Studien zum Datenschutz 79

Spiecker gen. Döhmann | Schertel Mendes | Campos (Eds.)

Digital Constitutionalism

Nomos

Studien zum Datenschutz

Edited by
Prof. Dr. Dr. h.c. Spiros Simitis †
Prof. Dr. Indra Spiecker genannt Döhmann, LL.M.

Volume 79

Indra Spiecker gen. Döhmann | Laura Schertel Mendes
Ricardo R. Campos (Eds.)

Digital Constitutionalism

Nomos

The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available on the Internet at http://dnb.d-nb.de

1st Edition 2025

Published by
Nomos Verlagsgesellschaft mbH & Co. KG
Waldseestraße 3–5 | 76530 Baden-Baden
www.nomos.de

Production of the printed version:
Nomos Verlagsgesellschaft mbH & Co. KG
Waldseestraße 3–5 | 76530 Baden-Baden

ISBN 978-3-7560-0541-3 (Print)
ISBN 978-3-7489-3864-4 (ePDF)

DOI https://doi.org/10.5771/9783748938644

Online Version
Nomos eLibrary

Table of Contents

II. Data Protection and Privacy Rights in the Digital Age

III. AI, Consumer Protection, and Online Governance in a Digital World

Introduction

This volume collects the contributions of the Workshop on 'Digital Constitutionalism: A Normative and Institutional Framework for Conflict Resolution Under Construction', held at Goethe University Frankfurt on March 3rd and 4th, 2023. To discuss and to address these important challenges, top legal experts from Germany, Brazil, and Europe gathered for a cross-disciplinary investigation into the pressing issues. This unique event, fostering a comparative law perspective, sought to unravel complexities and explore potential solutions in the realm of digital constitutionalism. By harnessing the collective wisdom and expertise of these esteemed scholars, the conference aimed to pave the way for collaborative efforts in shaping the evolution of constitutional law in the digital landscape.

The topic of digital constitutionalism is becoming increasingly important in the current debate on the effects of digitalization. Almost every fundamental right is in one or more aspects genuinely affected by the chances triggered by digitalization; old conflicts break out and new conflicts arise. Established legal understandings and hidden prerequisites on which constitutions are typically built are challenged. The fundament on insights from philosophy, psychology, sociology and political science, among others, has been shattered. Established terms and normative concepts such as public sphere, media, administration, separation of public and non-public actors, and services of general interest or enforcement must be redefined under conditions of great technical dynamics creating significant legal uncertainty. The dichotomy between fostering innovation and preserving rights in digitized social and economic milieus gives rise to a number of fundamental dilemmas. And any formulation of rights in the digital age is encumbered by uncertainty, prompting a quest for optimal solutions for protection, safety and security which is impossible to fulfill by any state or society. Traditional mechanisms of enforcement face unprecedented challenges in establishing trust within a digitalized state, necessitating a reevaluation of their efficacy in a realm characterized by unparalleled technological dynamism. Ever-increasing means of surveillance contribute to fields of tension between just this security and the necessary freedom for a democratic, rule-of-law state guarding and governing autonomous, free and individual citizens.

Central to this discourse are the pressing questions that demand nuanced consideration within the realm of digital constitutionalism. The book addresses central questions: Are present concepts of the state and constitutionalization sufficient to define rights and duties within the dynamics and ubiquity of digital services and products, hardware and software, networks and platforms? How do we have to redefine law to solve new conflicts, possibly even to resolve them, especially in view of the new forms of enforcement and control? Are existing dogmatic notions of intervention, justification and practical concordance for resolution between conflicting individual rights still sufficient? Are the existing constitutional concepts equipped to effectively safeguard private rights and state obligations amidst the dynamic landscape of digital innovation with its inherent change of power and diffusion of responsibility? How can the role of platforms and intermediaries be redefined in terms of fundamental rights and specific digital constitutional law reflecting both their importance but also their vulnerabilities? How can we understand sovereignty in an environment where hidden normative values and technologically determined standards construe a reality which is quickly devoid of individual experience, even less control? How do we constitutionally cope with external effects of third parties when discussing infringements into individual rights? How must our conceptual frameworks surrounding intervention, justification, legitimation and conflict resolution adapt to the evolving digital terrain? How do we create trust in new services and new technologies and how do we determine the threshold for human intervention created when traditional legal mechanisms no longer seem as effective as in the analogue world and where transparency and individual control fails? What are the best solutions to reconcile innovation and dynamism with the protection of rights in the digital environment, when the very formulation of rights in the digital age is subject to uncertainty? Do we have to alter our view on infrastructure?

Closely related are the aspects of living constitutionalism when the constitutional foundations are transferred to regulation and administrative law: Does the European digital agenda, which encompasses pivotal legislative initiatives beginning with the General Data Protection Regulation and being enhanced with legislation such as the Digital Markets Act, Digital Services Act, AI Act, Data Governance Act, and Data Act, offer a viable pathway to navigate conflicts and address rights violations in the burgeoning digital socio-legal ecosystem including new digital social, market and legal orders in tune with the constitutional settings?

