13

The Paradox of Digitalisation in the Case of the COVID-19 Apps: What Lessons Can We Learn from This Strange Experience?

Paula Veiga

13.1 INTRODUCTION

The rise of the internet and digitalisation have profoundly changed social relations and spread their influence in the juridical field. There is nothing new about this realisation. But the failure of COVID-19 apps during the pandemic in the Western world indicates that the trend of social adherence to digitalisation is neither automatic nor without restraint.

The mainstream analysis of contact-tracing apps is commonly closely related to data protection standards and digital surveillance technologies in order to obtain important gains: to prevent mass surveillance, and to protect human rights and the rule of law.[1] I reiterate 'closely related' because this second millennium has brought dramatic progress towards the recognition and enforcement of human rights, which is a positive development.

In this chapter, another perspective is sought – a broader one, perhaps even more comprehensive – based on the perplexity from our recent experience of contact-tracing apps, which embodies, as already said, a non-adherence to digital platforms in this particular case, unlike other areas (online shopping contracting, networks…).[2] These mentioned areas also pose several juridical problems, namely one of the real threat of the 'private' profiling of citizens and exploiting their vulnerabilities for commercial purposes. Therefore, one cannot assess the contact-tracing app experience in light of this element only. The scenario may be more complex than that.

Perhaps a broader analysis of this experience can answer how human rights law should develop in the face of the challenges of digital technologies.

[1] The literature is extensive. See, e.g., L. Bradford, M. Aboy, and K. Liddell, 'COVID-19 contact tracing apps: a stress test for privacy, the GDPR, and data protection regimes' (2020) 7 *Journal of Law and the Biosciences* 1, 1–34.

[2] The literature on digitalisation is starting to be extensive. Some recent thoughts can be seen in C. Kaufmann, 'Responsible business in a digital world – what's international law got to do with it?' (2021) 81 *Heidelberg Journal of International Law* 3, 781–815; J. F. MacLennan, 'Facing the digital future: public service broadcasters and state aid law in the European Union' (2017) 2 *Cambridge Yearbook of European Legal Studies*, 159–202.

In the first two decades of the twenty-first century, the rule of law scenario and its paradigms changed through digitalisation, the exceptionalism of the pandemic, and the need for the protection of human rights worldwide.[3] That is the background to the contact-tracing app experience, and we must take a deeper and more serious look at this apparently transitory phenomenon.

13.2 THE IMPACT OF DIGITALISATION: SOME HIGHLIGHTS FROM THE PUBLIC LAW PERSPECTIVE

Digitalisation is a hyper-complex phenomenon that uses new resources and new formats, and creates new problems in the juridical realm. The internet is not just an information platform, nor an ordinary channel of communication; it is the new centre of social communications. Almost all areas of our lives are reflected in cyberspace: economy, politics, trade, education, family, financial transactions, but also criminal activities, terrorism, and so on. This means that the issue is not only technological or economic, but also legal. The technological process has changed cultural norms and social behaviour, which also changes legal behaviour.

Among the juridical problems, there is one that deserves to be specifically mentioned: digitalisation has created a new good, very different from the classical physical goods we were used to – that is, data. In the twenty-first century, data will be the most valuable asset, especially personal data, and, as far as we can see, policy will struggle to control the flow of data. Data demands a different approach to regulating juridical relations, as it is not intended for exclusive use as the classical physical goods were. As we immediately intuited, this will be reflected in legal concepts as it is warrantable that classical notions, such as 'ownership', can be modified to form new or alternative concepts. It is now clear that digitalisation will always be accompanied by the collection, storage, and processing of large amounts of data, so-called big data, that will differ in terms of shape, size, and speed. Before the digital age, data essentially meant information about a certain content, collected by identifiable people. This has changed with digitalisation. Data is now a *container* for information. As the historian Yuval Noah Harari says, in a rather pessimistic view, there is a

[3] About these changes in the juridical paradigm, caused by digitalisation, see S. Koloß, 'Facebook and the rule of law' (2020) 80 *Heidelberg Journal of International Law* 2, 509–31; D. Harvey, *Collisions in the Digital Paradigm: Law and Rule-making in the Internet Age* (Oxford: Hart Publishing, 2017); M. Belov, *Rule of Law at the Beginning of the Twenty-first Century* (The Hague: Eleven International Publishing, 2018); about general changes in the twenty-first century, see A. v. Bogdandy, 'Globalization and Europe: how to square democracy, globalization and international law' (2004) 15 *European Journal of International Law* 5, 885–906. A notion of an international approach to rule of law can be seen in E. Katselli, 'The rule of law and the role of human rights in contemporary international law', in R. Dickinson et al. (eds.), *The Rule of Law and the Role of Human Rights in Contemporary International Law* (Cambridge: Cambridge University Press, 2012), pp. 131–52. My recent thoughts about the issue can be found in P. Veiga, *Direito Constitucional e Direito Internacional no Contexto do Constitucionalismo Global: Um Roteiro Pedagógico* (Lisbon: Petrony, 2020).

