Digital technology during times of crisis

Poullet, Yves

Published in:
Law, surveillance and the humanities

Publication date:
2022

Document Version
Publisher's PDF, also known as Version of record

4

Digital Technology during Times of Crisis: Risks to Society and Fundamental Rights

Yves Poullet

I. Introduction

In the introduction to his 2012 work entitled *Crisis(es) and Law*, Jacques Larrieu defines crisis as a 'disorder' causing 'the disintegration of the norms that usually regulate society'.[1] This disorder can in turn give rise to a 'law of circumstance' which is to be considered dangerous but which can also be a source of progress as it invites specialists to conceive of a 'new legal system that draws lessons from the crisis'.

Digital technology is an important part of the response to crises, and its use in the service of the struggle against them plays a major role in the disruption of the functioning of our legal system, in an undoubtedly more insidious than conscious manner. Of course, the upheaval that digital technology causes in the legal system is not specific to times of crisis. What is unmistakably specific to such times, however, is how this tool is used during periods of unrest, and how its legitimisation makes the law forget its own foundations. If digital technology is sometimes the object of specific legislation, it is above all because it constitutes the very condition of the effectiveness of the regulatory measures taken by our governments, an effectiveness that runs the risk of negating certain freedoms.

Should the use of such effective tools therefore be abandoned? The answer is 'no', but it is undoubtedly necessary to limit their implementation with a legal framework adapted to these exceptional times. The goal of this reflection, therefore, is to guide the development of such a framework, in the same way as Gligorijević attempts to do in Chapter 5 of this collection.

[1] Larrieu, 'Avant-propos', 9–12. In the same vein can be added the reflections of the authors of a thematic edition of the magazine *Droit et Société* devoted to the COVID crisis (Abitboul et al., 'Ce que 2020 a fait au droit'), who conclude that if 'the crisis denies the law', it nonetheless does not deny 'reflection that is specific to it'.

The present reflection covers two areas of application. The first concerns the lessons learned during the struggle against the pandemic.[2] The measures implemented today against COVID-19, or those envisaged for use against future pandemics, all have a restrictive impact on freedoms that goes beyond their simple limitation and sometimes represents a challenge to their very essence. Digital technology is omnipresent in these measures: the use of artificial intelligence in the search for new tools (vaccines and others) and in the analysis of the causes of the pandemic, its spread, its prevention and its impacts;[3] the creation of databases, whether it be of infected persons, the vaccinated, or of caregivers; the monitoring of people, for example through the use of systems put in place in our mobile phones with the goal of detecting the presence of contaminated people in one's entourage; the use of drones to monitor compliance with travel restrictions, and so on.[4] The biopolitical foundations of such policies are investigated by Sabot in Chapter 2 of this collection.

The second area of application focuses on the use of digital technology in the fight against crime in one area in particular: the use by police or intelligence services of data kept by communication service providers.[5] Digital evidence is now a major tool used in solving a growing number of crimes. Examples of this can be found in Grabosky and Urbas's chapter on application to online child exploitation,[6] as well as in the French Code of Criminal Procedure, which has been revised several times, and allows for

> the installation of a technical device whose purpose is, without the consent of the interested parties, to access computer data in any place, to record, store and to transfer it, whether it is stored in a computer system, displayed on a

[2] In this regard, see the following studies: Poullet, 'Pandémie, numérique et droits de l'homme', 246–63; Parsa and Poullet, 'Les droits fondamentaux à l'épreuve du confinement et du déconfinement', 137–203; Poullet, 'COVID et libertés'.

[3] In this regard, see the OECD's response to Coronavirus on 23 April 2020, 'Using artificial intelligence to help combat COVID-19', available at https://www.oecd.org/coronavirus/policy-responses/using-artificial-intelligence-to-help-combat-covid-19-ae4c5c21/.

[4] To take just one example from Belgium: on 12 January 2021, a simple decision of the Minister of the Interior modified the previous ministerial decision of 28 October 2020, which organises emergency measures to limit the spread of the COVID-19 coronavirus. The modification intended to give the National Office of Social Security the power to use datamining and AI across various administrative databases, for the purpose of profiling, monitoring and surveillance of the Belgian population.

[5] Today, only traditional service providers are targeted, but we know that tomorrow, the European Union, in the context of the revision of the ePrivacy Directive (2002/58/EC, 12 July 2002), intends to extend data retention obligations to any communication and information platform, and therefore to new services on the Internet, such as Voice over Internet Protocol (VoIP), instant messaging, messages exchanged through social networks such as Twitter and Facebook, and e-mail, instead of traditional communication services.

[6] See Grabosky and Urbas, Chapter 7 of this collection.

> screen for the user of an automated data processing system, or entered by typing out characters or received and transmitted by remote devices.[7]

Finally, the use of machine learning systems (artificial intelligence) also represents an opportunity for law enforcement.[8] Returning to our primary interest in this matter, the legal possibility is acknowledged, under Article 15 of the ePrivacy Directive,[9] for Member States to oblige communication providers to retain communication data (but not its content) and to allow police and judicial authorities as well as intelligence services to access such data. A recent decision of the Court of Justice of the European Union (CJEU) concerns the conditions of this access.[10] According to the Court, only a strictly defined state of emergency can justify the obligation of communication providers to preserve data beyond the simple limitations which, in normal circumstances, are provided by Article 52 of the Charter of Fundamental Rights of the European Union (EU Charter).

Whether it concerns the pandemic, tracking down criminal offenders or terrorist operatives, or the struggle against global warming or natural disasters, the use of the resources of digital technology and the development of ever more powerful applications of such resources is clearly a strong temptation for our leaders. The Commission on Information Technology and Liberties[11] refers to

[7] The French Code of Criminal Procedure, through the Act of 14 March 2011 on the orientation and programming for the performance of internal security, already included this possibility of access to digital evidence (L. 2014-1353, 13 November 2014, JORF, 14 November). The law of 13 November, whose tendency was to strengthen the provisions relating to the fight against terrorism singularly expanded this recourse and a law of 3 June 2016 (L. 2016-731, 3 June 2016, JO 4 June) further extended these possibilities of real-time and remote access to all flagrante or preliminary investigations for cases of crime and organised delinquency upon authorisation of the judge of liberties and detention and upon request of the Public Prosecutor. A 2019 decree (2019-1602 published in the JO of 31 December 2019) specifies the contours of this capturing of digital evidence.

[8] In the face of increasingly numerous data collected in an increasingly ubiquitous manner, the processing capacities of computers make it possible to facilitate both the tasks of prevention and the detection of offences and their authors. For example: detecting racist messages on the Internet; using emotional analysis systems to analyse the reactions of suspects or, by means of facial recognition, identifying a criminal or a person suspected of terrorism in a crowd; using the cross-referencing of multiple socio-economic data, including consumption, mobility and expenditure, to track down a criminal or to predict how dangerous a person may be; calculating how dangerous a convicted person may be in the future (see *State v Loomis* (2016) WI 68, 371 Wis. 2d 235, 881 N.W.2d 749).

[9] 2002/58/EC, 12 July 2002.

[10] *Privacy International and others* (C-623/17, C-511/18, C-512/18 and C-520/18) (CJEU, 6 October 2020).

[11] CITL Ruling, 'Ruling No. 2020-046, 24 April 2020 on a proposed mobile application called "Stop-Covid"', available at https://www.cnil.fr/fr/publication-de-lavis-de-la-cnil-sur-le-projet-dapplication-mobile-stopcovid.

this as 'technological solutionism',[12] defined as the convenient recourse to the tool of technology as a response to the challenges posed by emergency situations, with the belief that it will solve the problem.

