The Risk of Digitalization: Transforming Government into a Digital Leviathan

JOSÉ VIDA FERNÁNDEZ*

ABSTRACT

This paper provides an overview of the threats posed by digitalization, particularly with regard to the public sector. It starts by describing digital risks as true global risks and argues that their scope and severity have not been recognized until now. The most well-known challenges come from the transformation of the private sector (economy, society, and individuals) and the emergence of large private powers that dominate the digital environment (digital feudal lord). However, there are even greater challenges coming from the digitization of government, creating almighty public bodies detached from laws that kept them locked until now.

I. DIGITALIZATION: A NEW GLOBAL RISK

The unstoppable digital transformation that most countries are undergoing is giving rise to growing concern about the negative effects this process brings. Our society is increasingly dependent on digital technologies (traditionally known as information and communication technologies) that are modifying our activities (economic, social, personal) but which we understand and control less and less. The progressive increase in the relevance of digital technologies in our existence forces us to reflect not only on the advantages, but also on the risks they introduce and how they can pose a threat to our current way of life.

In fact, we can identify a new global risk category: digital risks.

* Professor of Administrative Law, Public Law Department, Universidad Carlos III de Madrid (jose.vida@uc3m.es). This work is part of the research projects "Artificial intelligence in the national health care system: solutions to specific legal problems" (PID2021-128621NB-I00) and "The Impact of Artificial Intelligence in Public Services: A Legal Analysis of its Scope and Consequences in Healthcare" (PGC2018-098243-B-I00) directed by José Vida Fernández and founded by the Ministry of Science and Innovation of Spain (MCIN/AEI/10.13039/501100011033/) and by "FEDER: A way of Making Europe."

Indiana Journal of Global Legal Studies Vol. 30 #1 (Winter 2023)

These are becoming part of the so-called "risk society"[1] insofar as they are risks derived from technological innovation that threaten our existence at a global level. This is similar to what happens with technological developments that lead to other threats such as climate change, epidemics, or terrorism. Thus, those digital risks are not merely threats of information networks and systems addressed by cybersecurity, but have a broader and deeper meaning. Digital risks refer to all transformations resulting from digitalization that can threaten basic aspects of our current life in economic, political, or social terms.

A. Digital Risk: Too Fragile an Acknowledgment

Digital risks are very unique in nature as they do not physically compromise our survival—this can be seen with environmental, health, or security risks. On the contrary, digital risks affect people's rights, political freedom (including the very functioning of democracy), and, ultimately, human dignity, in addition to data privacy and information security.

Thus, digital risks are very distinct and different from traditional global risks because of the object that is threatened. In the case of digital risks (considered as "risks from digital environments") the object to be protected is not the "digital environment" (which would be the source of the risk) but fundamental rights, political freedom, and human dignity, which can be affected in many different ways in digital environments (from violation of privacy, racial or gender discrimination, to social exclusion). Thus, when we speak of "health" or "environmental" risks, the object to be protected can be perceived straightforwardly as it is tangible (population health, natural environment) and an end in itself. On the contrary, in the case of digital risks we find that the object to be protected (fundamental rights and human dignity) is abstract and artificial, and it is not the digital environment that needs to be protected, since it is precisely something that threatens the process.

This unique nature of digital risks makes them more difficult for citizens to identify. It is therefore harder to engage in a public debate on digital risks in order to address them through governance and

1. Risk society is the way our society deals with hazards and insecurities induced and introduced by modernisation itself. *See* ULRICH BECK, RISK SOCIETY: TOWARDS A NEW MODERNITY 50 n.1 (1992) ("In social science's understanding of modernity, the plough, the steam locomotive and the microchip are visible indicators of a much deeper process, which comprises and reshapes the entire social structure."); *see also* ULRICH BECK, WORLD RISK SOCIETY (1999).

regulation. So, there is "too fragile an acknowledgment" of digital risks.[2] It is very difficult to identify digital risks and become aware of them, unlike traditional global risks that can produce physical damages. Conversely, as the complexity of the technological world increases, our understanding of it and of the reality around us decreases.[3] Digital risks are becoming more uncertain, more complex, and, therefore, more difficult to identify.