new universal narrative that replaces religious authority and the humanist ideology with the authority of the algorithm and big data.[4]

Another aspect that deserves special attention in light of public law is connected to more recent activities in the digital world. While in the early years of this century, discussions focused on the opportunities and risks of the internet, namely the protection of privacy and data; we are now facing a new type of activity, and therefore new challenges – those associated with the globalisation of communication infrastructures and markets, artificial intelligence (AI), big data, and its consequences for the collective interest (e.g., health services, political elections). Considering this, some of the most important problems caused by digitalisation in public law concern the information and technology revolution and its connections with the humanist traditions in which constitutions are based. How is it possible to enhance the legitimacy of the new information order, the impact of digitalisation on democracy and will-formation processes, the impact of digitalisation on the courts and administrations, namely the limits of digital justice, and the impact of the digital revolution on data protection, privacy, and human rights.

At the constitutional level, since the constitutional state and constitutions were built around the principle of human dignity, it is inevitable that the domain of the machine and the emergence of AI, with its new paradigms (acceleration, instantaneous action, and connectivity), will bring changes to several pillars of constitutionalism, namely the pillar of rights, the institutional pillar, and the pillar of legitimacy.

In this field, the most immediate concerns of digitalisation are related to: (a) the protection of rights, (b) the birth of new rights (e.g., the right to be forgotten, the right to social access to the internet), (c) the new understanding of competences, since the internet goes beyond the jurisdiction of state or region (legal orders, both national and international, are based on the Westphalian concept of sovereignty and state-centred power), and (d) public discourse and the formation of political will.

This means a change in the constitutional system, especially because the internet increases the ability of citizens to exercise their fundamental rights, but also increases the risk of threats to fundamental rights, and, related to the public sphere, the internet emphasises the special role of private actors. To express this succinctly, digitalisation can be a tool for both protecting and violating human rights, with direct implications for the cyber- and physical security of individuals.

Besides the pillar of rights, States must of course reorganise their classical functions that were based on territoriality. Some authors argue that there is a trend to territorialise cyberspace (aka 'sovereignty fever'). I feel it is too soon to reach that conclusion. As already stated, space and territory have been important as bases for the law for several centuries (in fact, territory is even a political construction in the legal field). All these have changed with the internet and digitalisation.

[4] Y. N. Harari, *21 Lessons for the 21st Century* (New York, NY: Vintage Publishing, 2019).

The (new) public sphere is public–private, fragmentary, immediate, and egocentric.[5] This makes it difficult to distinguish between individual information and press information, and therefore the exact new notion of public opinion. Still considering the pillar of rights, the existing rights have gained a new dimension in the context of applying new technologies, and this necessitates a reinterpretation. We can also see the emergence of *new* digital rights.

Overlooking the rights themselves, and considering both the categories of fundamental rights and human rights, digitalisation implies, above all, a redefinition of privacy and other (personal) rights related to free will, as well as all rights connected with communication through the media (namely, freedom of expression and freedom of press and media). In addition to the framework of rights already broadly affirmed, there is the legal consecration (at constitutional and international levels) of new rights (digital rights), such as the right to access the internet irrespective of economic condition, the right to digital education, the right to neutrality on the internet, the right of access online data, innovations, creations, and knowledge generated by public funds, and the right to be forgotten.

There is (as yet) no international Bill of Digital Rights, which, in order to be approved, should be under the auspices of the United Nations. But in international law new configurations of human rights arise, especially the rights to freedom of expression and privacy. In this context, we can recall the UNESCO Recommendation concerning the promotion and the use of multilingualism and universal access to cyberspace (2003), that states the need for the coexistence of public and private, as well as civil society at the local, national, regional, and international levels, and the principle of universal access to the internet as a service of public interest.[6] The World Summits on the information society (Geneva, 2003; Tunis, 2005) should also not be forgotten.

In the European law context, and considering the Europeanisation of the protection of fundamental rights through technology, it is worth mentioning Directive 2009/136/EC of the European Parliament and the Council,[7] a process that was initiated with the first Directive on the protection of personal data.[8] We should also

[5] About the classical public sphere, see J. Habermas, *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society* (Cambridge: Polity Press, 1989).

[6] UNESCO, Recommendation concerning the Promotion and Use of Multilingualism and Universal Access to Cyberspace, 15 October 2003, www.unesco.org/en/legal-affairs/recommendation-concerning-promotion-and-use-multilingualism-and-universal-access-cyberspace.

