This is the Accepted Manuscript version of

Edoardo Celeste, Dennis Redeker and Mauro Santaniello, 'Anchoring Digital Rights: Digital Constitutionalism in Hard Times' in Claudia Padovani, Véronique Wavre, Arne Hintz, Gerard Goggin, Petros Iosifidis (eds), Global Communication Governance at the Crossroads (Springer 2024), 217-237

CHAPTER 13

Anchoring Digital Rights: Digital Constitutionalism in Hard Times

Edoardo Celeste, Dennis Redeker and Mauro Santaniello

Edoardo Celeste
School of Law and Government, Dublin City University, Ireland
edoardo.celeste@dcu.ie

Dennis Redeker
Centre for Media, Communication and Information Research (ZeMKI), University of Bremen, Germany
redeker@uni-bremen.de

Mauro Santaniello
Internet & Communication Policy Center (ICPC), University of Salerno, Italy
msantaniello@unisa.it

Acknowledgments: Dennis Redeker would like to acknowledge the support for this project by the Center for Advanced Internet Studies (CAIS) through a residential fellowship in 2021. Mauro Santaniello would like to acknowledge the support for this research by the Italian Ministry for Education, University and Research (MIUR) through the grant PRIN 2017RFS2JY in 2021.

The COVID-19 (Coronavirus SARS-CoV-2) pandemic that began in 2019 has been devastating to individuals and communities around the world: hundreds of millions have tested positive to the disease, and millions have unfortunately died from it (WHO, 2022). The ongoing global COVID-19 pandemic has further intensified the role of digital communication technologies, particularly the Internet, in education, social life, politics and commerce. This, in turn, has further boosted the attention that states, civil society and media pay to the Internet and its regulation due to the even more crucial role it plays in society. Early on in the pandemic, and starting in March and April 2020, academics and commentators raised privacy, data protection and surveillance issues with regard to technologies deployed to learn about the spread of the virus or to "track and trace" those who may have contracted it (see e.g. Ahn, Park, Lee, & Hong, 2020; Buckee et al., 2020). State policy responses proliferated around the world with an unprecedented speed across domains, including the regulation of digital services and the Internet (Buthe, Messerschmidt, & Cheng, 2020; Cheng, Barceló, Hartnett, Kubinec, & Messerschmidt, 2020). Ways to track and trace the

virus in societies were quickly followed by other policy areas in which fundamental rights on the Internet are affected, particularly the regulation of disinformation on social media.

Nations states were not the only entities responding to the COVID-19 pandemic. Most large social media platforms have taken steps against COVID-19 related misinformation and reported on these steps against the background of the increasing pressure to do so (European Commission, 2020c). In addition, Google and Apple have cooperated with device and software solutions to create the "Exposure Notification system" that allows for government-sponsored and private sector applications to run contact tracing using Bluetooth in order to gauge and register distances between devices. These regulatory and technological advances came not without their own caveats for human rights, and in particular for that sub-set of fundamental rights that are related to the digital dimension and that in this paper we call 'digital rights'.

Some crucial digital rights, including those that have in recent years seen better protection such as *privacy*, the *right to access to the Internet* and *freedom of expression,* were deeply impacted by countermeasures to the Covid 19 pandemic. Privacy and freedom of expression are identified in the Universal Declaration of Human Rights (UDHR), while access to the Internet is often argued to be a fundamental right and instrumental for the enjoyment of a range of other human rights (see e.g. IRPC, 2018; Tully, 2014). Hard limitations to the exercise of these rights occurred in different forms in different regions of the world, and, above all during the first global wave of the pandemic, in the first half of 2020, they were largely accepted by populations. However, in several countries, as we will argue later in this chapter, several forces emerged to counteract and limit these restrictions, and to preserve digital rights through several techniques.

We argue with Murphy (2014) that the above processes, caused by exogenous events, can be conceived of as swings of a pendulum between increased control and surveillance on the one side and enhanced fundamental rights protection on the other. Murphy considers exogenous events, such as the 9/11 terror attacks or the Snowden revelations, as having long-lasting effects on civil rights across jurisdictions and causing "the pendulum to swing" in one direction or another. Once a swing of the pendulum has occurred, it does require time and/or additional exogenous events to move it back against the force of inertia. For instance, in the case of the 9/11 terror attacks, policy responses such as the US Patriot Act have swung the pendulum in the direction of surveillance. In the case of the Snowden revelations, we have witnessed a global awakening of civil society and the public concerning large-scale surveillance operations conducted by Western intelligence agencies (in part caused by the post 9/11 legal and policy reactions), even if this attention has largely *not* been translated into privacy-enhancing policies (cf. Pohle & Van Audenhove, 2017). This shows that indeed social forces play a significant role in fostering debates about fundamental rights and freedoms. In particular, in this chapter, we consider the current pandemic as an exogenous event that caused a full swing toward digital control and surveillance, with (social) forces simultaneously pulling the pendulum towards stronger digital rights protection.

This chapter aims to analyze these forces, which, against the pressure of the pandemic, work to keep the pendulum in place, restoring a position of equilibrium between surveillance trends and digital rights protection. We examine the law, and in particular the process of constitutionalization of digital rights (section 2), civil society actors working against infringements of human rights on the Internet resulting from the shock of the pandemic (section 3), and the political shaping of technological design during the first phase of the global health crisis (section 4). Specifically, we consider these elements as three separate – but at times interrelated – "ratchet

effects" that help sustain the emergent rights-based order the Internet, as visually represented in the diagram below.