Furthermore, it is not surprising that these two areas are being brought together. Could it not be argued that the same technologies of surveillance and control are at work in both cases,[13] and that the privilege granted to the use of such technologies could be explained by a similar logic? That is to say, in light of the state of emergency and the seriousness of the situation, such technologies provide an unparalleled efficiency in the service of the given priority, whether it be regarding individual liberties and the right to health on the one hand, or the right to public security on the other. Indeed, the trade-off is often set in terms of liberty versus security, but it need not be so, as Gligorijević explains in Chapter 5 of this collection.

The 'Pandemic' law, recently adopted by the Belgian Parliament, establishes the procedure that must be put in place in order to declare such a state of emergency. In addition, Article 15 of the Council of Europe's Convention on Human Rights (ECHR) provides a strict overarching framework for this state of emergency.

The potential of digital technology fully justifies the anxiety of judges, data protection authorities and civil liberties associations in the face of what tomorrow may be a commonplace tool in the hands of governments or, even worse, of certain companies acting in the service of private interests or at the very least in a vaguely defined notion of the 'public good'. This is the main theme throughout the following reflection, as well as elsewhere in the volume. Indeed, to reflect the tandem between surveillance and 'public good', Brunon-Ernst, in Chapter 6 of this collection, describes the concept of bien(sur)veillance coined by Cynthia Fleury.

This discussion therefore begins with the examination of the CJEU 2020 judgment in *Privacy International and others* on access to communications data by law enforcement authorities. The second point of discussion studies Article 15 of the ECHR, the application of which was recommended to the Member States during their fight against the pandemic, and then compares

[12] At the 2008 South by Southwest festival, Facebook founder Mark Zuckerberg said, 'As the world faces many major issues, what we are trying to build as a company is an infrastructure on which to unravel some of them.' Along the same lines, Eric Schmidt, executive chairman of Google, announced at a 2012 conference, 'If we get it right, I think we can fix all the world's problems.' Laugee, 'Solutionisme'.

[13] On this point, refer to the examples given by Calay, 'L'empire des logiciels', 18; Tesquet, *État d'urgence technologique*, 48–52.

the Belgian law voted on 15 July with the requirements of this article. The third point broadens the discussion, relying on the importance of implementing an even more radical limitation of the use of digital technology outside of this state of emergency. The conclusions drawn here call on our legislators to act in order to ensure, in the name of the rule of law, a collective and democratic control of the development of digital technology in the service of freedom, without neglecting the common good.

II. The CJEU's 2020 Judgment on the Widespread Retention of Communications Data

The data retention obligation imposed on Internet service providers and content hosts to retain the traffic, location and civil identity data of all their users in a widespread and undifferentiated manner, for a period of one year, is based on the permissive provisions of Article 15(1) of the ePrivacy Directive. Beyond this precise legal reference, should this not also be considered as an interference justified by the right to security guaranteed in Article 6 of the EU Charter and by the requirements of national security, for which the responsibility lies solely with the Member States by virtue of Article 4 of the Treaty on the European Union (Maastricht Treaty)? The petitioning associations and companies contested the absence of measures governing the implementation of this obligation and, consequently, the right of the police and intelligence services to collect and process the data thus stored by the providers.

Concerning the dispute, the CJEU ruled as follows:

> in situations where a Member State is facing a serious threat to national security that proves to be genuine and present or foreseeable, that Member State may derogate from the obligation to ensure the confidentiality of data relating to electronic communications by requiring, by way of legislative measures, the general and indiscriminate retention of that data for a period that is limited in time to what is strictly necessary, but which may be extended if the threat persists.[14]

The Court added that the injunction must be proportionate, implemented for a time period limited to what is strictly necessary, and is to be subject to effective monitoring controls, either by a court or by an independent administrative body. The latter are to be tasked with verifying the implementation

[14] *Privacy International and others* (C-623/17, C-511/18, C-512/18 and C-520/18) (CJEU, 6 October 2020).

of the conditions and guarantees provided by the Court. If these are met, the automated analysis of data must be permitted, particularly that relating to the traffic and location of all users of electronic communications.

This judgment has been interpreted differently by the French Conseil d'État (Council of State) and the Belgian Constitutional Court. In France, the Council of State leaves the interpretation of the emergency situation – which the CJEU cites as a reasonable justification for the widespread retention of communication data – to the discretion of the national executive powers, considering that in light of recent events there exists a threat of terrorism:

> France is faced with a threat to its national security, assessed with regard to all the fundamental interests of the Nation listed in Article L. 811-3 of the Interior Security Code, which, by its intensity, is considered serious and real . . . Moreover, France is particularly exposed to the risk of espionage and foreign interference, notably because of its military capabilities and commitments as well as its technological and economic potential.[15]

The Belgian Constitutional Court adheres to the strict interpretation of the Court.[16] It notes, following European jurisprudence, that the widespread retention measure poses a far greater threat to privacy and freedom of expression than any other measure of limited access to data concerning particular citizens. It emphasises that data retention should be used only in response to serious threats to national security such as terrorism and not to public safety objectives such as serious crime.[17] The Belgian Court therefore considered that,

> In order to satisfy the requirement of proportionality, the legislation must lay down clear and precise rules governing the scope and application of the

[15] Conseil d'État [Council of State; the highest court in the administrative legal system], *French Data network et al.*, 21 April 2021, n 393099, 394922, 397844, 397851, 424717, 424718. As a justification of the generalised obligation for data retention, the Council of State added that 'France is also facing serious threats to public peace, linked to an increase in the activity of radical and extremist groups. These threats are of such a nature as to justify the obligation of the generalised and undifferentiated retention of connection data' and, in an even more critical manner towards the European judge, 'the obligation for the judge to set aside the provisions of national law imposing a generalised and undifferentiated retention of connection data for purposes other than safeguarding national security would deprive of effective guarantees the objectives of constitutional value of preventing breaches of public order, in particular breaches of the security of persons and property, and of tracking down the authors of criminal offences'.

[16] Judgment 57/2021, *OBFG et al.*, 21 April 2021, n 6590, 6597, 6599 and 6601.

[17] As held by the CJEU in *Privacy International and others* (C-623/17, C-511/18, C-512/18 and C-520/18) (CJEU, 6 October 2020), 136.

> measure in question and imposing minimum safeguards, so that the persons whose personal data is affected have sufficient guarantees that data will be effectively protected against the risk of abuse. That legislation must be legally binding under domestic law and, in particular, must indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary.[18]

On this basis, the Court considered that a decision ordering electronic communications service providers to carry out such data retention must be subject to effective review either by a court or by an independent administrative body, such as the CJEU has required.[19]

When assessing the risks to our freedoms that are involved, what is undoubtedly striking in both the European and Belgian decisions is the emphasis on accounting for the potential of the use of digital technology in the implementation of regulatory provisions. Thanks to powerful AI systems, these new risks revolve in particular around the profiling of individuals, the automated detection of sensitive data, and geolocation, as well as the illicit use of communication data. It is in this light that the annulment of the national provisions authorising the widespread conservation of communication data and the prohibition in principle of any instrument of mass surveillance are justified.[20]

Recent developments in digital technology have unmistakably permitted a far greater effectiveness within criminal law than the traditional tools of police and judicial investigation, and even of intelligence services, and as such, the infringements on our individual and collective liberties must have appropriate limits placed upon them. Therefore, as the Belgian Constitutional Court notes,

> The judgment of the Court of Justice of 6 October 2020 imposes a change of perspective with respect to the choice that the legislator has made: the obligation to retain data relating to electronic communications must be the exception, not the rule. Regulations providing for such an obligation must also be subject to clear and precise rules concerning the scope and application of the measure in question as well as imposing minimum requirements. This

[18] Judgment 57/2021, *OBFG et al.*, 21 April 2021, 132.