[7] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector, and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (Text with EEA relevance), OJ L 337, 18.12.2009, 11–36.

[8] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, 31–50.

remember Regulation 2015/2120, which establishes measures dealing with access to the open internet and amends Directive 2002/22/EC on universal service, as well as Regulation 531/2012 on roaming on public mobile communications networks in the European Union (EU),[9] and, finally, the well-known Regulation on Data Protection (Regulation 2016/679), which repealed the aforementioned Directive 95/46/EC.[10]

13.2.1 *The Specific Case of Digitalisation among Health Norms*

One of the areas crucial to digitalisation is that of public services, in which health services are usually included.[11] This implies the development of a digital citizenship, a citizenship that will entail a new way of understanding relations between administrations and citizens where recognition of rights are concerned, namely the confidence for citizens about electronic ways of working (e.g., privacy and security issues). Of course, the EU is trying to develop a common vision of how e-government services will develop, and subsequently is committed to its implementation.

Alternatively, digitalisation is favouring the development of a new 'health market', namely through the reorganisation of therapy and business models offered by digital platforms, such as tablets with computer chips, implants with sensors, fingerprints, fitness trackers, and medical apps. The use of digital technologies concerning health poses special technical as well as philosophical and juridical problems, as this involves dealing with well-recognised sensitive data.[12] But doctors, pharmacists, and companies have banded together to develop applications that promise to redefine the way medicine is practised. There will likely be a need for new models, such as patient-oriented care and a more efficient system (perhaps an interconnected and smart-healthcare system capable of solving complicated situations in the healthcare sector using digital tools). Insurance companies will require special attention, as they will be responsible for handling sensitive data.

The main framework is already enacted by the General Data Protection Regulation (GDPR) (generally, processing data can be carried out without the consent of the individual). This health issue is also well known from the pandemic, as all over the world, and especially in Europe, the Council of Europe Member States moved forward in an attempt to make use of digital technology to slow down the

[9] Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union (Text with EEA relevance), OJ L 310, 26.11.2015, 1–18.

[10] General Data Protection Regulation (GDPR), OJ L 119, 04.05.2016; cor. OJ L 127, 23.5.2018.

[11] An analysis can be found in V. L. Raposo, 'The doctor just poked you: os novos desafios da e-health' (2014) 57 *Boletim das Ciências Económicas* 3, 2903–33.

[12] See, for all, how GDPR deals with health data.

spread of the virus.[13] The COVID-19 apps could, therefore, if they had been successful in Europe, have served as an experiment for the digitalisation of healthcare. This was not, in general terms, the case (one exception, at least in the first period of the pandemic, was the Italian Immuni). One should never forget that smart management of healthcare ('telemedicine') includes treatments connected to the use of medical apps, through which independent owners collect data, including healthcare data on the person concerned, which can be used for different purposes.

13.3 COVID-19: DIGITALISATION METHODS AND JURIDICAL CONCERNS

13.3.1 *The Most Fundamental Constitutional Problems Posed by COVID-19*

A constitutional and pluralist view of public law sees citizens and communities as subjects of legitimacy, and in this context the ability of the law to achieve political inclusion. That is why constitutionalism focuses above all on the impact of governance arrangements on human rights.

On 11 March 2020, the World Health Organization (WHO) recognised the spread of the disease as a pandemic and soon states and their governments needed to take specific measures. Apart from disrupting international supply chains, adding popularity to anti-migrant policies, and weakening globalisation, the administration of the crisis led to restrictions on several human rights (e.g., quarantine, travel, isolation) and forced states to resort to the use of public coercion and protective measures, including business closures and social distancing.[14]

At the constitutional level, the pandemic implies a return to two classical and constitutionally protected juridical concepts that were required to be balanced: freedom and security.[15] The complex agreement between these two concepts – freedom and collective interest – explains why COVID-19 primarily posed three constitutional issues among occidental constitutional states: (a) the place of parliaments in epidemic (emergency) circumstances and the operationalisation of the 'law of the crisis' that signifies, as a rule, a rebalancing of the various powers, determining the centrality of the executive power, in general, and the government, in particular (a

[13] In this context, see P. Donaldson, 'Covid-19 vaccines. A global common good' (2020) 1 *The Lancet Healthy Longevity* 1, e6–e8.

[14] The implications of COVID-19 in the human rights field are well listed in E. Gilmore, 'La lucha contra COVID-19 es una batalla por los derechos humanos', 17 April 2020, EU External Action, https://bit.ly/2FXqdhT.