THE CONSTITUTIONALIZATION OF DIGITAL RIGHTS

In 1955, Italian jurist Piero Calamandrei, in a speech on the newborn Italian Constitution, compared individual freedom with air: it is when one starts feeling the lack of air that one perceives its importance for human life (Calamandrei 1955). Similarly, in the current times of Covid-19 pandemic, generations of people have experienced for the first time an unprecedented restriction of individual freedoms. It is precisely in these hard times, when freedoms once given for granted are affected by emergency measures, that we realize the importance of our fundamental rights. If on the one hand, the 'pendulum' effect that we described in the introduction has certainly chilling consequences on individual rights - in the name of public health, many governments indeed imposed unprecedented restrictions - on the other hand, exogenous events such as the global pandemic we are living can also lead to the emergence of constitutional counteractions (Celeste 2019). The sense of hitting rock bottom from a fundamental right perspective may generate or reinvigorate trends pushing towards a reaffirmation of constitutional guarantees. It is exactly at this moment - indeed in a 'constitutional moment' we could say (Celeste 2019) - that the idea of (re)anchoring rights, especially digital rights, which are among the most affected in a time where our physical life has turned digital, finds new vigor. Identifying a way of safeguarding them in a legal environment that is put under stress by at first sight most pressing exigencies, such as the need of protecting public health, becomes one of the main objectives of the constant rights balancing exercise which characterizes modern constitutional systems.

A first way in which this reverse pendulum effect manifests itself is through a process of constitutionalization of digital rights. The legal scholarship has used the notion of 'constitutionalization' with a variety of different meanings (see Kleinlein 2012). This term has been referred to as the process of acquisition of constitutional relevance by a specific principle, circumstance or object (Azzariti 2011; Amoretti & Gargiulo 2010). It has been considered as a synonym of codification when constitutional norms were involved (Brown 2012), or has also been intended as the process of introduction of constitutional values and principles in a dimension which formerly did not possess them (O'Donoghue 2014; Wiener et al. 2012). There is certainly some overlap among these interpretations of the concept of constitutionalization, however the last one definitively appears to be the broadest of the three and well-fitting the current phenomenon involving digital rights.

The virtual ecosystem does not represent an independent realm, the "new home of Mind" (Barlow 1996), subject to its own rules and escaping the laws of the physical world. Our digital and physical lives can no longer be regarded as two separate silos (Dowek 2017). Especially the current pandemic has shown to what extent these two dimensions are interrelated. Our existence seamlessly overtakes the boundaries of the digital world to exercise a plurality of everyday activities, including basic fundamental rights, such as the right to freely communicate, access knowledge, organize protests and assemblies, and profess our political or religious faith. However, if on the one hand, the cyberlibertarian idea of legal independence of cyberspace has been debunked, on the other hand, envisaging an unchallenging extension of existing constitutional law to the digital environment is naïf. State constitutional architectures currently in place have been framed for an analogue ecosystem. The digital revolution is challenging existing constitutional

rules: some of them need to be stretched to guide the virtual society, others need to be reinterpreted and adapted to newly emerging needs. Constitutional law, although set to define the long-term leading principles of a society and to last for longer periods of time than ordinary law, is not set in stone. Constitutional law has constantly evolved to reflect societal evolutions. In this way, constitutional texts have progressively incorporated new rights that emerged after scientific and industrial revolutions, wars and civil protests. So, the constitutional ecosystem is gradually changing under the pressure of the digital revolution, too.

The core principles of contemporary constitutionalism are extended, generalized, adapted, translated and rearticulated to address the challenges of the digital society (Celeste 2019; Teubner 2012). In this way, for example, the scope of classic rights such as freedom of expression, freedom and secrecy of correspondence, freedom of association and assembly is widened to encompass human actions in the virtual world (Celeste 2022). Core constitutional values like non-discrimination, the protection of individual privacy, and due process acquire new meanings, supporting the emergence of novel principles such as net neutrality, the prohibition of mass surveillance and due process in the context of online content moderation performed by private platforms (Suzor 2019; Celeste 2022). Even new rights specifically targeting the digital society emerge, such as the right to Internet access, data protection and e-democracy (Celeste 2022). In this sense, one can denote this ongoing phenomenon as constitutionalization: in the digital society, traditional constitutional principles struggle to apply, and are therefore gradually adapted, translated and instilled in a novel form.

What is important to highlight is that such a phenomenon of constitutionalization does not necessarily imply a revolution of contemporary constitutionalism (Celeste 2019). The extent of change prompted by the digital revolution in the constitutional arena is so evident that the scholarship has talked of the emergence of a 'digital constitutionalism', using an expression akin to 'democratic constitutionalism' or 'liberal constitutionalism' (see Redeker et al. 2018; Padovani and Santaniello 2018; Celeste 2019). However, digital constitutionalism does not denote a new form of constitutionalism. The adjective 'digital' rather denotes the context where constitutionalism aims to apply. Digital constitutionalism can be regarded as a strand of contemporary constitutionalism seeking to address the challenges of the digital revolution (Celeste 2019). As previously said, constitutional law has always evolved. Therefore, constitutional provisions may change in the digital society, but the DNA of contemporary constitutionalism remains preserved (Celeste 2022). Digital constitutionalism indeed emerges as the ideology advocating for the perpetuation of foundational principles of contemporary constitutionalism, such as the rule of law, the separation of powers, democracy and the protection of human rights, in the mutated scenario of the digital society. Digital constitutionalism provides the set of values and principles that are currently informing the process of constitutionalization of digital rights.