[19] Ibid., 139.

[20] In the same vein, with regard to the questioning of the 'Privacy Shields' agreements entered into by the European Commission in the context of trans-border data flows to the United States for not meeting the requirements of the GDPR, see the *Schrems II* decision (*Facebook Ireland v Schrems* (C-311/18, 16 July 2020)).

> regulation must ensure that interference is limited to what is strictly necessary and that it 'must always meet objective criteria that establish a connection between the data to be retained and the objective pursued'.[21]

Therefore, it would clearly be useful to elaborate on how this state of emergency is defined and enacted, based on the lessons drawn from Article 15 of the ECHR. The latter provides a rudimentary framework for these systems of emergency measures and was recently invoked in the context of the pandemic.

III. From the Fight against the Pandemic to Article 15 of the European Convention on Human Rights

1. The Struggle against the Pandemic and Restrictions on Our Freedoms

There can be no doubt that what is misrepresented as the 'war' on COVID-19[22] can be used to justify certain decisions in the context of a technological 'emergency' that is itself justified by the 'health emergency' the world currently faces. Today, it is time to measure the extent of the damage inflicted upon our freedoms. The right to education, to assemble in public, to worship, to free expression and free enterprise, to mobility and to privacy are all either limited or suspended or, in any event, sacrificed so as to safeguard public health at all costs. Garapon writes, 'the measures adopted in the emergency resemble an immense medical prescription extended to the entire population, more than to the law',[23] whose only guide is statistics such as those concerning the lack of hospital beds, those of the deaths that nobody likes to count, as well as those concerning vaccinations that some governments have made compulsory for at least some professions.

At the same time, what are even more worrying are the societal risks that this torrent of emergency measures conceals, such as the gradual disappearance of the rule of law and of democratic rights. The European Parliament Resolution of 13 November 2020 on the pandemic and the rule of law echoes this concern:

> these measures have an impact on democracy, the rule of law and fundamental rights as they affect the exercise of individual rights and freedoms, such as freedom of movement, freedom of assembly and of association, freedom

[21] Judgment 57/2021, *OBFG et al.*, 21 April 2021, 132, 133.

[22] In particular, see President Macron's statements on 16 March 2020, where he announced to the French public that containment measures were necessary to curb the spread of COVID-19, declaring in a serious tone that 'We are at war', available at https://www.lemonde.fr/politique/article/2020/03/17/nous-sommes-en-guerre-face-au-coronavirus-emmanuel-macron-sonne-la-mobilisation generale_6033338_823448.html.

[23] Garapon, 'Un moment d'exception'.

> of expression and information, freedom of religion, the right to family life, the right of asylum, the principle of equality and non-discrimination, the right to privacy and data protection, the right to education and the right to work.[24]

In support of the regulatory measures taken, we note the multiplication of data processing and databases created throughout the COVID-19 pandemic, which have been used to trace the disease and therefore the individuals carrying or likely to carry the virus. It is on these measures that the debates inciting the strongest resistance have been focused, especially those led by the data protection authorities, the guarantors of our data protection.[25] The European Parliament Resolution summarises the importance of digital technology in the fight against COVID-19 and the related risks:

> measures to combat the pandemic that restrict the right to privacy and data protection should always be necessary, proportionate and temporary in nature, with a solid legal basis; new technologies have played an important part in the fight against the pandemic, but at the same time bring significant new challenges and have raised concerns; the governments of some Member States have resorted to extraordinary surveillance of their citizens through the use of drones,[26] police surveillance cars with cameras, tracking by means of location data from telecommunications providers, police and military

[24] European Parliament resolution of 13 November 2020 on the impact of COVID-19 measures on democracy, the rule of law and fundamental rights (2020/2790(RSP)), 13 November 2020, P9 TA(2020)0307. The resolution builds on the Commission's 30 September 2020 Communication 'Rule of Law Report 2020 – The State of the Rule of Law in the European Union' (COM(2020)0580) and the accompanying twenty-seven chapters organised by country on the rule of law in the Member States (SWD(2020)0300-0326), which address the impact of COVID-19-related measures taken by Member States on democracy, the rule of law and fundamental rights.

[25] The reader will find a complete and impressive list of opinions, statements, etc. of Data Protection Authorities and other national and international data protection bodies at https://globalprivacyassembly.org/covid19/. See also the very extensive site of the LSTS research team of the VUB (Brussels): 'Data Protection Law and the COVID 19 Outbreak', available at https://lsts.research.vub.be/en/data-protection-law-and-the-covid-19-outbreak.

[26] On the use of drones for pandemic control purposes, it should be noted that, in a summary order issued on 18 May 2020, the Council of State ordered 'the State to cease, without delay, carrying out surveillance measures by drone in Paris, out of respect for the health security rules applicable to the decontamination period'. It ruled that these drones were used outside the framework provided by the 'Informatique et Libertés' Act and were a 'serious and manifestly illegal infringement of the right to privacy'. French Council of State, Juge des référés, 18/05/2020, 440442, available at https://www.legifrance.gouv.fr/ceta/id/CETATEXT000041897158/.

> patrols, monitoring of mandatory quarantines via house calls by the police or mandatory reporting via an app; some Member States have introduced contact tracing apps, even though there is no consensus about their effectiveness and the most privacy-friendly, decentralised system is not always used; in some Member States the reopening of public spaces has been accompanied by the collection of data through mandatory temperature checks and questionnaires and the obligation to share contact details, sometimes without due regard for the obligations that stem from the General Data Protection Regulation.[27]

Are all these measures simple limitations of our freedom or are they more radical suspensions of it? Do they even perhaps constitute an attack on its very essence, which Article 52 of the EU Charter prohibits? Article 52 does in fact sanction the possibility of limitations to the fundamental rights set out in the EU Charter, but it also imposes guidelines on these limitations:

> Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.[28]

Where then can the basis for the suspension of fundamental rights and freedoms be found, at a time when digital technology is granting the regulatory provisions, sometimes even simply of the local municipal police, a much more significant impact on our freedoms? Is freedom of assembly, including that of trade unions, still possible when drones monitor gatherings and have a dissuasive effect on the population? Vaccination, even if it is presented as a moral 'obligation', is imposed on citizens who know they are being 'tracked' by a widely accessible database, even when going to a pharmacy to obtain medicine not related to COVID-19, or when seeking to sit down at a restaurant or participate in a so-called mass event.[29]

The limitation of fundamental rights should therefore not be confused with the derogation or suspension of these rights. Derogations 'suspend' fundamental freedoms for a given time period, in given exceptional circumstances,

[27] 2020/2790(RSP), 13 November 2020, P9 TA(2020)0307.

[28] Article 52 of the EU Charter.