[15] The balance needed is particularly evident in F. Piovesan and M. Morales Antoniazzi, 'Covid-19 e a necessidade de uma abordagem holística e integral da proteção dos direitos humanos', 25 April 2020, Blog Constitucional; *M. Morales Antoniazzi and S. Steininger*, 'How to protect human rights in times of Corona? Lessons from the inter-American human rights system', 1 May 2020, EJIL:Talk!, www.ejiltalk.org/how-to-protect-human-rights-in-times-of-corona-lessons-from-the-inter-american-human-rights-system/.

stronger executive); (b) the adequacy of the legal basis of the measures adopted; and (c) the proportionality of the measures materially adopted.

In terms of the justice systems, it is worth noting that there was almost an automatic response from states considering the suspension of the judicial service and the procedural deadlines that represents an impact on the universality of access to process and effective judicial protection. There were also several influences on the functioning of democracy, such as the postponement of elections, restriction of the rights of freedom, and the right to assembly.

All rights are susceptible to being restricted under certain conditions. In light of the European Convention on Human Rights, those restrictions shall not affect the legality principle, must have a legitimate aim, and must respect the proportionality principle. This instrument even has its own Article (Article 15) that rules the derogation of the Convention in times of emergency, under certain limits.[16]

13.3.2 *Apps during the Pandemic: Their Possible Significance and Role*

The COVID-19 pandemic made us face many problems and also contradictions.[17] One was its 'cosmopolitanism' – COVID-19 spread all over the world – on the one hand, and the national response to it on the other. Indeed, despite the fact that there is nowadays undeniably more international coordination than during previous pandemics (namely through the WHO), the fight against the virus continued to take place within the national framework, which reinforced the notion of sovereignty that was otherwise dissolving through the globalisation and digitalisation processes. At least in Europe, borders regained a new meaning with COVID-19.

When COVID-19 initially spread, proposals for monitoring the epidemic through technology soon emerged all across the world, but in Europe in particular, both organised by the EU and by each national state. In general, the European proposals were

[16] Article 15 (*Derogation in time of emergency*) of the European Convention on Human Rights:

1. 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.
2. No derogation from Article 2, except in respect of deaths resulting from lawful acts of war, or from Articles 3, 4 (paragraph 1) and 7 shall be made under this provision.
3. Any High Contracting Party availing itself of this right of derogation shall keep the Secretary General of the Council of Europe fully informed of the measures which it has taken and the reasons therefor. It shall also inform the Secretary General of the Council of Europe when such measures have ceased to operate and the provisions of the Convention are again being fully executed.

[17] I have had the opportunity to reflect on some of them in P. Veiga, 'Uma lição da pandemia: renúncia à globalização ou limites a essa renúncia? Ressignificação do Estado', in A. S. Pinto Oliveira and P. Jerónimo (eds.), *Liber Amicorum Benedita Mac Crorie*, vol. II (Braga: UMinho Editora, 2022), vol. II, pp. 381–90.

concerned with defending the rule of law and two particular human rights – data security and privacy. The key features were the aggregation of data (and subsequent anonymisation), the purpose, principle, and voluntariness.[18] The apps, according to European parameters, were designed to the highest standards of data privacy and data security. Their aim was not to track individuals and not to hold personal information. But even in the EU, where there is sophisticated regional integration, the response to the pandemic was far from uniform and efficient.

Of course, an app does not replace the human side of constraining the disease, but it is generally accepted that it can help. Like a piece in a puzzle, it is a tool to facilitate the resolution of the problem. These systems would enable people who had tested positive for COVID-19 to share information about their recent contacts, so that those individuals could be contacted and given appropriate public health advice to help limit the spread of the virus.

The official response, both from the European Data Protection Committee (EDPC) and the Council of Europe were issued in April 2020. The EDPC enacted Guidelines No. 4/2020 on the use of location data and contact-tracing tools in the context of COVID-19, on 21 April, with the Council issuing a document on 7 April. The European Commission also highlighted that contact tracing was just an instrument within the public health strategy, while clearing the advantages in creating a single app for mobile devices at the European level. However, the responses were fragmented and uncoordinated. Examples of national responses include the Italian Immuni, the German Corona Warn, the Irish COVID Tracker, and the Portuguese StayAway Covid.

In light of the rule of law and the right to privacy, there are five basic ideas to be kept in mind: (a) the pandemic was an exceptional scenario and called for exceptional measures; (b) the proportionality principle has a different meaning in normal times and times of exception; (c) privacy is intrinsic to the idea of the Rule of Law; (d) the Right to Privacy is a fundamental right and a human right (protected in Europe by Article 8 of the European Convention on Human Rights); and (e) Protection of Data and Privacy are two different rights, but both are protected in the European context.

This immediately means a juridical framework to treat personal data, informed consent, and the responsibility of treating data – all statutes in the GDPR.

The contact-tracing apps can be integrated into individual measures in the pandemic to avoid infection, alongside testing and vaccination – this implies responsibility, in addition to liberty.