The process of constitutionalization of the digital society, however, has not to be merely intended as a progressive codification of digital rights into state constitutions. One has generally the tendency to associate the notion of constitutions to the state dimension, and consequently the process of constitutionalization to the idea of legal codification. Yet, in the global digital society, multinational online platforms emerge besides nation states as new dominant actors; the notion of citizenship is no longer central in a digital environment where users can be simultaneously subject to different rules adopted by public and private actors (Suzor 2019). The existing scholarship on the notion of digital constitutionalism has made it clear that the process of constitutionalization of the digital society involves a plurality of simultaneous responses from different actors. Digital

rights considerations progressively emerge in state (constitutional and ordinary) law as well as in the rules of private actors, in decisions of national judges and private supervisory bodies, in institutionalized discussions involving national and supranational parliaments as well as in civil society groups' deliberations and initiatives (Fitzgerald 2000; Suzor 2010; Karavas 2010; Redeker et al. 2018; Santaniello et al. 2018; Celeste 2019; 2022). The process of constitutionalization is not uniform or unitary, but has to be necessarily fragmented to act on the multiple layers of the global digital society (Celeste 2021). New constitutional norms addressing the challenges of the digital society are emerging not only in the form of new legal provisions in state constitutions, in the internal rules of online private companies, in the case law of public and private judges; but also, as the next two sections will illustrate, they may ferment in multifarious political initiatives at the level of civil society, and be instilled in the 'code' of new digital technology instruments.

TRANSNATIONAL DIGITAL RIGHTS ACTIVISTS

The constitutionalization of the digital environment is not proceeding at random. Among other forces, it is driven by actors who consciously advocate for a better protection of digital rights. Digital rights activists, who are in the trade (or vocation) of protecting fundamental rights through their advocacy, research and outreach, were surprised as much as everyone else by the fast-approaching global pandemic, its scale and its persistence. They clearly saw the forces that would affect the pendulum to swing into the direction of more control and surveillance, rather than more digital rights protection. However, akin to a first-responder, digital rights activists were alert immediately, expecting the pandemic to be highly relevant to their work. Civil society representatives feared for the pandemic to un-do their successes in digital rights protection and hasten the rise of the state in the Internet policy field. The sense of alert is well-captured by a statement made by Estelle Massé of the non-governmental organization (NGO) Access Now cautioning that "while resources for public health are scarce, governments around the world should not see this health crisis as an opportunity to invest in controversial technology and systems for surveillance" (Manancourt 2020). The Digital Freedom Fund published a statement warning that "oppressive regimes are rapidly adopting 'fake news' laws [...] ostensibly to curb the spread of misinformation about the virus, but in practice, this legislation is often used to crack down on dissenting voices or otherwise suppress free speech" (Reventlow 2020). As the pandemic spread globally, digital rights activists consciously fought to be a ratchet that keeps rights in place.

Throughout the pandemic, with more people being dependent on digital technologies than ever before - for work and schooling or to find information about the virus - digital rights activists advocated for rights-based approaches with regard to a variety of public policies. For instance, Privacy International started a new dossier "Tracking the Global Response to COVID-19" dedicated to state and corporate policies related to the pandemic, demonstrating the large number of policy proposals and some of their implications for privacy and other rights. For the purposes of this chapter, transnational rights activists are defined as non-state, non-profit actors who engage in advocacy across borders in the field of digital rights. These activists are either organized in formalized NGOs or they act as individuals and may or may not see themselves as part of a larger transnational advocacy network in the digital rights field. In these networks, other actors may be involved, too. Arguably. Media organizations, international organizations such as the Council of Europe or UNESCO, a number of government agencies and some companies have an interest in a rights-based approach to digital governance.

In 2020 and 2021, like many people around the world, NGO staff and individual activists often worked remotely to promote their agenda. Unlike other groups - such as staff in government ministries however, digital rights activists strongly rely on a large transnational network of collaborators, who engage in a frequent exchange of information and support each other across borders. This is particularly important where organized civil society is relatively small on a national level; in these cases, knowledge sharing across borders is vital to effective advocacy. Transnational networks of activists also often coordinate their campaigns in order to be more effective at shaming governments on account of their human rights record with the help of their international collaborators (Murdie & Davies 2012). This "boomerang effect" of transnational advocacy networks, first described by Keck and Sikkink (1998), requires effective networking and communications, made possible in recent decades by regular physical meetings of activists. One of the potential futures for digital rights activists was that the pandemic could weaken these networks and make cooperation at scale more difficult.

RightsCon and the global Internet Governance Forum (IGF) are arguably the two most important fora for exchange among transnational digital rights activists. Both are regular events that had to be moved online for the first time. They usually depend on an intermingling of people irrespective of their national origin and an exchange with other stakeholder groups such as state and corporate representatives, academics and technical experts. Indeed, RightsCon took place remotely in 2020 and 2021. Access Now, which organizes the annual meeting, states on their website the number of participants of both the physical meetings in 2019 and before, and the meetings of 2020 and 2021. On the outset, going digital has been a success in terms of total number of participants. While in 2018 and 2019, 2,520 and 2,797 showed up in Toronto, Canada and Tunis, Tunisia respectively, the number rose to 7,681 in 2020 and further to 9,120 in 2021 (Access Now 2018; 2019; 2020; 2021). Additionally, the burden to be part of a meeting even as an NGO in a low-income country has been significantly lowered through fully moving it online. The online platform utilized by Access Now allowed for some interaction and random mingling. However, the level of engagement of the average participant is likely lower than that of someone traveling to the conference, spending days in a physical space with like-minded activists. Nonetheless, the organizers took the experience of 2020 and 2021 as a justification to move the conference series online, at least for 2022 (Access Now 2021).