[29] It is beyond the scope of this chapter to discuss the questions raised by compulsory vaccination. On this point, see the recent reflections of Bioy, 'Vers la vaccination obligatoire contre la Covid?'

such as a state of health emergency, terrorist attacks or a state of war.[30] Article 15 of the ECHR states that they can only be justified in exceptional circumstances. It follows then that states are no longer obliged to meet the conditions of justification imposed for restrictions on fundamental rights when they find themselves in the specific circumstances and conditions of derogation laid out in Article 15.[31] In view of the extent of the restrictions imposed by the laws, ordinances and even decrees of all kinds issued by the public authority, the latter should have referred to Article 15 of the ECHR in order to justify them. Article 52 of the EU Charter does not prohibit this recourse,[32] but imposes it in the case where derogations or suspensions of freedoms are envisaged. Article 15 of the ECHR establishes a system of sanctions which, while authorising significant restrictions on freedoms in the name of well-specified higher public interests, are nonetheless delineated in order to maintain the rule of law, which is precisely what is endangered in such circumstances.[33] For this reason, both French and Belgian constitutional writers have justifiably regretted that the governments of these two countries did not implement this article when they took measures to combat the pandemic.[34]

[30] Colella, 'Chapter 1: L'acception des notions de restriction, limitation et dérogation', 126.

[31] De Schutter, *International Human Rights Law*, 585n. See also the strong statement of the Secretary General of the Council of Europe, Pejčinović Burić, on 7 April 2020 at the moment of publication of the 'toolkit' for all European governments on respect for human rights, democracy and the rule of law during the COVID-19 crisis, available at https://rm.coe.int/sg-inf-2020-11-respecting-democracy-rule-of-law-and-human-rights-in-th/16809e1f40.

[32] As an authoritative interpreter of the EU Charter, the FRA (European Agency for Fundamental Rights) notes: 'The Charter does not affect the possibilities of Member States to avail themselves of Article 15 of the ECHR, allowing derogations from ECHR rights in the event of war or of other public dangers threatening the life of the nation, when they take action in the areas of national defence in the event of war and of the maintenance of law and order, in accordance with their responsibilities recognised in Article 4(1) of the Treaty on European Union and in Articles 72 and 347 of the Treaty on the Functioning of the European Union.'

[33] On the totalitarian shift facilitated by so-called states of emergency, see the work of Basilien-Gainche, *État de droit et états d'exception*, 125: 'The rule of law refers to the law and the norm, to normality and the ordinary: it is a political goal of the State, a horizon of perfection nourished by the separation of powers and the guarantee of rights. As for states of emergency, they evoke disorder and the extraordinary, the concentration of powers and the restriction of rights.'

[34] Thus, in France, Sudre's post on the *Club des juristes* website 'La mise en quarantaine de la Convention européenne des droits de l'Homme', 20 April 2020 as well as that of Costa, 'Le recours à l'article 15 de la Convention européenne des droits de l'homme'; in Belgium, Ost, 'Nécessité fait loi?', 26–7; Verdussen, 'Droits humains et crise sanitaire'.

2. The Legal Regime of Article 15 of the ECHR

In contrast to France and Belgium, no fewer than ten signatory countries of the ECHR wished to enact Article 15 in the context of the pandemic.[35] Article 15 authorises derogations of rights and freedoms in a state of emergency, subject to prior notification of the Secretary General of the Council of Europe:

> In time of war or other public emergency threatening the life of the nation any High Contracting Party may take measures derogating from its obligations under this Convention to the extent strictly required by the exigencies of the situation, provided that such measures are not inconsistent with its other obligations under international law.[36]

This provision of the ECHR introduces the theory of the state of necessity to justify the exceptions,[37] while imposing strict conditions on Member States in order to control the exercise of such exceptions. While it can clearly be invoked in relation to situations of public order disturbance such as war or terrorist threats, can Article 15 be applied to situations such as a pandemic? According to the jurisprudence of the ECHR,[38] the interpretation of the words 'other public emergency threatening the life of the nation' allows this to be extended to cases of pandemic and has been implicitly approved by the Council of Europe by the very fact of its publication in 2020 of the 'toolkit' for the use of Article 15, on the subject of the pandemic.

[35] It is interesting to note that while both France and Belgium have not (yet) made use of this exception during the pandemic, other countries have started the procedures since mid-March 2020. See Venice Commission, 'Interim Report on the measures taken in the EU member States as a result of the Covid-19 crisis and their impact on democracy, the Rule of Law and Fundamental Rights', 8–9 October 2020 (CDL-AD(2020)018-e), para. 35, available at https://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2020)018-e. See also Council of Europe (Press Unit), 'Fact Sheet: Derogation in Time of Emergency', 2, available at https://www.echr.coe.int/documents/fs_derogation_eng.pdf; and, for detailed information on the context in which these derogations were formulated, the web page of the Council of Europe Treaty Office.

[36] Regarding this Article invoked by some member countries of the Council of Europe on occasions other than the pandemic and often for reasons of combating terrorism, see, in particular, Renucci, *Droit européen des droits de l'homme*, 33–5.

[37] It should also be noted that Article 17 of the ECHR sets out in a more general way the principle of prohibition of abuse, in particular by public authorities.

[38] In this regard, we cite the *Lawless v Ireland* judgment (1/7/61), in which the court held that the terms of Article 15 refer to 'a situation of crisis or exceptional and imminent danger which affects the entire population and constitutes a threat to the organised life of the community making up the State', and the *Ireland v UK* judgment of 18 January 1978 (Series A No. 25, para. 207), which leaves States a wide margin of manoeuvre in interpreting the concepts of Article 15.

Among the conditions set for the system of derogations from the ECHR, three material conditions can be distinguished:[39] first, the occurrence of serious circumstances, of public dangers threatening the life of the nation; second, the absolute necessity of being able to derogate from individual liberties; and third, the respect of other obligations arising from international law. In addition to these substantive conditions, a formal condition must be added, namely notification to the Secretary General of the Council of Europe of both the measures taken and the reasons for them, in accordance with the third paragraph of Article 15. States must also inform the Secretary General of the Council of Europe of the date on which '*the provisions of the Convention are again fully implemented*'. Finally, the Secretary General, at the moment of the publication of the 'toolkit' on the use of Article 15 during the Coronavirus pandemic on 7 April 2020, recalled that, according to the jurisprudence of the Council of Europe, derogations must be proportionate and framed, if possible, by legislative measures:

> At the same time, any derogation must have a clear basis in domestic law in order to protect against arbitrariness and must be strictly necessary to fighting against the public emergency. States must bear in mind that any measures taken should seek to protect the democratic order from the threats to it, and every effort should be made to safeguard the values of a democratic society, such as pluralism, tolerance and broadmindedness. While derogations have been accepted by the Court to justify some exceptions to the Convention standards, they can never justify any action that goes against the paramount Convention requirements of lawfulness and proportionality.[40]

Thus, the state of necessity does not take precedence over the legality and proportionality of the proposed restrictive measures.[41]

[39] 'Guide on Article 15 of the European Convention on Human Rights: Derogation in Time of Emergency', updated 30 April 2021, available at https://www.echr.coe.int/documents/Guide_Art_15_ENG.pdf.

[40] 'Toolkit' for all European governments on respect for human rights, democracy and the rule of law during the COVID-19 crisis, available at https://rm.coe.int/sg-inf-2020-11-respecting-democracy-rule-of-law-and-human-rights-in-th/16809e1f40.

[41] With regard to this Article, see the comments of the Council of Europe advisory body European Commission for Democracy through Law (Venice Commission) in its report 'Interim Report on the measures taken in the EU member States as a result of the Covid-19 crisis and their impact on democracy, the Rule of Law and Fundamental Rights', 8–9 October 2020 (CDL-AD(2020)018-e), available at https://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2020)018-e.