[18] Initiatives from the European Data Protection Board and from the Council of Europe, both from April 2020. European Data Protection Board, 'Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the Covid-19 outbreak', 21 April 2020, www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042020-use-location-data-and-contact-tracing_en and European Council, Council of the European Union, 'Covid-19', www.consilium.europa.eu/en/topics/covid-19/.

Traditional contact tracing is performed by teams of trackers who have to rebuild all the interactions a positive person had. This process consumes both time and resources. The time needed to identify contacts is a critical issue. The stress on responsibility is very important in the case of this tool, with statements that included the idea of a shared responsibility between communities and governments. The implicit value of the app was, therefore, beyond its technology; it instilled a sense of responsibility for the citizens to be part of the solution in addressing the spread of the COVID-19 virus. But it seems that beyond privacy concerns, other issues were at stake, namely efficacy, lack of transparent communication, and sacrifice of privacy when the sacrifice was not worthwhile (disbelief in the usefulness of the app).

All in all, while testing and vaccination were a relative success, contact-tracing apps were a complete failure in Western states. The main tool to combat the pandemic was, of course, vaccines, authorised from December 2020, as voluntary and free for all citizens.

It is also worth remembering that the success of the contact-tracing apps depended on the willingness of the citizens to permanently install and use them; in other words, voluntariness. But, once again, vaccines were also voluntary. That is why the question remains: why did citizens refuse to subscribe to this tool when it comes to the protection of public health, if they normally download applications for other (minor) purposes, which also have juridical consequences? What justifies this dual use of technology in the light of the law?

We must keep in mind that technology should guard patient privacy, but equity and collective benefit are also issues of concern.

13.3.3 *An Effort to Find a Justification …*

The COVID-19 period was trying, but its consequences were far-reaching. A major proof of this is given by the UN Security Council Resolution 2532 (2020), a symbolic mark, which characterised COVID-19 as a threat to peace and international security, demanding, therefore, for the first time in history, a humanitarian pause in world conflicts.[19]

The pandemic caused the mobilisation of a state of emergency in most countries and in Portugal, in particular, within the framework of the 1976 Constitution for the first time since its entry into force (even though emergency powers have been in the Constitution from the outset). In the Portuguese case, the first patient was diagnosed on 2 March 2020 and the first death occurred fourteen days later.[20]

[19] UN Security Council resolution 2532 (2020) [on cessation of hostilities in the context of the coronavirus disease (Covid-19) pandemic], 1 July 2020, S/RES/2532 (2020).

[20] State of emergency is ruled especially in articles 19 and 138 of 1976 Portuguese Constitution (the text is available in English at www.parlamento.pt/sites/EN/Parliament/Documents/Constitution7th.pdf). The regime is explained in English by C. Santos Botelho, 'Covid-19 and stress on fundamental rights

States were faced with the legal projection of the effects of a pandemic in terms of fundamental rights, a crisis framed by a normative framework that is easily blurred. The admixture of these components gives rise to several questions. Among them are the distinction between situations of normality and situations of exception, the central role played by the executive in the context of the response to the crisis, and the subordination of exceptional measures to the rule of law.

Alternatively, we should never forget that digitalisation and, with it, mass surveillance, are omnipresent in society. Measures of surveillance (all at the heart of the digitalisation process) and privacy infringements are not always of the same degree and must be highlighted in categories, identifying the severity of possible human rights infringements. Let us hierarchise those according to three possible degrees: highly intrusive responses, intrusive responses, and mildly intrusive responses.

That said, it is necessary that one asks why contact-tracing apps were so inefficient during an era of digital applications, especially keeping in mind that the guiding principles of all action in times of a pandemic are freedom and responsibility, as already noted. In other words, in this balance between freedom and responsibility, it is worth asking why the contact-tracing apps were perceived as such a serious interference in informational self-determination. The first idea that one can imagine is the fear of being segregated or marginalised in communities once it became known that a citizen tested positive. But the scenario can be more complex than that.

First, because if it is true that the Western legal system is not built to impose restrictions on personal freedom when there is no culpability or direct benefit, it is also worth remembering that in an emergency situation rights are under stress.[21] Second, the COVID-19 pandemic led to restrictions in a range of areas. Common examples are the right to freedom of movement and assembly, the right to a fair trial, the right to education, and the right to private and family life.

I believe that the first important lesson to learn from this strange experience is the urgent need to regulate the health market properly, based on the ideas that digitalisation demands de-territorialisation, de-centralisation, and de-nationalisation. In technological terms, the system worked. However, the new wave of techno-optimism was in doubt. The problem was that technology was not enough. I believe the main threats felt by citizens were: (a) the use of the data produced by such tools for disease modelling and epidemic dashboards; (b) the information on health decisions through technology-driven disease testing; and (c) the use of technology to counter health-related discrimination.

in Portugal: an *intermezzo* between the state of exception and constitutional normality' (2020) *Revista Catalana de Dret Public (Catalan Journal of Public Law)*, special issue.