The IGF, a United Nations-initiated project, similarly had to transition to a fully remote mode in 2020, a fact that has affected the number and distribution of participants. After 3,679 participants attended the IGF on-site in Berlin in 2019, the number of registered participants connecting remotely a year later stood at 6,150 (Internet Governance Forum 2020; 2021). Compared to the year before, more people indicated that they are newcomers to the IGF (59% compared to 53%), and that they were female (47% compared to 42%). Most notably, the share of "Western European and Others" participants was significantly lower in 2020 (35% compared to 55% in 2019), causing the overall distribution between regions to be more balanced. The share of civil society participants relative to other stakeholder groups remained relatively constant (42% compared to 39% in 2019). The 2021 iteration of the IGF was held as a hybrid event with more than 2,700 participants attending the conference in Katowice in person of 10,371 who were registered (Internet Governance Forum 2022). Here, too, the boost of online participation can be considered to be an effect of the pandemic. However, other meetings, which are known to be important gatherings for transnational digital rights activists have been canceled in 2020, including the Internet Freedom Festival and the Forum on Internet Freedom in Africa (FIFAfrica).

These convenings represent a fertile ground not just for coordination on logistical matters but also places where rights and principles for the Internet are being debated intellectually. The IGF and similar conferences have given rise to a number of so-called Internet bill of rights documents (cf. Celeste 2019; Redeker et al. 2018), which in turn are contributing to the constitutionalization of digital rights, e.g. through adoption and discussion of documents such as the Charter of Human Rights and Principles for the Internet (at IGF 2009), Marco Civil da Internet (at IGF 2015) or the Toronto Declaration (at RightsCon 2018). Digital rights activists present and debate these principled documents regularly with their peers, potentially creating inspiration for the next document or translating a document to the national or regional level. They also communicate their normative priorities to corporations, state representatives, international organizations, those involved in the technical development of the Internet, and the media. From this transnational context, national and regional initiatives of Internet bills of rights like the Italian Declaration of Internet Rights or the EU's Lisbon Declaration of 2021 look like a piece of the puzzle rather than a disparate intervention. Acknowledging the pandemic, the latter specifically states that "digital tools have effectively lessened the negative impacts of the pandemic, while exacerbating the existing disparities" (portugal.eu 2021).

For new rights to be entrenched into the multiple layers of the constitutional order of the Internet, which can occur in a variety of ways as outlined previously, digital rights activists play an important role in scandalizing the effects of modern technologies on fundamental rights. Recent examples include the pinpointing of specific risks to digital rights in the wake of discussions about a digital vaccine passports, with activists arguing that current policy proposal "threaten human rights by creating space for exclusion and discrimination to flourish, and posing serious long-term threats to the privacy and security of millions of people across the globe" (Access Now 2021). More recently, strategic litigation in the digital rights field has proliferated, partly inspired by a case bringing down of the International Safe Harbor Privacy Principles between the US and the EU instigated by Maximillian Schrems, an individual litigant. These legal actions are also based on scandalizations that "bring out truths and historical responsibilities or to raise debate and scandal, thus generating significant learning pressures on political and functional systems" (Golia & Teubner 2021: 19), including in the case of the Safe Harbor decision, the scandalizations around the Snowden revelations about widespread spying on ordinary (EU) citizens.

Scandalization requires attention from the (global) audience, which it appears has not vanished during the pandemic. In fact, based on the interviews with digital rights groups conducted in late 2020, one might even think that the opposite may be the case, particularly in the early months of the Covid-19 pandemic. Internet access quickly became a lifeline for people around the world to learn about the pandemic and precautions against the virus, specifically with regard to vulnerable groups (see Cyberlaw Clinic et al. 2021). A representative of the KeepItOn campaign, working against Internet shutdowns and slowdowns globally remarked that their campaign was "vindicated" by the and gained attention and support due to the pandemic's impact on the right to access to the Internet (interview, October 2020). A similar attitude was uttered by a senior member of the Internet Rights and Principles Coalition, which authored the Charter of Human Rights and Principles for the Internet: Reflecting on the impact of the pandemic on the work of the Coalition, she stressed that an increasing number of citizens and activists were requesting the information and support from the Coalition, which they were - while pleased about the attention - in fact not yet able to provide (interview, October 2020). In sum, transnational digital rights activism itself has not been as starkly affected by the pandemic as the limitation on in-person exchange and advocacy could have meant. Consequently, like the developing legal constitutional safeguards in

place, digital rights activism represents a ratchet against a swing of the pendulum toward more control and surveillance of the digital society.

DIGITAL ARCHITECTURES

For a long time, the Internet has been considered as an architecture of freedom *per se*, a tool that would have promoted free speech, democracy, and grass-root participation all over the world. That belief was mostly grounded on the idea that the basic features of that network - decentralization, openness, anonymity - would have resisted any attempts of top-down control and manipulation. However, during the 1990s it became more and more evident that those early features were not natural properties of the Internet's architecture, and that they could be changed in order to serve different political aims.