Even if these digital risks are identified, the fact is that no real harm is perceived to be caused by them. Digital disasters with serious damage on a global scale—such as the NSA's Prism Surveillance system revealed by Edward Snowden or the Cambridge Analytica affair of Facebook[4]—have not provoked a citizens' global mobilization similar to those in defense of the environment or health. These digital scandals have dissolved over time and therefore citizens are not on their guard. People are unaware and underestimate the damage caused, although it is clear these massive violations of privacy and manipulation have had fatal consequences. The problem is that the damages suffered in digital environments are not perceived as real damages since freedom and rights die without humans being physically hurt.[5]

When these digital risks are considered real risks with concrete harms, they are largely consented. Indeed, "dataisms" are widespread in society, so it is assumed as something natural to give up rights and freedoms in order to reach a higher stage in evolution (homo deus) through big data and artificial intelligence.[6] Without entering into this debate, it can be seen that most citizens are slipping into "dataism," as they assume the risks and even stoically bear the damages of digital

---

2. *See generally* Ulrich Beck, *The Digital Freedom Risk: Too Fragile an Acknowledgment*, 22 QUADERNS DE LA MEDITERRÀNIA, 141, 141–44 (2015) (contrasting the difficulty in perceiving the damage suffered in the digital environment with events such as the Chernobyl disaster, global warming or the COVID-19 pandemic, in which a catastrophic situation occurs with concrete physical damage that generates awareness and the adoption of measures to address these risks).

3. *See generally* JAMES BRIDLE, NEW DARK AGE: TECHNOLOGY AND THE END OF THE FUTURE (2018).

4. *See generally* EDWARD SNOWDEN, PERMANENT RECORD (2019) (discussing PRISM, the program of the U.S. National Security Agency (NSA)); BRITTANY KAISER, TARGETED: THE CAMBRIDGE ANALYTICA WHISTLEBLOWER'S INSIDE STORY OF HOW BIG DATA, TRUMP, AND FACEBOOK BROKE DEMOCRACY AND HOW IT CAN HAPPEN AGAIN (2019) (discussing Cambridge Analytica and the U.S. 2018 elections).

5. Beck, *supra* note 3, at 144.

6. *See* Chris Anderson, *The End of Theory*, WIRED (June 23, 2008, 12:00 PM) (discussing the new era of dataism), https://www.wired.com/2008/06/pb-theory/; *see also* YUVAL NOAH HARARI, HOMO DEUS: A BRIEF HISTORY OF TOMORROW (2017).

services as a fair price to enjoy their functionalities.[7]

B. The Growing Threat of Digital Risks

The unique nature of digital risks, together with the late development of the technological revolution have meant that we have not been aware of their relevance until very recently, despite their growing and serious threat.

Digital risks are not limited to the violation of our privacy, but can reach much deeper and affect free will, limiting or making our own human condition disappear. Digital technologies fight to capture our attention[8] and can trap us in a certain ideological frame or "filter bubble."[9] It is a "friendly Big Brother" that knows us better than we know ourselves and can condition our thoughts and opinions.[10] Even more invasive technologies are being developed that can record mental data from brain impulses and manipulate them, leading to the recognition of neuro-rights to preserve the physical and psychological integrity of the individual.[11]

The evolution, scope, and consequences of digital risks are very different from traditional global risks not only because of their unique nature, but also because they occur in a hitherto unprecedented scenario. Digital innovation is not centered on the control and exploitation of nature, as is the case with other global risks. On the contrary, we are in the "age of surveillance capitalism"[12] in which

---

7. This is the case of Google Maps, which can track its users to offer them the best routes, or in the case of intelligent assistants (such as Alexa, Siri or OK Google), which can be allowed to monitor conversations in exchange for the use of all their functionalities.