[21] The stress on human rights in a pandemic crisis is demonstrated by an unprecedented number of states derogating from the International Covenant on Civil and Political Rights and from regional human rights conventions during COVID-19: S. Molloy, 'Covid-19 and derogations before the European Court of Human Rights', 10 April 2020, Verfassungsblog, https://verfassungsblog.de/covid-19-and-derogations-before-the-european-court-of-human-rights/.

In addition, there are always contextual issues. Social, political, economic, and psychological factors can affect citizens when adopting and/or using technology. We can imagine how attitudes towards the pandemic and the general attitude of the people before and during the pandemic can change (from negative – dissatisfaction, unhappiness, compliance, etc., to positive – satisfaction, appreciation, etc.).

In the Portuguese example (the one I know best), people were not sufficiently encouraged to start using the app. This involves two simple steps – the first is how to install the app and the second is instructions on how to operate the app using a smartphone. However, we must not forget that Portugal has many citizens without digital skills (especially the elderly who may not be conversant with new technologies), and the developers of the app did not consider them.

There was not enough public awareness about the app, and information and knowledge on usage was limited. The main efforts came from the government. However, the media did not promote the use of the app, either in the press or on radio stations, unlike what happened in other countries (e.g., Germany, with the Corona-Warn-App).[22] Specialists at the time reported that we would need at least 60 per cent of the population to download and actively use the contact-tracing app in order for it to be useful.

Let us go beyond the surface and utilise this experience to reflect on digitalisation and its implications in the juridical area. The digital transformation in the legal world can generate two paths: (a) the need for the right to 'give in' to new technologies, reducing the level of legal protection for those rights negatively affected by technologies; and (b) the call to update and reconceptualise the existing legal framework to accommodate new technological developments.

The real and critical challenge for public law and human rights protection in the digital age is finding and maintaining the appropriate balance between the advantages and disadvantages that the application of technology brings; that is, how to ensure that technological development moves within a framework that provides the well-being of human society.

13.4 THE LESSONS LEARNED

In contemporary democracies, trust in public and political institutions has collapsed in the last decade of the twentieth century and the beginning of the twenty-first century.[23] This is probably one substantial explanation for the non-adherence to the COVID-19 app in the Western states (first lesson). Added to that, the COVID-19 crisis highlighted the issue of trust in democracies, as governments had to both

[22] See C. Brause, 'Mit dieser Warn-App will die Regierung das Leben wieder normaler machen', 1 April 2020, *Welt*, www.welt.de/wirtschaft/article206935981/Coronavirus-Mit-dieser-Warn-App-will-die-Regierung-das-Leben-wieder-normaler-machen.html.

[23] G. Abiri and J. Buchheim, 'Beyond true and false: fake news and the digital epistemic divide' (2022) 29 *Michigan Technology Law Review*, 59–109.

undertake (unprecedented) restrictive measures to manage the spread of COVID-19 and to rely on the citizens' willingness to adhere to these measures.

Cyberspace is a global network, primarily for private entities and institutions, and that includes public institutions – which poses a fundamental question about the role of the state in this new world of goods and services.

A constitutional approach means a policy that deals with digital technologies from a perspective also aimed to protect fundamental rights and democratic values, which includes framing the debate within the information society; this is increasingly subject to the power of public and private actors implementing automated decision-making technologies. As a first consequence, far from simply applying existing law in cyberspace, there is an urgent need for online laws, such as the GDPR (second lesson). Especially in the healthcare field, we should amplify the call for building and strengthening stable global healthcare data and technology governance frameworks to assist digital surveillance suitable for overall healthcare systems. An appropriate institutionalisation of a rights-based framework would enhance trust, as well as longer-term geographical equity and comprehensive health and care. With the COVID-19 app experience, we have learned that technology as embellishment does not work at all.

In that field, the Council of the EU has considerable experience, as it played a crucial role in consolidating the constitutional dimension of the right to privacy and data protection in Europe, through the Data Protection Directive. So it is desirable that the institution focus on strengthening governance of digital healthcare systems, with at its heart the concept that healthcare is a public good (rather than health data as a public good).

The notion of the rule of law is also at stake. Indeed, the crisis of the rule of law is the crisis of trust. To exemplify that, just remember two recent European situations: the non-enforcement of refugee laws in Europe and high-level corruption in public entities. These two quite different examples prove that rules are also not being obeyed in Europe, which generates a problem of trust.