It is currently commonplace that the Internet has no nature, and that it is shaped by social forces. Also, it is clear enough that the early design of the Internet has been changed towards a more centralized, bordered, and monitored architecture. These transformations have allowed state actors to exploit the Internet for the exercise of a tighter control over digital communications inside and outside their own borders, and private companies to develop new business models based on user's surveillance and content commodification (Zuboff 2018). During the last two decades, several studies have highlighted the crucial role of the Internet architecture in defining constraints and opportunities for enhancing and protecting human rights online. Extremely summarizing scholarly contributions from legal, political and communication research, we can say that code is law (Lessig 1999), protocols have politics (DeNardis 2009), and design is normative (Brown & Marsden 2013). Indeed, decisions made about Internet design have a political nature, since they are the outcome of human interactions which are influenced by the interests, visions and beliefs of people involved in the designing process. Also, these decisions usually embed political values into the Internet architecture, which in turn affects societies relying on digital networks (DeNardis 2013:10). Whether the embedded values have to do with human rights protection and democratic principles or do they prioritize security and societal control depends on the political action of multiple actors involved in the technical configuration of digital architectures.

Thus, how can the design of the networks be used as an anchor, or ratchet, for the safeguarding of human rights in the digital realm? A way to use the Internet architecture - meant as the ensemble of standards, protocols, data exchange facilities, and telecommunication infrastructures - in order to protect human rights is to build and maintain technologies based on design philosophies and principles that emphasize user's freedom and control over data, or that make monitoring and manipulating activities more difficult to achieve. This may be the case of peer-to-peer networks, encrypted communications, distributed data storage, open source software, anonymizing tools, and alike. A dazzling example of these *designs of freedom* is provided by Signal, a messaging service launched in 2015. Signal is an open source application that does not collect neither data nor metadata from the user, thus turning away from business models that monetize these kinds of information. More importantly, Signal was the first messaging application using end-to-end encryption for both instant one-to-one messages and group chat, a feature that was soon adopted also by other popular messaging service providers such as Facebook Messenger, WhatsApp and Zoom. Other relevant examples of architectures protecting users' rights are those peer-to-peer platforms embedding privacy-by-design features into their functioning (Musiani 2013, 2014). Protecting digital rights by technical configurations can also be achieved by

redesigning existing technologies and standards to face weaknesses or architectural features exploited by human rights violators. This is the path followed, for example, by the Internet Engineering Task Force (IETF) after Snowden's revelations about electronic mass-surveillance activities led by the US government and its Five Eyes allies. Consequently, in August 2018 the IETF adopted a new version of the Transport Layer Security (TLS) standard in the attempt to "prevent the kind of mass surveillance that Snowden exposed" (Kiernan & Mueller 2021).

On the other hand, a number of problems affecting the possibility to instantiate human rights in Internet standards and protocols have been identified, including technical feasibility, local differences about which rights are worthy of protection and with what priority, legitimacy of standard-setting organizations in defining the agenda of digital rights at the global level, ambiguity about definitions of rights vis-a-vis the necessity to clearly operationalize them in order to be encoded into the Internet design, the absence of strict obligations for non-state actors in protecting human rights, and the risk of fragmentation resulting from different normative approaches to Internet governance (Cath & Floridi 2017; Mueller & Badiei 2018). Furthermore, having human rights considerations while developing Internet standards and architectures entails long and time-consuming deliberative processes, which can be out of sync during crises and emergency situations. Predicaments such as economic crises, terror attacks and - as in this case - pandemics may force institutions and politicians to critically look at digital technologies in order to find rapid solutions and reliable instruments to mitigate risks and losses, following an approach defined as "technological solutionism" (Morozov 2013). However, during the Covid-19 pandemic, legal constraints and advocacy activities, such as those illustrated in the previous sections, have proved to be effective in keeping the pendulum on the digital rights' side. This is the case of contact tracing apps rapidly developed and adopted in many countries with the aim to hinder the outbreak of Covid-19 through proximity detection, exposure risk calculation and infection alert. In order to work in a proper and effective manner, these apps must collect data about the users' movements, the people they meet, the duration of the encounters, as well as health conditions of people involved. Even though this unprecedented collection of personal data and sensitive information was justified by the need to preserve both individual and collective safety, it was globally accompanied by considerations about privacy and possible abuses by governments and private companies. Particularly in Europe, the design of these apps was flanked - and somehow shaped - by both legal constraints and civil society campaigning. The EU General Data Protection Regulation (GDPR) provides a strong normative framework with its principles of lawfulness, fairness, transparency, purpose limitation, data minimization, storage limitation, accuracy, integrity, confidentiality and accountability. On April 8, 2020, the EU Commission issued a recommendation concerning mobile applications for Coronavirus tracking, asking all member states to ensure that these apps were compliant with "the right to privacy and the protection of personal data along with other rights and freedoms enshrined in the Charter of Fundamental Rights of the Union" (European Commission 2020a). Also, the Commission provided an official "Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection", with a set of technical requirements inspired by the provisions of the GDPR (European Commission 2020b).

Other pushes towards compliance with personal data protection came from the private sector as well as the civil society. On April 10, 2020, Apple and Google, the two companies that hold a de facto duopoly over mobile operative systems (iOS and Android, respectively) announced a joint effort to provide developers of contact tracing apps with an API to interact with their

software[1]. The two companies made clear that only privacy-preserving and decentralized solutions would have been supported by their systems. This pushed some developers to change their original plans for centralized data storage, like it happened in Italy with the app Immuni. Also, a comparative research project on Covid-19 apps developed all over the world shows that "platforms have responded to the global pandemic and infodemic with additional extraordinary measures to demarcate public interest niches from the wider commercial environment of the app store" (Dieter et al. 2021, p. 24). Another important contribution towards privacy-friendly solutions came from the global academic community. On April 19, 2020, more than 300 scientists in over 25 countries issued an open letter to ask governments to adopt open, transparent, decentralized and privacy-by-design contact tracing apps[2].

