jean-Thomas Lesueur, May 2018
- 🟦 **Brexit: What impact on British global power?**, Pierre-Alain Coffinier, April 2018
- 🟩 **Péril sur l'électricité belge**, Book of Jean-Pierre Schaeken Willemaers, Brussels, éditions Texquis, 2018
- 🟨 **La France a-t-elle besoin d'un deuxième porte-avions ?**, Jean-Sylvestre Mongrenier, 2nd edition, April 2018
- 🟩 **Formation professionnelle : 6 propositions pour aller plus loin**, Michel Fourmy, April 2018
- 🟩 **Le modèle scandinave est-il bon pour la France ?**, Sébastien Laye, February 2018
- 🟦 **Coopération structurée permanente : un étroit chemin vers une défense européenne**, Jean-Sylvestre Mongrenier, December 2017
- 🟨 **Stratégie américaine au Sahel : vers un tournant décisif ?**, Jérôme Pigné, November 2017
- 🟨 **XIXe congrès du PCC : le triomphe de la religion politique chinoise**, Emmanuel Dubois de Prisque, October 2017
- 🟨 **Revue stratégique : une « France forte » mais avec quels moyens ?**, Jean-Sylvestre Mongrenier, October 2017
- 🟦 **Macron et l'Europe : un volontarisme sans dessein ni méthode**, Jean-Sylvestre Mongrenier, Sepember 2017
- 🟩 **L'utopie du tout renouvelable**, Book of Jean-Pierre Schaeken Willemaers, Brussels, éditions de l'Académie royale de Belgique, 2017
- 🟦 **Les cinq scénarios du Brexit**, Pierre-Alain Coffinier, July 2017
- 🟨 **Gaullo-mitterrandisme ou néo-conservatisme : quelle diplomatie pour la France ?**, Jean-Sylvestre Mongrenier, June 2017
- 🟩 **Législatives 2017 : les failles du programme économique de la « République en marche ! »**, Sébastien Laye, June 2017
- 🟨 **L'Asie du Sud-Est et la tentation autoritaire : l'impact du modèle chinois**, E. Dubois de Prisque and S. Boisseau du Rocher, June 2017
- 🟥 **Élections présidentielles 2017 : le comparateur de programmes**, in partnership with *Le Figaro*, February-May 2017
- 🟦 **Les Européens : combien de divisions ?**, Note de Benchmarking, May 2017
- 🟧 **Refonder la politique de lutte contre la pauvreté**, rapport, April 2017
- 🟧 **Refonder la politique du handicap**, Note, March 2017
- 🟪 **Propositions pour refonder la politique migratoire française**, Jean-Thomas Lesueur, January 2017

Cyrille Dalmont is a Research Fellow at the Thomas More Institute. Holder of a Master in public law, former parliamentary assistant and former mission officer in a large French metropolis, he has now joined the private sector. At the Thomas More Institute, he analyses the social and political changes brought about by the emergence and development of Artificial Intelligence, Robotics and home Automation. It focuses in particular on regulatory issues and ethical issues related to their deployment in the public space and in the private lives of individuals and families. In particular, he is the author of the note *Intelligence artificielle et santé : 10 propositions anti-brouillard pour régulation éclairée* (in French, november 2018, more).

Paris
8, rue Monsigny, F-75 002 Paris
Tel : +33 (0)1 49 49 03 30

Brussels
Avenue Walkiers, 45, B-1160 Bruxelles
Tel : +32 (0)2 374 23 13

www.institut-thomas-more.org
info@institut-thomas-more.org

This document is owned by the Institut Thomas More asbl. The words and opinions expressed in this document only involve the responsibility of the author. Its reproduction, partial or total, is allowed on two conditions: to obtain the formal approval of the Thomas More Institute asbl and to make its provenance clear.