There are therefore three arguments in favour of following the procedure and the conditions of Article 15 of the ECHR:

1. Openness: Article 15 requires transparency and legitimacy of both the measures and the reasons.
2. Verification by peer review and the Council of Europe itself: the communication to the Council of Europe of the measures taken or envisaged allows a *benchmarking* of the decisions in relation to those of other states and is done so under the vigilant eye of the organs of the Council of Europe, which, on this comparative basis, can question the states on the proportionality of the measures.
3. Need for democratic parliamentary deliberation, insofar as the Council of Europe will be bound by a text that has received the assent of the legislature after a comprehensive legislative process has been carried out.[42]

Other advantages can also be added, including the obligation to set a duration for the emergency measures that does not exceed the length of the health emergency, any extension to which must be justified and duly investigated by the Council of Europe; and the requirement to demonstrate that the measures taken are necessary, adequate and strictly proportionate. Finally, the distinction between limitation and restriction or suspension of freedoms invites reflection on the notion of the 'essence' of freedoms and rights introduced by Article 52 of the EU Charter. This notion implies that we have consideration of not only the content of the prescriptions but also the measures of effectiveness of such prescriptions, particularly those consisting in the use of digital technology. In any case, it is an invitation to distinguish, as did the French bill that has now been abandoned,[43] between the measures taken to

[42] 'A declaration of a state of emergency may be issued by parliament or by the executive. Ideally, it should be declared by parliament or by the executive subject followed by immediate approval by parliament. In urgent cases, immediate entry into force could be allowed – however the declaration should be immediately submitted to parliament, which can confirm or repeal it.' Venice Commission, 'Interim Report on the measures taken in the EU member States as a result of the Covid-19 crisis and their impact on democracy, the Rule of Law and Fundamental Rights', 8–9 October 2020 (CDL-AD(2020)018-e), para. 34, available at https://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2020)018-e. The Venice Commission is a body created by the Council of Europe on the situation of the rule of law in different countries.

[43] It is known that the project was finally withdrawn by the French government following criticism from the Council of State and the senators, insofar as the planned measures did not allow for sufficient control by the Parliament. See https://www.publicsenat.fr/article/parlementaire/urgences-sanitaires-le-gouvernement-retire-un-projet-de-loi-controverse-186392.

curb the pandemic – those justified by the crisis situation 'in case of serious health threats and situations'[44] – from those required by the state of health emergency, that is to say, 'in case of a health disaster endangering, by its nature and gravity, the health of the population'.[45] It is solely in this second case that the state of emergency which justifies restrictions to freedoms and not simple limitations should be applied in accordance with the prescriptions of Article 15 of the ECHR. It is certain, therefore, that in the name of the state of emergency, the government adopted measures that went beyond the simple limitation of freedoms and in reality were a true suspension of such freedoms, which it could only justify by recourse to Article 15 of the ECHR.

These 'essential' restrictions and the consequent suspension of rights and freedoms must be subject to an analysis of proportionality and to an even more careful analysis of their motivations beyond mere simple limitations, insofar as they must be of an exceptional nature for a situation that is universally judged to endanger the safety of the nation.[46] Here, we are faced

[44] French Council of State, 'Opinion on a draft law instituting a permanent health emergency management system', 21 December 2020: 'The state of health crisis will be declared by simple decree "in case of threat or serious health situation". It will be extended, every two months. During this system, the Prime Minister and the Minister of Health will be able to take or authorise the prefects to take measures of an essentially sanitary nature (individual decisions to place or maintain patients in quarantine or isolation, measures to make health products available to patients, necessary measures for the organisation and operation of the health care system, temporary price control measures and requisitions). This system of measures could intervene in particular in the event of a global, national or local epidemic, a nuclear or industrial accident, an earthquake, an attack [. . .].'

[45] Ibid.: 'The state of health emergency will be declared, as it is the case today, for one month "in case of a health disaster endangering, by its nature and gravity, the health of the population". In addition to the measures provided for in the state of health crisis, the Prime Minister may also take measures other than health measures (administrative police measures) as he did for the COVID-19 epidemic: regulation of the movement of people and the opening of establishments available to the public, prohibition of leaving the home, limitation of gatherings in public places, and any other measure restricting the freedom of enterprise. The Prime Minister may also make access to certain places and the exercise of certain activities conditional on screening or preventive or curative treatment (as is currently the case, for example, for compulsory tests before traveling by plane).'

[46] In this respect, see the clear statement of the French Council of State: 'The necessary, proportionate and appropriate character of such a measure cannot be considered as excluded in the perspective, which is that of the bill, of having perennial legal means of response to health disasters whose gravity cannot be anticipated. The measure can make it possible, by itself, to reconcile, in the event of particularly serious epidemics, the effective exercise of certain freedoms with the objective of protecting public health, instead of more generalised or more restrictive measures of the freedoms in question, in particular the freedom of movement and the freedom of enterprise.' Ibid.

with the restrictive interpretation of the state of emergency developed by the CJEU in relation to the obligation of the widespread retention of communication data, for which the application of Article 15 ECHR should have also been envisaged. In the case of the data retention obligation, the right to security is used to justify restrictions on our freedoms and, in the name of efficiency, democratic processes are brought into question; in the second case, it is the right to health that justifies this same movement.

3. The So-Called Belgian 'Pandemic' Law

Is Belgium's response in the form of the so-called 'Pandemic' law adequate?[47] There is no doubt that the text voted on is problematic. To be sure, the law transforms the state of emergency in fact into a state of emergency in law, insofar as it is Parliament that declares said state of emergency.[48] Fortunately, the legal text confers great importance on what forms the starting point of the emergency measures even though the law, regrettably, does not contain any reference to the procedure of Article 15 ECHR. The state of emergency is declared by the King following a judgment issued by the Council of Ministers after consultation with experts and on the advice of the Minister of Public Health. This judgment, which comes into effect as soon as it is published, is subject to parliamentary discussion at short notice and must be confirmed by a law also adopted at short notice. The same procedure must be followed, and the same conditions apply, in the case of an extension.

The law is partial and is only targeted at the health emergency.[49] Beyond the provisions relating to the pandemic, however, should a general system of measures for the state of emergency not have been implemented, as the CJEU recommended when it opened the debate on the widespread retention of communication data? Secondly, the text seems to us to miss the main point, which is of maintaining the rule of law in the context of a state of emergency. Regarding this last point in particular, it insufficiently takes into account the 'technological' element, a consideration of which is essential to the maintenance of such a rule of law. These two points are developed below.

In the context of a state of emergency, it is surprising that the clearly central question of freedoms has not led to the questioning of what constitutes the very condition and guarantee of the latter, namely respect for the rule

[47] Law on administrative police measures during an epidemic emergency, 14 August 2021, (Mb., 20 August 2021).

[48] We cannot go into the details of all the arguments submitted in our report to the Parliament March 2021, at the request of its president. Some extracts are published in Poullet, 'La société et les droits fondamentaux aux risques du numérique en temps de crise', 185–95.