Trust, in light of the rule of law, is not trust in persons but trust in institutions (e.g., courts) and systems (e.g., the EU). This problem of trust has been reinforced by several measures in some states during the pandemic, as proven by people attending street events, criticisms of political leaders, and divided institutions.

The main problem of trusting institutions is related to the classical notion of the rule of law (the formal rule of law concept). One knows that there is an intrinsic ambiguity across legal traditions in this concept (there are differences between the English idea of 'the rule of law', the German *Rechtsstaat*, the French *l'Etat de droit*, the Italian *Stato di diritto*, etc.), but they all mean a relationship between state, constitution, governing, and law. In other words, this traditional concept is clearly related to notions of the separation of powers, general and public rules for all, and consistent and transparent regulation.

This system of checks and balances, along with the principle of the separation of powers, represents the common core of constitutionalism. The ideal of limited

government, intrinsic to any form of constitutionalism, requires the adoption of a system of reciprocal control among different branches or decision-making centres of the state, and rejects the unwarranted concentration of power in the general constitutional design (third lesson).

This is the core of public law, even with digitalisation in progress. That is why we should identify a new notion of public authority, which includes acts, institutions, and relations of states, supranational institutions, and international bodies, and apply it in these normative dimensions of public law, both offline and online. Indeed, all public institutions must act according to the standards of democratic public law, no matter if they are acting offline or online.

A healthy suspicion of power provides democracy its vitality, but, and let us stress this point, democracy depends on trust. Besides, liberty in democracy is not only individual liberty, but also collective liberty.

We should try to continue and widely reflect on this lack of trust. Modern societies are creating particularised trust based on race, ethnicity, lifestyle, moral identity, or religion. I am not sure if this scenario is helping the real standards of trust. What is clear is that public policy has to cope with diversity, but trust can withstand the pressure that diversity poses. One thing is certain: in the end, a failure of trust is a failure for democracy.

Public entities must assure trust in justice (perception of the judiciary), maintain awareness of any (dis)satisfaction with public services, pay attention to corruption, and its perception, and govern with transparency and accountability. There is no need to stress that good governance practices influence citizens' attitudes and behaviours towards the government (fourth lesson).

In Europe, the problem of trust is a problem both for political institutions and the courts, not only in European institutions, but also in national institutions. This means a long path to develop a collaborative way forward, where trust is seen as a value by institutions.

Besides, ensuring anonymity is not enough. The technology used in the social context must be considered; for example, when providing additional support to citizens that have experienced discrimination because they contracted the COVID-19 virus. Furthermore, the use of a smartphone application to trace those individuals that an infected person has been in contact with in order to prevent the spread of COVID-19 is not such a novel situation.

From a broader perspective, there are benefits in enabling voluntarism, solidarity, and public modes of association, even in political relations (fifth lesson). The simple fact that national decision-making has shifted from domestic policies to policies that result from participation in a global or transnational decision-making process alters the dynamics of all decision-making. This will mean limiting coercive organisation in favour of voluntary association, enabling broader participation. Not all, but certain kinds of rights – in particular, rights of association, speech, and political participation – must shift from problem-solving mode and from a coercive manner

to include participatory relations (according to the all affected principle). This principle says, roughly, that all those who are affected by a decision should have a right to participate in making it. The explanation is simple: it is only when strangers are no longer treated as bearers of malign intent that the possibilities of extensive trust can develop.

It is clear that globalisation and the proliferation of communicative platforms is taking people away from 'vertical' interactions in which representative politics is typical, toward more distributed, flatter, or 'horizontal' modes of sociality, working, and organising, which poses special problems for democracy itself, as this leaves us in a 'post-representative' political moment, which means that the advent of online communication has had both good and bad effects on the practice of democracy.

It is also pointless to recall the normative concept developed by Jürgen Habermas – the public sphere. For Habermas, modernity was formed from the development of a division between state and society.[24] The public sphere became politicised and was transformed into a political public sphere and this concept – the political public sphere – is the most difficult and controversial issue in terms of the constitutional power posed by digitalisation. It suffers a profound alteration in the Habermasian sense; that is, as a sphere of communication. Habermas explains this situation as one where individuals can discuss critical issues and gain knowledge of public issues. In this way, political public opinion is formed – a public and shared space in which decisions are made through dialogue.

Indeed, communication, an essential element for the formation of will within a community, is now guided by a new paradigm. I even question if digital communication is still 'only' a way of exercising freedom of expression.

This new paradigm is more accelerated, more instantaneous, and more connected. The public sphere, as already stated, became fragmentary, immediate, egocentric, and public–private. Besides, it includes a great divergence of publics, the political, the cultural, and so on. Knowledge is generated and disseminated in a decentralised manner and the reconstruction of meaning is carried out by acceptance and reproduction without any control. The protagonists are unknown. They are no longer ministers of religious cults, artists, or intellectuals. But will it be the will of leaders (political, business, etc.) or instead the will of the media? Or even none of these? Within the political will, new methodologies merge (informal information, fact-checking), where fact and opinion become mixed.