Retrospectively, all the efforts to keep these apps in line with fundamental rights' protection were, at least partially, successful. Indeed, most contact tracing apps in use in the world have been built taking into serious consideration both institutional recommendations and concerns by digital rights activists and private companies. The great majority of them rely on Bluetooth instead of the more invasive GPS, their source code is open, and they usually store data on the user device instead of a central server. Also, their adoption is voluntary and their functioning has been audited, approved and monitored by data protection authorities. Of course, this is not an universal condition, and centralized systems have been deployed in both democratic and non-democratic countries[3]. Also, looking at the bigger picture about the relationships between the pandemic and electronic surveillance, David Lyon (2022) has raised two crucial concerns. The first one relates to the fact that contact tracing apps rely on the massive use of smartphones, which are "the key component of contemporary surveillance systems" (Lyon 2022: 33). The second concern is that states' responses to the pandemic have both legitimized the extensive use of a broader set of surveillance technologies - such as vaccine passports, thermal cameras, facial recognition systems, drones, etc. - and have widened the scope of surveillance beyond the public space, bringing it into the domestic environment by means of smart working, school at home, and online shopping. Further, looking at the near future, several emerging technologies such as artificial intelligence, the Internet of Things, advanced robotics, 5G and quantum computing present numerous challenges to the protection of digital rights. On the one hand, they reshape the design principles of digital networks, often embedding in their architecture political values which are substantially different from the constitutional tradition of liberal democracies. On the other hand, these technologies bring digital networks closer and closer to the human body, enabling an unprecedented set of consequences for users and even for disconnected people. This process of materialization of the digital experience comes with new threats to fundamental rights, and requires an attentive - and expensive - oversight over their designing process in order to keep it in line with democratic values and principles.

CONCLUSION

[1] See Google's announcement, https://www.blog.google/inside-google/company-announcements/apple-and-google-partner-covid-19-contact-tracing-technology/, and Apple's announcement, https://covid19.apple.com/contacttracing.
[2] The Joint Statement on Contact Tracing can be accessed at https://drive.google.com/file/d/1OQg2dxPu-x-RZzETlpV3lFa259Nrpk1J/view
[3] Examples of democratic countries adopting centralized contact tracing systems are South Korea, Israel, Australia and Canada. The most discussed case of a centralized system is the Chinese Health Code.

During the ongoing global health crisis, the pendulum is oscillating again between compression and enhanced protection of fundamental rights. On the one hand, we have witnessed a higher risk of compressing fundamental rights, and in particular those rights which are most related to the digital environment where our lives have transitioned in these times of pandemic. And on the other hand, this enhanced risk - be it factual or merely potential - has triggered a consistent response favoring a bolder definition and affirmation of digital rights, what we have called a process of 'constitutionalization' of digital rights. Paradoxically, therefore, the storm we are living in is helping us anchor fundamental rights better than before. This chapter has analyzed three societal agents and layers that prompt this change. First of all, we have recognized that the law is evolving. Particularly, constitutional law, which was framed to tackle the challenges of an analogue society, is currently evolving to address the issues of the digital ecosystem. However, given the global nature of the Internet and its players, nation state legislators and judges cannot alone define the principles that will govern the digital society. The core principles of contemporary constitutionalism are progressively translated into the digital context by a plurality of actors, including civil society activists and computer scientists. The first group, indeed, is free to promote innovative ways of interpreting core constitutional principles in a way that better addresses societal needs, without fear of being subject to corporate objectives or being caged by national political demands. Computer scientists, and technicians more in general, have in turn the power to forge the code, which acts as law in action, sometimes even before law is even officially adopted. Then, they can play a fundamental role in anticipating legislative changes by instilling new principles advocated by digital rights activists in the code of new digital technology products and services.

The multiplicity of governance processes we have identified in this chapter renders the complexity of current global media policy as a policy domain (Raboy & Padovani 2010). Indeed, the great variety of actors, issues, and venues that interact in defining, establishing and protecting digital rights testify a non-linear, and often confusing, articulation of policy processes which assembles lawmakers, activists and engineers, as well as scholars from diverse disciplines, private companies, the media, and individual persons. It is the political action of all these actors that will be decisive in fastening the pendulum on one side or the other. Given the process of digital convergence, moreover, the question about which side of the pendulum will prevail assumes a crucial relevance in shaping the future of human communication as a whole. From this perspective, those digital rights which will be enshrined in digital constitutionalization processes are likely to serve also as guidelines and normative frameworks for emerging technologies in the near future. In this sense, the pendulum turns into a crossroads as the pandemic, and policies adopted to face it, make evident the difference between two forking paths. One leaning towards a more controlled and centralized digital environment where security is prioritized over individual rights and democratic principles. The other is heading towards a constitutionalized digital environment.

REFERENCES

Access Now (2018). RightsCon Toronto 2018. Retrieved from: https://www.rightscon.org/past-events/toronto-2018/

Access Now (2019). RightsCon Tunis 2019. Retrieved from: https://www.rightscon.org/past-events/tunis-2019/

Access Now (2020). RightsCon Online 2020. Retrieved from https://www.rightscon.org/past-events/online-2020/

Access Now (2021). Protocol for exclusion: why COVID-19 vaccine "passports" threaten human rights. Retrieved from: https://www.accessnow.org/covid-19-vaccine-passports-threaten-human-rights/

Access Now (2021). Save the date for RightsCon: June 6-10, 2022. Retrieved from https://www.rightscon.org/save-the-date-for-rightscon-june-6-10-2022/

Ahn, N.-Y., Park, J. E., Lee, D. H., & Hong, P. C. (2020). Balancing Personal Privacy and Public Safety in COVID-19: Case of Korea and France. *arXiv preprint arXiv:2004.14495*.