[49] A notion which is too broadly defined by the 'Pandemic' law (see article 3 2°).

of law. The European Parliament Resolution of 13 November 2020 on the impact of COVID-19 measures on democracy, the rule of law and fundamental rights, which has already been discussed here, highlights this danger.[50]

This European Parliament affirmation of the necessary respect for the rule of law leads in particular to its demand that the legislature and the judiciary be able to play their role in support of freedom:[51]

> whereas government-led emergency measures that respect the rule of law, fundamental rights and democratic accountability are needed to combat the pandemic and should be the cornerstone of all efforts to control the spread of COVID-19; whereas emergency powers require additional scrutiny to ensure that they are not used as a pretext for changing the balance of powers more permanently; whereas measures taken by governments should be necessary, proportional and temporary; whereas emergency powers carry a risk of abuse of power by the executive and of remaining in the national legal framework once the emergency is over, and consequently appropriate parliamentary and judicial oversight, both internal and external, and counterbalances have to be ensured to limit this risk.[52]

[50] The Resolution provides: 'whereas the functioning of democracies and the checks and balances to which they are subject are impacted when a health emergency situation causes shifts in the distribution of powers such as allowing the executive to acquire new powers to limit individual rights and to exercise competences usually reserved for the legislature and local authorities [. . .]. Such is the situation when the courts can no longer meet or are reluctant to rule in cases of emergency, and when the bodies responsible for controlling legality or constitutionality cannot rule insofar as the norms adopted by the executive are beyond their control. This is the case at a time when associations can no longer express themselves in the street and when even the media have difficulty welcoming the detractors of anti-COVID-19 measures, in the name of a broad conception of misinformation, far from the principle of the freedom of expression affirmed by the jurisprudence of the Council of Europe since the *Handyside* case: freedom of expression is applicable not only to 'information' or 'ideas' that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb the State or any sector of the population. Such are the demands of that pluralism, tolerance and broadmindedness without which there is no 'democratic society"'.' Quotations in the judgment are from *Handyside v The United Kingdom*, no. 5493/72, Judgment Strasbourg, 7 December 1976, 49.

[51] On the difficulty of the legislature to play its role in the crisis caused by COVID-19, see The Robert Schuman Foundation, 'The impact of the health crisis on the functioning of parliaments in Europe', available at https://www.robert-schuman.eu/en/doc/ouvrages/FRS_Parliament.pdf.

[52] In the same sense, see the article in *Le Soir* of 23 March 2021, which denounces the 'heist of the century on the private life of Belgians'. The article aims at 'blowing the whistle' by declaring that there is 'an unprecedented amount of incompetence, [. . .] of a system of state management that is beyond parliamentary control, beyond the reach of the Council of State or the citizen's right of appeal, and beyond the reach of a supervisory authority that is increasingly devoid of its substance'.

On this basis, the European Parliament makes a number of recommendations, in particular:

- to ensure that if legislative powers are transferred to the executive, any legal act emanating from the executive is subject to subsequent approval by parliament and ceases to have effect if not approved within a specified period, and to address the excessive use of fast-track and emergency legislation
- to examine how to more effectively safeguard the central role of parliaments in crisis and emergency situations, especially their role in monitoring and overseeing the situation at the national level.

In order for Parliament to play its role in overseeing the executive, Belgian law should have specified the procedure that Parliament should follow so as to assess the proportionality and necessity of measures proposed by the government, otherwise the legislature runs the risk of being nothing more than an endorsement chamber.

Our second point concerns the absence of any provision relating to the use of digital technology in the fight against COVID-19. Initially, the text included an article calling to mind the requirements laid out in the data protection legislation. For reasons of unclear wording and fear of a provision that would appear to circumvent the mandatory European provisions and their translation into Belgian law, the Data Protection Authority (DPA), together with others, had argued for this article to be withdrawn.[53]

We find this regrettable. First, as has already been mentioned, the administrative police measures, the use of which are regulated by the 'Pandemic' law, often involve as a condition of their efficacy the processing of personal data. It is therefore important to keep in mind the rules surrounding the creation of such databases. Second, while each administrative or police measure involves an apparently distinct implementation of data processing, it would have been useful if, on this occasion, Parliament would be entitled to request access to a global and unfragmented view of the processing thus created and the links between them. Third, it was a good opportunity to recall the principles of legality, minimisation and transparency in regards to the individual citizen,[54] principles that are at the heart of data protection legislation and that guarantee the respect of the rule of law. Fourth, certain obligations should have been imposed such as 'Privacy by design' or 'Privacy by default', for instance the obligation to carry out a 'Privacy Impact

[53] This is the notice 24/2021 of 2 March 2021 on the draft law on administrative police measures during a pandemic emergency.

[54] Transparency undoubtedly requires that all the elements provided for in Article 6.4 of the GDPR are to be included in the text for the creation of data processing to combat COVID-19.

Assessment' and to establish the modalities of its drafting (i.e. who participates in this assessment? Who evaluates the report? Is the report published? etc.).

Other points include the questions of medical confidentiality and, more broadly, of access to databases containing medical information which could have been the subject of a provision making reference to the prohibition in principle of access to persons not covered by medical confidentiality and which provided the procedure that, if necessary, should be followed to allow such access to persons not covered by confidentiality; as well as the question of the limited duration of the data processing created in the framework of the fight against COVID-19. Finally, the principle affirmed by the European Data Protection Board (EDPB) could have also been highlighted:

> The EDPB generally considers that data and technology used to help fight COVID-19 should be used to empower, rather than to control, stigmatise, or repress individuals. Furthermore, while data and technology can be important tools, they have intrinsic limitations and can merely leverage the effectiveness of other public health measures. The general principles of effectiveness, necessity, and proportionality must guide any measure adopted by Member States or EU institutions that involve processing of personal data to fight COVID-19.[55]

As such, the need to put technology at the service of citizens certainly is the message sent by data protection authorities.

Beyond data protection issues, should we not address the question of freedom of expression and the fight against the misinformation that the business models of our communication platforms only intensify through their algorithms which exploit machine learning technologies and the profiling of Internet users? Should we not also reflect on the social justice issues raised by the digital revolution? We know that illiteracy excludes certain portions of the population from any use of applications or information that require access to or even the handling of technology,[56] and that vaccination databases are also a tool for the exclusion from certain places of a subset of the population which, for good or bad reasons, refuses vaccination, the merits of which are not up to the authorities to discuss.

[55] 'Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak', adopted 21 April 2020, 3, available at https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf.

[56] In France, it is considered that almost a fifth of the population does not have access to or does not know how to use a smartphone. In addition, this portion of the population is largely made up of the elderly as well as the economically vulnerable, those most at risk. There is also the need to take into consideration foreign populations who are often ill-informed due to the language barrier.

The 'Pandemic' law does not validate the existence, however necessary, of the societal debates raised by the sometimes too rapid adoption of technological tools. This adoption should have been subject to a mandatory evaluation prior to the design of such information systems. Above all, the need for a comprehensive evaluation of such systems, often hastily built, during and at the end of periods of crisis, should be legally affirmed.[57]

IV. Digital Technology, the State of Emergency and the Rules of Lawlessness

Let us begin by recalling the importance of the principles of minimisation and proportionality: the state of emergency in itself never justifies the creation of any kind of processing procedure. As mentioned in the legal notice issued by the Chambre de connaissance (Knowledge Centre) of the DPA,[58] the following conditions must be met:[59] first, that the data processing effectively allows the accomplishment of the objective pursued. It is therefore necessary to demonstrate, on the basis of factual and objective elements, the effectiveness of the processing of personal data in achieving the stated aims. Second, that this processing of personal data is the least intrusive measure with regard to the right to privacy. This means that if it is possible to achieve the intended purpose by means of a measure that is judged less intrusive in reference to the right to privacy or the right to protection of personal data, the data processing originally envisaged cannot be carried out.[60] This requires detailing and being able to demonstrate, with factual and objective evidence, why other less intrusive measures are not sufficient to achieve the desired objective.[61]

[57] Calay, 'L'empire des logiciels', 39, speaks of a 'data coup d'état' during the pandemic.