8. *See generally* TIM WU, THE ATTENTION MERCHANTS: THE EPIC SCRAMBLE TO GET INSIDE OUR HEADS (2016) (discussing the digital struggle to capture attention).

9. *See generally* ELI PARISER, THE FILTER BUBBLE: HOW THE NEW PERSONALIZED WEB IS CHANGING WHAT WE READ AND HOW WE THINK (2012).

10. *See* BYUNG-CHUL HAN, PSYCHOPOLITICS: NEOLIBERALISM AND NEW TECHNOLOGIES OF POWER 59–64 (2019); *see also* BYUNG-CHUL HAN, INFOCRACY: DIGITIZATION AND THE CRISIS OF DEMOCRACY (2022).

11. Chile was the first country to recognize neuro-rights in its Constitution through the modification of Article 19, number 1. In the case of Spain, the Charter of Digital Rights, approved by Agreement of the Council of Ministers on July 13, 2021, dedicates its section XXVI to neuro-technologies, establishing that the limits and guarantees for the implementation and use of neuro-technologies on people can be regulated by law.

12. SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER 16 (2019) ("Just as industrial civilization flourished at the expense of nature and now threatens to cost us the Earth, an information civilization shaped by surveillance capitalism and its new instrumentarian power will thrive at the expense of human nature and will threaten to cost us our humanity.")

humans are controlled and exploited by large corporations which, for technological, economic, and jurisdictional reasons, are beyond the reach of the public authorities.

Finally, it should be noted that the unstoppable process of digitalization has intensified in recent years, exponentially increasing the level of risks involved. It is an irreversible process and all countries, companies, and individuals will depend more and more on digitalization. But the most paradoxical thing is that digitalization, which is the source of risk, has also become the panacea, even for overcoming other global risks.[13] A dangerous inverse correlation is generated whereby the reduction in the level of the traditional global risks (environment, health, or safety) goes through the increase of digital risks.[14]

II. RISKS OF DIGITALIZACION:

A. Between Techno-Feudal Lords and a Digital Leviathan

1. Leaving the Digital Laissez-Faire Era

Identifying digitalization as a global risk is a first step toward taking it seriously and initiating a public debate on it. There is no turning back from this process and the digital Luddites will not be able to stop it. The question is how to deal with the digitalization that is reshaping our society, both in the public and private spheres, and generating new forms of power.

Digital transformation has so far taken place under the principle of freedom (*laissez-faire*) letting innovation unfold without limits. Information and communication technologies have developed freely and produced enormous advances, such as personal computers and the internet, but without specific legislation. Only ad hoc measures have been taken to address specific issues raised by these developments (child protection, copyright, content liability, etc.)[15] from a negative, ex

13. For fighting climate change (digital transition for decarbonization), curving pandemics (apps for COVID), for guarantying safety (surveillance devices).

14. *See* Thomas A. Hemphill, *The Innovation Governance Dilemma: Alternatives to the Precautionary Principle*, 63 TECH. SOC'Y 7 (2020) (recommending as the main tool for innovation (and risk governance in general) the adoption of artificial intelligence and data analytics for risk management and regulatory adjustment, without realizing the risks that such a remedy entail).

15. There is not an Internet Act as such, but legislation on child protection (Children's Internet Protection Act of 2000), copyright (Digital Millennium Copyright Act of 1998), liability (Communications Decency Act of 1996), and so on.

post, and strictly reactive-corrective approach.

However, the strategic nature of digital transformation and the emergence of relevant risks is leading many countries to abandon their passive and negative approach to digitalization. During the last decade countries are deploying alternative strategies for digital governance that involve positive, ex ante and proactive-preventive measures. We are at a turning point where an innovative legal framework for the new digital society and digital government is being forged.