Amoretti, F., & Gargiulo, E. (2010). Dall'appartenenza Materiale All'appartenenza Virtuale? La Cittadinanza Elettronica Fra Processi Di Costituzionalizzazione Della Rete e Dinamiche Di Esclusione. *Politica Del Diritto, 3,* 353–90. https://doi.org/10.1437/32851.

Azzariti, G. (2011). Internet e Costituzione. *Politica Del Diritto, 3*, 367–78. https://doi.org/10.1437/36045.

Barlow, J. P. (1996). *A Declaration of the Independence of Cyberspace*. https://www.eff.org/cyberspace-independence.

Brown, G. W. (2012). The Constitutionalization of What? *Global Constitutionalism 1 (2)*, 201–28. https://doi.org/10.1017/S2045381712000056.

Brown, I. & Marsden C. T. (2013). *Regulating Code: Good Governance and Better Regulation in the Information Age*. Cambridge, MA: MIT.

Buckee, C. O., Balsari, S., Chan, J., Crosas, M., Dominici, F., Gasser, U., . . . Schroeder, A. (2020). Aggregated mobility data could help fight COVID-19. *Science*, eabb8021. doi:10.1126/science.abb8021

Buthe, T., Messerschmidt, L., & Cheng, C. (2020). Policy Responses to the Coronavirus in Germany. *The World Before and After COVID-19: Intellectual Reflections on Politics, Diplomacy and International Relations, edited by Gian Luca Gardini. Stockholm–Salamanca: European Institute of International Relations*.

Calamandrei, P. (1955). *Discorso Sulla Costituzione*. https://www.youtube.com/watch?v=bBKSLvWb7hQ.

Cath, C. & Floridi, F. (2017). The design of the internet's architecture by the Internet Engineering Task Force (IETF) and human rights. *Science and Engineering Ethics 23 (2),* 449–468.

Celeste, E. (2019). Digital Constitutionalism: A New Systematic Theorisation. *International Review of Law, Computers & Technology 33 (1)*, 76–99. https://doi.org/10.1080/13600869.2019.1562604.

Celeste, E. (2022). *Digital Constitutionalism: The Role of Internet Bills of Rights*. New York; Abingdon: Routledge.

Celeste, E. (2021). The Constitutionalisation of the Digital Ecosystem: Lessons from International Law. *Max Planck Institute for Comparative Public Law & International Law (MPIL)* Research Paper No. 2021-16. https://doi.org/10.2139/ssrn.3872818.

Cheng, C., Barceló, J., Hartnett, A. S., Kubinec, R., & Messerschmidt, L. (2020). COVID-19 Government Response Event Dataset (CoronaNet v. 1.0). *Nature Human Behaviour, 4*(7), 756-768.

Harvard Law School Cyberlaw Clinic (2021). Lockdown and Shutdown: Exposing the Impacts of Recent Network Disruptions in Myanmar and Bangladesh. Retrieved from: https://clinic.cyber.harvard.edu/files/2021/01/Lockdowns-and-Shutdowns.pdf

DeNardis, L. (2009). *Protocol politics: the globalization of Internet governance*. Cambridge, MA: MIT.

DeNardis, L. (2013). The Emerging Field of Internet Governance. In Dutton W. H. (Ed.) *The Oxford Handbook of Internet Studies*. Oxford: Oxford University Press.

Dieter, M., Helmond, A., Tkacz, N., van der Vlist, F., Weltevrede, E. (2021). Pandemic platform governance: Mapping the global ecosystem of COVID-19 response apps. *Internet Policy Review, 10(3)*. https://doi.org/10.14763/2021.3.1568

Dowek, G. (2017). *Vivre, aimer, voter en ligne et autres chroniques numériques.* Paris: Le Pommier.

European Commission (2020a). *Commission Recommendation (EU) 2020/518 of 8 April 2020 on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data*. Retrieved from: https://eur-lex.europa.eu/eli/reco/2020/518/oj

European Commission (2020b). *Communication from the Commission Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection* 2020/C 124 I/01. Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020XC0417%2808%29

European Commission (2020c). *First baseline reports – Fighting COVID-19 disinformation Monitoring Programme*. Retrieved from https://ec.europa.eu/digital-single-market/en/news/first-baseline-reports-fighting-covid-19-disinformation-monitoring-programme

Fahey, R. A., & Hino, A. (2020). COVID-19, digital privacy, and the social limits on data-focused public health responses. *International Journal of Information Management*, *55*, 102181.

Fitzgerald, B. (2000). Software as Discourse? The Challenge for Information Law. *European Intellectual Property Review 22 (2)*, 47–55.