As one result of these complexities and challenges, some authors formulate special digital fundamental rights to meet new challenges. However, it is less than obvious that changes and challenges through digitization call for new fundamental rights and new institutional settings – in many cases, a thorough analysis of the existing understanding might just as well toughen up our existing constitutions for the digital turn and thus providing continued guidance for states and citizens alike.

The conference in March and the evolving chapters in this book provide a first analysis of the questions and also offer first answers and solutions. They reflect on the need to adapt existing constitutional norms, create new constitutional frameworks, and redefine the role of law in a changing digital, social and economic landscape. Our contributors shed light on the dynamic interplay between digital technologies and constitutional principles, exploring how legal frameworks adapt to the challenges and opportunities of the digital age. Through their insightful and complex, often interdisciplinary informed analyses, they highlight the evolving nature of digital constitutionalism and its implications for protection of rights, governance, and democratic normativity.

This volume, through its diverse contributions, makes a compelling case for the ongoing relevance and adaptability of constitutional principles in the face of digital transformation. It underscores the necessity of a nuanced, rights-based approach to digital governance, advocating for the development of digital fundamental rights as essential to upholding the constitutional order in the digital age. In doing so, it offers valuable insights for scholars, policymakers, and practitioners alike, charting a course for the future of digital constitutionalism.

Therefore, our authors deserve greatest appreciation for taking up these issues with us – and also for their patience. We are immensely grateful for a surrounding in which challenging and cutting-edge research is possible. The conference and the book were made possible by Frankfurt University's Research Initiative Contrust – Trust in Conflict, along with the generous support from the Alexander-von-Humboldt-Foundation. Profound and heartfelt appreciation is also owed to the invaluable assistance provided by the team Prof. Spiecker genannt Döhmann's Chair of Administrative and Constitutional Law, Information Law, Environment, and Legal Theory at the University of Frankfurt. In the course of the production of this book, her team at her new Institute of Digitalisation at Cologne University also assisted tremendously. A very warm thank-you goes to the indispensable

Berna Orak for her patience and wisdom in finalizing this book and getting the contributions to the publisher.

Cologne/Brasilia/Frankfurt, December 2024

Prof. Dr. Indra Spiecker genannt Döhmann
Prof. Dr. Laura Schertel Mendes
Dr. Ricardo Campos

I.
Digital Constitutionalism: Theoretical Foundations and Jurisprudential Perspectives

Conceptual Approaches to Digital Constitutionalism: A Counter-Critique

Edoardo Celeste[*]

Abstract: Over the past decade, the concept of digital constitutionalism has attracted attention from scholars from various disciplines, courts, policymakers, and private companies. This chapter aims to provide a systematic mapping of how this notion has been used and criticised over the past few years. In particular, this work reconstructs how theories of digital constitutionalism have evolved in recent scholarly works. This notion emerged with an innovative and progressive meaning, referring to an expanded constitutional dimension beyond the state. Recent scholarship has proposed a more holistic conception and has simultaneously applied this notion to specific fields or normative sources. The chapter proposes three models of categorisation of the emerging scholarly approaches to digital constitutionalism and presents three categories of critical arguments that have been moved to the theories of digital constitutionalism. The chapter concludes with a personal counter-critique to these views.

A. Introduction

> 'Digital constitutionalism refers to the concept of establishing a set of principles, norms, and rules that govern the use, protection, and regulation of digital technologies within a society. Just as a traditional constitution outlines the fundamental rights, responsibilities, and structure of a nation's governance, digital constitutionalism seeks to provide a framework for how digital technologies are managed and integrated into various aspects of society, including politics, economy, culture, and individual rights.

* I would like to thank all the colleagues who participated in the workshop '*Digital Constitutionalism. A Normative And Institutional Framework For Conflict Solving Under Construction*' (Frankfurt, 3-4 March 2023) for their feedback on an earlier presentation of this paper as well as Gary Brady for his research assistance.

> The key elements of digital constitutionalism might include: 1. Digital Rights: […]. 2. Data Protection and Privacy: […]. 3. Internet Governance: […]. 4. Cybersecurity: […]. 5. Digital Economy: […]. 6. Access and Digital Divide: […]. 7. Content Regulation: […]. 8. Algorithmic Transparency and Accountability: […]. 9. International Cooperation: […]. 10. Digital Sovereignty: […].
>
> Digital constitutionalism acknowledges the transformative impact of digital technologies on modern society and aims to establish a legal and ethical framework that respects fundamental human rights while promoting innovation and progress in the digital age. It's an evolving concept, as the challenges and opportunities presented by digital technologies continue to emerge and change over time.'[1]