In any case, countries are following quite different strategies to deal with this digital transformation, which can be classified into three main models. On the one hand, in the case of the Unites States, the aim is to maintain free competition and minimal intervention, although regulations are inevitably increasing. On the other hand, in totalitarian countries such as China or Russia, government takes over the digital sector, which becomes an instrument of power. In between, the European Union is developing an open, flexible, and adaptive model of governance that respects free market while ensuring security and trust, which is essential for digital innovation.

B. Techno-Feudal Lords

There are many issues arising from the digitization of companies and citizens that has led to a change in market, work, education, and personal life. A myriad of problems need new solutions as many are emerging from new types of markets (platform economy), labor relations (platform workers), consumers (prosumers), media (streaming platform), and political forum (social networks). However, one aspect all of these challenges have in common is the presence of a digital intermediary (platform, network, search engine) that serves as the basis for the development of the activity. Thus, the extraordinary private powers of the large technology companies (big tech) arise and they in turn dominate this digital environment.

This is an extraordinary gamble because, for the first time, a private empire governed by large companies is being generated with unprecedented levels of control, both by society and individuals. Big tech companies decide on public debate, cancel opinions, and help candidates win elections. They feed from citizens' data and can make people become transparent. Never before in history has such singular, global, and intense power been concentrated into so few companies

without the presence or intermediation of government.[16] These large technology companies operate outside the law acting as lords of the digital environment they own and with an absolute dominion over citizens, in a kind of techno-feudalism system.[17]

Faced with this new scenario, the traditional rights of citizens are insufficient to cope with the power of the big tech companies. The right to privacy is too narrow to cover the numerous issues that arise in the new digital environment. The problem is that fundamental rights were conceived as limits to the power of government and not to control big business. This is the case, for example, of large platforms such as Facebook or Twitter that manage citizens' freedom of expression. It is also the case with the right of communication, which is now controlled by platforms such as HBO, Netflix, or YouTube.

This situation is leading to major changes in the legal approach to managing and controlling these new private powers and the risks they pose. In both the United States and the European Union, it has become clear that competition rules are not sufficient to contain big tech. As a result, new regulation of large intermediary providers is emerging that incorporates real ex ante measures to try to contain their extraordinary power.[18]

C. Digital Leviathan Rising

Digitalization is also transforming the public sector and, although it is not as attractive and glamorous, it is increasing to such an extent that it deserves specific attention. Most of the best-selling essays and academic literature focus on the problem of big tech's control over digital society,[19] but do not concern themselves with the power of a digital government. It should be noted that the government has more

16. Global Risks Report of the World Economic Forum ranked the risk of "digital dependencies" and "digital power concentration." *See* WORLD ECONOMIC FORUM, THE GLOBAL RISKS REPORT 2022, at 95 (16th ed. 2022).

17. Technology platforms have characteristics similar to feudal fiefdoms as companies are rent-seekers and control preferences, purchases and behavior without being accountable. *See* Yanis Varoufakis, *Techno-Feudalism is Taking Over*, DIEM25 (July 9, 2021), https://diem25.org/techno-feudalism-taking-over/.

18. *See Proposal for a Regulation on a Single Market for Digital Services (Digital Services Act)*, at 1, COM (2020) 925 final (Dec. 15, 2020) (making the platforms liable for content (with the threat of large fines));)*; Proposal for a Proposal for a Regulation on Contestable and Fair Markets in the Digital Sector (Digital Markets Act),* at 1, COM (2020) 842 final (Dec. 15, 2020) (limiting the activities of some of Big Tech, particularly the gatekeepers, that control access to the market and dictate how markets operate). *See generally* STAFF OF H. COMM. ON THE JUDICIARY, 117th CONG., INVESTIGATION OF COMPETITION IN DIGITAL MARKETS (Comm. Print 2020).

19. *See* ZUBOFF, *supra* note 12; HAN, INFOCRACY, *supra* note 10.

data, more resources, and more power than any company, so digitalization can lead to unknown consequences.