Internet Governance Forum (2020). *IGF 2019 Participation and Programme Statistics*. Retrieved from: https://www.intgovforum.org/multilingual/content/igf-2019-participation-and-programme-statistics

Internet Governance Forum (2021). *IGF 2020 Participation and Programme Statistics*. Retrieved from: https://www.intgovforum.org/multilingual/content/igf-2020-participation-and-programme-statistics

Internet Governance Forum (2022). *IGF 2021 Summary Sixteenth Meeting of Internet Governance Forum*, 6–10 December 2021, Katowice, Poland. Retrieved from: https://www.intgovforum.org/en/filedepot_download/223/20706

IRPC (2018). *Charter of Human Rights and Principles on the Internet*. Retrieved from http://internetrightsandprinciples.org/site/wp-content/uploads/2019/09/IRP_booklet_Eng_6ed_4Nov2018.pdf

Karavas, V. (2010). Governance of Virtual Worlds and the Quest for a Digital Constitution. In C. B. Graber and M. Burri-Nenova Eds.) *Governance of Digital Game Environments and Cultural Diversity: Transdisciplinary Enquiries*, 153–69. Cheltenham-Northampton: Edward Elgar Publishing.

Keck, M. E., & Sikkink, K. (1998). *Activists beyond borders*. Ithaca: Cornell University Press.

Kiernan, C., & Mueller, M. (2021). Standardizing Security: Surveillance, Human Rights, and the Battle Over Tls 1.3. *Journal of Information Policy*, 11, 1-25. doi:10.5325/jinfopoli.11.2021.0001

Kleinlein, T. (2012). *Konstitutionalisierung Im Völkerrecht: Konstruktion und Elemente einer Idealistischen Völkerrechtslehre. Beiträge Zum Ausländischen Öffentlichen Recht und Völkerrecht.* Berlin & Heidelberg: Springer.

Lessig, L. (1999). *Code and Other Laws of Cyberspace*. New York: Basic Books.

Lyon D. (2021). *Pandemic Surveillance*. Cambridge, United Kingdom and Medford, MA: Polity.

Manancourt, V. (10 March 2020). Coronavirus tests Europe's resolve on privacy. *Politico*. Retrieved from: https://www.politico.eu/article/coronavirus-tests-europe-resolve-on-privacy-tracking-apps-germany-italy/

Morozov, E. (2013). *To Save Everything, Click Here: The Folly of Technological Solutionism*. PublicAffairs.

Mueller, M., Badiei, F. (2018). Requiem for a Dream: On Advancing Human Rights via Internet Architecture. *Policy & Internet, 11(1)*, 61-83.

Murdie, A. M., & Davis, D. R. (2012). Shaming and blaming: Using events data to assess the impact of human rights INGOs. *International Studies Quarterly*, *56*(1), 1-16.

Murphy, M. H. (2014). The pendulum effect: comparisons between the Snowden revelations and the Church Committee. What are the potential implications for Europe? *Information & Communications Technology Law, 23*(3), 192-219.

Musiani, F. (2013). Network architecture as Internet governance. *Internet Policy Review, 2(4)*. https://doi.org/10.14763/2013.4.208

Musiani, F. (2014). Decentralised internet governance: the case of a 'peer-to-peer cloud'. *Internet Policy Review, 3(1)*. DOI: 10.14763/2014.1.234

O'Donoghue, A. (2014). *Constitutionalism in Global Constitutionalisation*. Cambridge, United Kingdom: Cambridge University Press.

Padovani, C. & Santaniello, M. (2018). Digital Constitutionalism: Fundamental Rights and Power Limitation in the Internet Eco-System. *International Communication Gazette 80 (4)*, 295–301. https://doi.org/10.1177/1748048518757114.

Pohle, J., & Van Audenhove, L. (2017). Post-Snowden internet policy: between public outrage, resistance and policy change. *Media and Communication, 5(1)*, 1-6.

Raboy, M. & Padovani, C. (2010). Mapping Global Media Policy: Concepts, Frameworks, Methods. *Communication, Culture & Critique, 3(2)*, 150-169. https://doi.org/10.1111/j.1753-9137.2010.01064.x

Radu, R. (2020). Fighting the 'Infodemic': Legal Responses to COVID-19 Disinformation. *Social Media+ Society*, *6*(3), https://doi.org/10.1177/2056305120948190.

Redeker, D., Gill, L., Gasser, U. (2018). Towards Digital Constitutionalism? Mapping Attempts to Craft an Internet Bill of Rights. *International Communication Gazette 80 (4),* 302–19. https://doi.org/10.1177/1748048518757121.

Reventlow, N. J. (16 April 2020). Why COVID-19 is a crisis for digital rights. *Digital Freedom Fund*. Retrieved from: https://digitalfreedomfund.org/why-covid-19-is-a-crisis-for-digital-rights/

Suzor, N. (2010). The Role of the Rule of Law in Virtual Communities. *Berkeley Technology Law Journal* 25 (4), 1817–86. https://doi.org/10.15779/Z381M6P.

Suzor, N. (2019). *Lawless. The Secret Rules That Govern Our Digital Lives*. Cambridge: Cambridge University Press.

Teubner, G. (2012). *Constitutional Fragments: Societal Constitutionalism and Globalization*. Oxford: Oxford University Press.

Tully, S. (2014). A human right to access the internet? Problems and prospects. *Human Rights Law Review, 14*(2), 175-195.

WHO. (2021). *WHO Coronavirus Disease (COVID-19) Dashboard*. Retrieved from https://covid19.who.int/

Wiener, A., Lang, A. F., Tully, J., Maduro, M. P., Kumm, M. (2012). Global Constitutionalism: Human Rights, Democracy and the Rule of Law. *Global Constitutionalism* 1 (01): 1–15. https://doi.org/10.1017/S2045381711000098.

Zuboff, S. (2018). *The age of surveillance capitalism: The fight for the future at the new frontier of power*. London: Profile Books.