[58] DPA Notice no. 124/2021 of 12 July 2021, already quoted above, no. 41 and 42, 13–14.

[59] This is what Van Drooghenbroek calls the triple test. See *La proportionnalité dans le droit de la Convention européenne des droits de l'homme*, 31–8. The requirement of this triple test is recalled in many of the DPA's opinions on anti-COVID-19 measures. See in particular DPA opinion no. 34/2020, 28 April 2020; Request for an opinion concerning a preliminary draft of Royal Judgment no. XXX implementing article 5, § 1, 1°, of the law of 27 March 2020 empowering the King to take measures against the spread of the coronavirus COVID-19 (II), in the context of the use of digital contact tracing applications as a preventive measure against the spread of the coronavirus COVID-19 among the population (CO-A-2020-041).

[60] It is in this sense that the preference given to the anonymisation of location data in the context of automatic tracing is conceivable.

[61] The EDPB's 'Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak', adopted 21 April 2020, no. 14 onwards, available at https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf. The application of these requirements has fuelled the discussion in many of our countries about the choice between the DP-3T

If the necessity of data processing is established, it must still be demonstrated that the processing is proportionate (in the strict sense) to the objective this one pursues, that is, it must be shown that there is a fair balance between the various interests involved and the rights and freedoms of the persons concerned.

The benefits of the data processing in question must therefore outweigh the disadvantages for the individuals concerned. Once again, evidence must be provided that this analysis was performed prior to the implementation of the processing. An enshrinement in law of these guidelines for interpreting the principles of proportionality and minimisation would have been useful in guiding those who design the various data processing operations to be implemented, which in turn must be subject to a procedure that respects the principle of legality.

The analysis conducted by some authors of 'Datacracy'[62] or 'algorithmic governmentality'[63] notes the disappearance of a public space for discussion and the increase in power of both private and public actors who collect and manage this data and invest it with meaning through the power of digital technology, and above all through ever greater recourse to artificial intelligence. This artificial intelligence, based on algorithms that work in a more or less opaque way, purportedly represents reality and deduces its future behaviour, putting its power in the hands of its users, who are first of all the companies that implement it, then secondly government departments, and finally private citizens, if necessary.

This conclusion is consistent with Banita's appraisal, in Chapter 10 of this collection, of predictive policing through algorithms in the present volume. What other choice is there but to blindly follow this truth that emerges from computers, even if it means legitimising it through laws that organise its production through the creation of databases and instruments for collecting the necessary information, all the while entrusting obscure organisations

protocol (Decentralised Privacy Preserving Proximity Tracing), chosen by many European countries (Belgium, Germany, Italy, Portugal, etc.), and the competing Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT) protocol, chosen by France for its TOUSANTICOVID application. Both use Bluetooth Low Energy technology to track our meetings with other users and record them on the system installed on our mobiles. The protocols differ in their reporting mechanism: PEPP-PT requires clients to upload contact logs to a central reporting server; with DP-3T, on the other hand, the central reporting server never has access to the contact logs and is not responsible for processing and informing the contact clients, and therefore it appears to offer a better guarantee of protection of our data and makes it part of the system design itself.

[62] Guyader et al., 'La Datacratie'; Cardon, 'Le pouvoir des algorithmes'; Blandin, 'La gouvernance du monde numérique', 50–6.

[63] Supiot, *La gouvernance par les nombres*; Rouvroy, '"Adopt AI, Think Later"'; Rouvroy and Berns, 'Le nouveau pouvoir statistique', 88–103; Rouvroy and Berns, 'Gouvernementalité algorithmique et perspectives d'émancipation', 163–96.

with the task of expressing it? It should be noted that this artificial intelligence relies on a 'reductionism' of human beings, viewed in all their diverse aspects.[64] The urgency of the fight against terrorism as well as the urgency of protecting the health of citizens justifies all the more the use of the solutions offered by digital technologies and their truth. It is a matter of relying on the virtues of multiple hastily constructed processes to give citizens the comforting illusion of the presence of Big Brother. Thus, as Supiot notes, a 'government by numbers' is emerging,[65] that is to say, a government which relies solely on statistics claiming to give a better account of reality than that made through contact and dialogue with people.[66] Sabot, in Chapter 2 of this collection, makes a similar contention.

As the DPA's Knowledge Centre rightly notes about the cooperation agreement relating to the health passport, 'COVID Safe',

> A reasonable boundary must therefore be drawn between what is a matter of individual freedom and responsibility and what may be a matter of social control, taking care to impose restrictions on fundamental rights and freedoms only when strictly necessary and proportionate to the public interest objective pursued. In this evaluation, the Authority insists on the need to be particularly attentive to the real risk of creating a 'phenomenon of dependency', which could lead us in the future to accept that access to certain places (including everyday places) be subject to the disclosure of proof that the person concerned is not a carrier of infectious diseases nor any other pathologies. The Authority draws attention to the importance of ensuring that the solution put in place authorising access to certain places or events does not result in a shift towards a surveillance society.[67]

Furthermore, we note, following Rappin, that cybernetics is the 'privileged instrument' used by government to curb crises: 'One cannot help but be struck by the proximity between the cybernetic project, implemented by a government of, and by, emergency, and the "shock doctrine".'[68] The author is referring here to a concept coined by Naomi Klein: 'This is how the shock doctrine works: Like a terrorised prisoner who gives up the names of his comrades and renounces his faith, societies in a state of shock abandon rights that, under other circumstances, they would have jealously defended.'[69]

[64] On this point, see my reflections in Poullet, *Éthique et droits de l'homme*, no. 40 onwards; Rouvroy's interview in Bherer, 'En 2018, résistez aux algorithmes avec la philosophe Antoinette Rouvroy'.
[65] Supiot, *La gouvernance par les nombres.*
[66] In this respect, see the conclusions of Ost, 'Nécessité fait loi?', 32.
[67] DPA Notice no. 124/2021 of 12 July 2021, 14.
[68] Rappin, 'Algorithme, management et crise', 109–10.
[69] Klein, *Shock Doctrine.*

Thus, the state of emergency is discreetly and sustainably put in place through the use of technological tools during times of crisis. If the usefulness, even if it is questionable, of these tools may be justified in times of crisis, it is nevertheless to be feared that they will be maintained in the name of the services rendered, of the interests of those who manage or contribute to them, of the investments made in them, and of the habitual familiarity towards them developed by citizens who have become docile. If the state of emergency readily explains the recourse to digital technology, in turn digital technology takes over the state of emergency and turns it into a 'permanent emergency', with the unconscious complicity of the populace. Beyond the crisis of the pandemic, what digital technology does to the law is to reinforce a state of lawlessness through its consecration of the state of emergency.

V. Conclusion

In this respect, and so to be clear, it is useful to reiterate the assertion of Morozov, an ardent critic of technological solutionism, that 'technology is not the enemy; our enemy is the romantic and revolutionary problem solver who resides within'.[70] To be more precise, it is the overconfidence, undoubtedly backed by the interests of some digital actors, relayed by our governments and progressively instilled in the population that leads to such a situation. This observation therefore requires prudence, transparency and democratic control of our tools, as well as putting them to use in the service of society and of the rule of law, even in times of crisis.