Information and Communications Technology has been transforming government for decades favoring an agile, simple, and transparent functioning, essentially thanks to online government based on internet. The e-government allows permanent and unlimited distance access and interaction with citizens. However, it is only an instrument as it has solely affected the means for governmental action but has not produced changes in the essence of government.

In the last decade, disruptive technologies—such as artificial intelligence, blockchain, and cloud and edge computing—are spreading throughout governments. These new technologies are no longer simply tools to facilitate governmental activity, but they are transmuting and reshaping government functions. Digital transformation into i-government is affecting the core functions of government, as they are even being applied to decision-making.

These new technologies are beginning to be widely used in the executive branch. More agencies and administrative bodies are using disruptive technologies both to provide their services and to make decisions. But in addition, these disruptive technologies are beginning to be used in other branches of government, which creates more problems in terms of implications for democratic processes (in the case of the legislative branch) or due process (in the case of the judicial branch).

Although there is e-government regulation, there is still no legislation for the use of these disruptive technologies in government. This makes sense since these are innovations—such as artificial intelligence—that do not yet have any general regulations, so there cannot be a special one regarding their use in government. Therefore, these innovations are being incorporated under the previous legal framework that is obsolete and does not provide answers to the innumerable challenges and problems that arise in all branches of government.

Digital transformation is overflowing the constitutional and administrative framework, one which has taken centuries to devise and has led to the model we have for current governments—the rule of law and democracy principle. Now a Digital Leviathan is emerging for which we still do not have rules. It may become a more powerful subject without the checks and balances approach models we have used up until now.

D. Some Thoughts on Digital Government

These were some concerns discussed at the Conference "Digital Transformation of Government: Towards a Digital Leviathan" (June 25–26, 2022) organized by the Universidad Carlos III de Madrid and Indiana University and which I co-directed with Alfred C. Aman, Professor of Law at the Maurer School of Law (Indiana University). The papers are published in the *Indiana Journal of Global Legal Studies* (Volume 30, Issue 1).

A good starting point for addressing the risks and challenges of digitalization is to examine the bills of digital rights. It is not so much a matter of recognizing new rights but rather adapting existing rights to the digital environment. This is the approach of the EU Declaration on Digital Rights and the national charters of digital rights.[20] The new generation of digital rights is being promoted by some scholars, both from scientific and legal fields. This is the case of Rafael Yuste, a neurobiologist in Columbia, who has been advocating for years for the recognition of neuro-rights to protect free will,[21] and of Tomás de la Quadra-Salcedo, an emeritus professor of law who led the group that drafted the Spanish Charter of Digital Rights.[22]

Among the disruptive technologies, artificial intelligence stands out as the technology that is posing the most challenges in its use by government. Several proposals of AI regulation are moving through the legislative process in the EU and US and in other countries. In the case of the EU, the proposed AI regulation (AI Act) is based on securing trust to promote AI use, as Antonio Estella points out.[23]

However, the use of AI in administration is spreading in the absence of regulation, so it is developing under previous general rules—on data privacy, e-government, etc.—that are clearly inadequate to address the challenges and problems it poses. Therefore, there is an urgent need to

---

20. These are not merely Internet rights (like the 2014 Online Bill of Rights in Brazil or the 2015 Italian Declaration of Internet Rights) but go further as digital rights. *See generally Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Establishing a European Declaration on Digital Rights and Principles for the Digital Decade*, COM (2022) 27 final (Jan. 27, 2022); CARTA DERECHOS DIGITALES (CHARTER OF DIGITAL RIGHTS) (2021) (Sp.).

21. *See generally* THE NEURORIGHTS FOUNDATION, https://neurorightsfoundation.org.

22. *See* Rafael Yuste & Tomás De La Quadra-Salcedo, *Neurorights and New Charts of Digital Rights: A Dialogue beyond the Limits of the Law*, 30 IND. J. GLOBAL LEGAL STUD. (2023).