To sum up, all these changes represent a considerable challenge for the logic of constitutionalism in terms of legitimacy. This is why I can ask what the concrete manifestations are today of living in democratic spaces mediated by technology. In the spaces of discourse, which ones can be characterised as spaces of civic interaction and as spaces of political intervention? The control of access to resources

[24] F. Dallmayr, 'The discourse of modernity: Hegel and Habermas' (1987) 84 *The Journal of Philosophy* 11, 682–92.

and communications platforms indeed has considerable power to (re)configure discourses, and the answers to these questions are crucial. We should not forget the unequal distribution of the potential associated with such technologies, and the specific state of the virtual public sphere also distorts intercultural dialogue. In other words, virtual social networks can limit and distort the dialogue between cultures because of the virtual public sphere they create. That is one of the reasons I am in favour of encouraging the public financing of online communications so that they are not co-opted by commercial interests. Cultivating a will towards civic participation in society, keeping non-profits involved so that access remains affordable, is essential to democracy and the protection of fundamental rights. A virtual self-government by 'cyberians' is highly problematic, since the real world, through the state, is the only institutional structure that seems able to fulfil the important and irreplaceable task of promoting social and political integration that forms the collective identity (the formula that contains in itself the ideas of common interest and community). In this sense, there are several discussions, namely about 'echo chambers', specific platforms created by political parties, parliamentary decisions via AI, possible uses of AI for the realisation of social rights, and so on.

It is clear that the new regulations have to address one basic distinction: the exercise of democracy through the internet and the exercise of democracy on the internet. In the former, cyber-attacks, namely from authoritarian governments and non-state actors, pose a clear and increasing threat to democracies across the world, especially through their interference in free and fair elections (we must keep in mind that there is state influence on the internet by some states and international legal protection from that interference), and the manipulation of information sources for political discourse and decision-making. In the latter scenario, besides considering the rule of law, a new premise for democracy itself arises as technology becomes an integral part of a truly democratic global society. Indeed, in this new scenario, democracy itself and its realisation involves monitoring strategies that deal with the asymmetry of information and imbalance of power. Of course, an appropriate approach in confronting and criticising government power, a logical and rational critique of political, economic, social, and cultural issues, bilateral dialogue, and free audience (all) with government officials can help.

Good governance theory advocates the responsible, accountable, and transparent management of human, financial, economic, and natural resources for the sustainable and equitable development of all institutions. First of all, this requires the government to be accountable for its actions by implying transparency and access to information for its citizens. Governments also need to be responsive to people's needs by exhibiting responsiveness and safeguarding human rights, in order to achieve public trust. On the other hand, public authorities must use common-sense at the core of their speeches, embedded in an overall togetherness narrative. This will lead to mutual agreement, pragmatic rationality, and cooperative compliance from citizens. Building a common public culture is essential for trust in public

affairs. Otherwise, we experience the division of society into parallel societies with little to no intergroup trust and the risk of mutual suspicion.

With the digitalisation of the public environment, it is not only the state and public authorities that can be a threat to our rights, but also private entities. That was the idea in the birth of fundamental rights in the eighteenth century. Today, the threat can come from both sides, but that is a completely different question and it is not addressed in this chapter.

This is, I believe, the core provided by the legal frameworks of public and private law. They follow different rationales. Private law allows actors to act solely in pursuit of their self-interest, whereas public law requires a higher standard, often referred to as the pursuit of a common interest. The public character of an act or behaviour thus derives from its relation to that common interest. It depends on the social sphere from which it originates. If the activity is part of the sphere where self-interest is a sufficient justification, the act is private; if it belongs to the sphere where common interests are predominant, it is public.

In times of crisis, such as the COVID-19 pandemic, citizen trust in the system is one of the central features ensuring citizen compliance and the functioning of a democratic society, which includes the role of democracy and how citizens assess its performance. That evaluation also comes from the published discourse. We cannot forget that it was that public discourse that associated the use of apps with surveillance, questioning whether these measures are 'typically' European.

13.5 CONCLUSION

It is time to conclude. From all that has been written, it is clear that I believe that trust, regulation, redefining the rule of law, and the role of the state are crucial factors in overcoming the general perception of the loss of rights. That perception has developed since the beginning of digitalisation and was particularly clear during the experience of contact tracking to control COVID-19. That is why I believe this represents a new set of challenges in the art of the law. It is important to keep in mind that we have online and offline rights, national and international orders, and states that will not give up their roles, and, last but not least, citizens who have claims relating to privacy and also protection and security.