That the crisis in all its forms, and not only the health crisis, requires a state of emergency, and in this context in particular, the implementation of technological tools and information systems able to fight it, we are in complete agreement. However, it is also important to add that this state of emergency warrants guidelines that are to be found within the framework of the ECHR and, we believe, in a Belgian law that frames the actions and procedures which must be followed in these contexts of crisis. These measures are essential in order that the guidelines capable of guaranteeing the maintenance of our freedoms, social justice and our rule of law are imposed *in tempore non suspecto*. Within the framework of this law, which reconciles a state of emergency with the rule of law,[71] it is even more important to consider provisions relating to information systems, for there is a strong temptation, in the name

[70] Morozov, *To Save Everything, Click Here*, 358.

[71] On the difficulty of reconciling the rule of law and the state of emergency, see the thesis by Basilien-Gainche, *État de droit et états d'exception*, 263ff., in which the author examines the eleven conditions for the respect of the rule of law by the rulers in case of recourse to the state of emergency.

of urgency and effectiveness of the measures taken, to build a society of excessive profiling and surveillance through technological solutions.

VI. Bibliography

Abitboul, Serge, Alberto Alemanno, Emmanuelle Barbara, Jean Cattan, Christine Coslin, Mireille Delmas-Marty, Jean-Gabriel Flandrois, Laura Kövesi, Hans W. Micklitz, Hubert de Vauplane, and Jean Ziegler. 'Ce que 2020 a fait au droit.' *Le Grand Continent*, 4 January 2021. https://legrandcontinent.eu/fr/2021/01/04/ce-que-2020-a-fait-au-droit/.

Basilien-Gainche, Marie-Laure. *État de droit et états d'exception: une conception de l'État*. Paris: Presses universitaires de France (Collection Fondements de la politique), 2013.

Bherer, Marc-Olivier. 'En 2018, résistez aux algorithmes avec la philosophe Antoinette Rouvroy.' Interview. *Le Monde*, 29 December 2017. https://www.lemonde.fr/idees/article/2017/12/29/en-2018-resistez-aux-algorithmes-avec-la-philosophe-antoinette-rouvroy_5235555_3232.html.

Bioy, Xavier. 'Vers la vaccination obligatoire contre la Covid? Que dit le droit de la santé? Que répondent les droits fondamentaux?' *Le Club des juristes*, 8 July 2021. https://blog.leclubdesjuristes.com/vers-la-vaccination-obligatoire-contre-la-covid/.

Blandin, Annie, 'La gouvernance du monde numérique: que fait l'Europe?' *Comprendre la souveraineté numérique*, *Cahiers français* 415 (May–June 2020): 50–6.

Calay, Vincent. 'L'empire des logiciels, menace pour les démocraties?' *Cahier de prospective de l'IWEPS* 5 (July 2021). https://www.iweps.be/wp-content/uploads/2021/07/CAPRO05-150721-1.pdf.

Cardon, Dominique. 'Le pouvoir des algorithmes.' *Pouvoirs* 164, no. 1 (2018): 63–73.

Colella, Stéphanie. 'Chapter 1: L'acception des notions de restriction, limitation et derogation.' In *La restriction des droits fondamentaux dans l'Union européenne*. Brussels: Bruylant, 2018.

Costa, Jean Louis. 'Le recours à l'article 15 de la Convention européenne des droits de l'homme.' *Le Club des juristes*, 27 April 2020. https://blog.leclubdesjuristes.com/recours-article-15-cedh/.

De Schutter, Olivier. *International Human Rights Law: Cases, Materials, Commentary*. 2nd ed. Cambridge: Cambridge University Press, 2014.

Garapon, Antoine. 'Un moment d'exception.' *Esprit* 464 (May 2020): 87–92.

Guyader Alain et al. 'La Datacratie.' *Pouvoirs* 168, no. 1 (2018): 7–18.

Klein, Naomi. *The Shock Doctrine: The Rise of Disaster Capitalism.* Toronto: Vintage Canada, 2007.

Larrieu, Jacques. 'Avant-propos.' In *Crise(s) et droit*, 9–12. Toulouse: Presses de l'Université Toulouse 1 Capitole (Collection Institut fédératif de recherche 'Mutation des normes juridiques'), 2012.

Laugee, François. 'Solutionisme.' *Revue européenne des médias et du numérique* 33 (2014), reprinted on the journal's website, 30 July 2021. https://la-rem.eu/2015/04/solutionnisme/.

Morozov, Evgeny. *To Save Everything, Click Here: The Folly of Technological Solutionism*. New York: Public Affairs, 2013.

Ost, François. 'Nécessité fait loi? La santé n'a pas de prix? Ce que le Covid fait au droit.' In *La pandémie de Covid-19 face au droit*, edited by Saba Parsa and Marc Uyttendaele, 17–43. Limal: Anthemis, 2020.

Parsa, Saba, and Yves Poullet. 'Les droits fondamentaux à l'épreuve du confinement et du déconfinement.' In *La pandémie de Covid-19 face au droit*, edited by Saba Parsa and Marc Uyttendaele, 137–213. Limal: Anthemis, 2020.

Poullet, Yves. 'COVID et libertés: quelques considérations.' In *L'utilisation du numerique dans la lutte contre la COVID – enjeux techniques, éthiques et juridiques*, edited by Yves Poullet and David Doat, 75–125. Paris: L'Harmattan, 2022.

———. *Éthique et droits de l'homme dans notre société du numérique*. Brussels: Belgian Royal Academy (Collection Mémoires de l'académie), 2020.

———. 'La société et les droits fondamentaux aux risques du numérique en temps de crise – plaidoyer pour un régime légal strict de l'état d'exception.' In *Droit et pandémie*, edited by Françoise Tulkens and Saba Parsa, 165–205. Limal: Anthemis, 2022.

———. 'Pandémie, numérique et droits de l'homme – un étrange cocktail!' *Journal de droit européen* 270, no. 6 (2020): 246–63.

Rappin, Baptiste. 'Algorithme, management et crise: le tryptique du gouvernement de l'exception permanente.' *Quaderni* (2018): 103–14.

Renucci, Jean-François. *Droit européen des droits de l'homme*. 6th ed. Paris: LGDJ, 2015.

Rouvroy, Antoinette, '"Adopt AI, Think Later": The Coué Method to the Rescue of Artificial Intelligence.' https://www.academia.edu/42067794/_Adopt_AI_think_later_The_Cou%C3%A9_method_to_the_rescue_of_artificial_intelligence.

Rouvroy, Antoinette, and Thomas Berns. 'Gouvernementalité algorithmique et perspectives d'émancipation. Le disparate comme condition d'individuation par la relation?' *Réseaux* 177 (2013): 163–96.

———. 'Le nouveau pouvoir statistique ou quand le contrôle s'exerce sur un réel normé, docile et sans événement car constitué de corps "numériques" [. . .].' *Multitudes* 40 (2019): 88–103.

Sudre, Frédéric. 'La mise en quarantaine de la Convention européenne des droits de l'Homme.' Post. *Le Club des juristes*, 20 April 2020. https://blog.leclubdesjuristes.com/la-mise-en-quarantaine-de-la-convention-europeenne-des-droits-de-lhomme/.

Supiot, Alain. *La gouvernance par les nombres. Cours au Collège de France (2012–2014)*, Paris: Fayard, 2015.

Tesquet, Olivier. *État d'urgence technologique. Comment l'économie de la surveillance profite de la pandémie.* Paris: Premier Parallèle, 2021.

Van Drooghenbroek, Sébastien. *La proportionnalité dans le droit de la Convention européenne des droits de l'homme – prendre l'idée simple au sérieux*. Brussels: Bruylant, 2001.

Verdussen, Marc. 'Droits humains et crise sanitaire – l'état mis au défi.' *La libre Belgique*, 19 July 2020.