23. *See* Antonio Estella, *Trust in Artificial Intelligence: Analysis of the European Commission Proposal for a Regulation of Artificial Intelligence*, 30 IND. J. GLOBAL LEGAL STUD. (2023).

enact specific legislation on the use of AI in government to bring it in line with the constitutional principles of the administrative state, as I claim.[24]

The difficulties of fitting AI into the traditional categories of administrative law are obvious. This mismatch between the new technology and the old rules is analyzed by Gilles Guglielmi,[25] who considers algorithm not as rules and technology but as soft law always under the rule of law.

One of the most problematic aspects of AI to us is transparency and access to the algorithm in AI used in government. Experiences to date have rejected or hindered access to the algorithm, preventing accountability and violating transparency and reason-giving, which are common principles of government action. This makes it necessary to rethink the conditions of access to algorithms to ensure transparency and the right to have an open and clear public decision, as Estrella Gutiérrez David claims.[26]

Another controversial issue regarding the use of AI is facial recognition. Although some forms of facial recognition are being banned, it is something that is becoming more and more widespread and allows control in a way that has never existed before. Governmental power is bearable because there are areas in which citizens can be left out of its reach. However, an omnipresent government is unbearable and even more so when it is used to control certain sectors of the population, giving rise to what Antonio Pelé calls necropolitics.[27]

The digitization of government is not limited to AI as there are other disruptive technologies that are also transforming its essence. Specifically, blockchain is one of the technologies with the most potential to improve administrative activity and give rise to hitherto unknown possibilities. Migle Laukyte analyzes the potential of blockchain use in government and how it can make a decisive

---

24. *See* José Vida Fernández, *Artificial Intelligence in Government: Risks and Challenges of Algorithmic Governance in the Administrative State,* 30 IND. J. GLOBAL LEGAL STUD. (2023).

25. *See* Gilles Guglielmi, *The Contentious Issues of Governance by Algorithms*, 30 IND. J. GLOBAL LEGAL STUD. (2023).

26. *See* María Estrella Gutiérrez David, *Government by Algorithms at the* Light *of Freedom of Information Regimes: A Case-by-Case Approach on ADM Systems within Public Education Sector*, 30 IND. J. GLOBAL LEGAL STUD. (2023) (analyzing the MIUR, Ofqual, Parcoursup, and Houston cases).

27. *See* Antonio Pelé, *On Facial Recognition, Regulation and 'Data Necropolitics'*, 30 IND. J. GLOBAL LEGAL STUD. (2023).

contribution to the right to good administration.[28]

Digitization has always had a special impulse in those areas where huge information processing is required and it contributes to increase public revenues. This is the case of the tax system, which has undergone a special development in almost all countries, and particularly in Denmark, as Peter Koever Schmidt and Louise Fjord explain.[29]

IV. CONCLUSION

Digitalization is transforming our society at an accelerating pace. Digital transformation has enormous advantages but it also brings great threats that must be considered. Digital risks must be considered to be true global risks in order to initiate a public debate on their consequences and how to regulate them.

The digital society has arrived but we do not have the institutions in place to govern this new digital world. The use of disruptive technologies in government is taking place without specific regulations to ensure their use. It is important that the public debate is not limited to the new forms of economy, work, and social relations, but also reaches the new digital government. Otherwise it may be too late and we may find ourselves in the hands of a Digital Leviathan.

---

28. *See* Migle Laukyte, *Blockchain and the Right to Good Administration: Adding Blocks to or Block'ing of the Globalization of Good Administration?*, 30 IND. J. GLOBAL LEGAL STUD. (2023).

29. *See* Louise Blichfeldt Fjord and Peter Koerver Schmidt, *The Digital Transformation of Tax Systems: Progress, Pitfalls and Protection in a Danish Context*, 30 IND. J. GLOBAL LEGAL STUD. (2023).