This is the answer provided in August 2023 by the freely accessible version of ChatGPT (model GPT-3.5, as of August 2023) to the following query: "please define 'digital constitutionalism'". ChatGPT had no hesitations. It resolutely offered us a definition. Digital constitutionalism would consist in establishing constitutional rules for the 'use, protection, and regulation of digital technologies'. We are given even a decalogue of 'key elements of digital constitutionalism', with the caveat -though- that digital technologies continually develop, eventually making digital constitutionalism an 'evolving concept'.[2] It is only when I stubbornly rephrase my question in 'what is digital constitutionalism?' that ChatGPT more humbly admits: 'As of my last knowledge update in September 2021, the term "digital constitutionalism" doesn't have a widely recognized and standardized definition. It is a concept that is still evolving and being discussed within academic, legal, and policy circles. […] For the most current understanding and discussions on this topic, I recommend consulting recent academic literature, policy documents, and expert opinions.'[3] A conclusion that Bard, Google's chatbot whose freely available version continually sources information from the

1 ChatGPT-3.5, answer to 'please define "digital constitutionalism"', https://chat.openai.com/, 8 August 2023.

2 This statement seems to justify why ChatGPT uses a conditional form in 'The key elements of digital constitutionalism *might* include […].

3 ChatGPT-3.5, answer to 'what is digital constitutionalism?', https://chat.openai.com/, 8 August 2023.

Internet, gave me immediately when prompted with the same questions I asked to ChatGPT.[4]

The absence of consensus of what 'digital constitutionalism' means was what prompted me to publish one of my first works on this topic, entitled "Digital Constitutionalism: A New Systematic Theorisation'.[5] In this article I mapped the existing use of the concept of digital constitutionalism, noticing that very often authors employed this expression without defining it. I then provided a theory to reconcile these various scholarly positions, proposed a definition, and clarified its relationship with the notion of 'constitutionalisation' of the digital society, a term that was often used interchangeably with that of 'digital constitutionalism'.

Over the past few years, this concept has not only attracted attention from scholars from various disciplines, but has also been used by courts, policymakers, and private companies.[6] Generally speaking, this increased use has not added further clarity to the contours of this concept. From a scholarly perspective, we can observe the emergence of distinguishable 'approaches' to the use of digital constitutionalism as well as a series of criticisms to this concept. This chapter aims to focus on the scholarly use of digital constitutionalism and to provide a systematic mapping of how this notion has been used and criticised over the past few years. This work will be structured in four parts. Section B will reconstruct how the use of this concept has evolved in recent scholarly works, complementing my previous mapping exercises.[7] Section C will propose a new categorisation

4 Bard, answer to 'what is digital constitutionalism?', https://bard.google.com/, 8 August 2023: 'Digital constitutionalism is a concept that refers to the adaptation of constitutional values and principles to the digital age. It is a broad term that encompasses a variety of ideas about how to ensure that digital technologies are used in a way that respects human rights, democracy, and the rule of law. […] Digital constitutionalism is a relatively new field, and there is no single agreed-upon definition or set of principles.'.

5 Edoardo Celeste, 'Digital Constitutionalism: A New Systematic Theorisation' (2019) 33 International Review of Law, Computers & Technology 76.

6 See, e.g., Gilmar Ferreira Mendes and Victor Oliveira Fernandes, 'Constitucionalismo Digital e Jurisdição Constitucional: Uma Agenda de Pesquisa Para o Caso Brasileiro' (2020) 16 Revista Brasileira de Direito 1; Cristiano Codagnone, Giovanni Liva and Teresa Rodriguez de las Heras Ballell, 'Identification and Assessment of Existing and Draft EU Legislation in the Digital Field' (2022) EU Parliament Study <https://www.europarl.europa.eu/RegData/etudes/STUD/2022/703345/IPOL_STU(2022)703345_EN.pdf>; Facebook, 'Global Feedback & Input on the Facebook Oversight Board for Content Decisions' <https://about.fb.com/wp-content/uploads/2019/06/oversight-board-consultation-report-2.pdf>.

7 Celeste, 'Digital Constitutionalism' (n 5).

of the emerging scholarly approaches to digital constitutionalism. Section D will present three main types of critical arguments that have been moved to the theory of digital constitutionalism. Finally, Section E will conclude with a personal counter-critique to these views.

B. Concept evolution

I. The origins

The notion of digital constitutionalism was first used with its most original and innovative meaning. Firstly, by referring to the idea of applying constitutional norms to private actors, and thus overtaking the traditional anchoring of the constitutional dimension to the State. Secondly, by looking at normative sources that are not traditionally considered as constitutional, including not only legal sources such as private law, but also norms emerging in political discussions or at the level of civil society, and thus often devoid of any binding legal character.

1. Beyond the State

In what we could call the 'first generation' of scholars using the concept of digital constitutionalism – I include in this flexible category works published in the decade from 2009 to 2018 – this notion referred to the idea of applying constitutional rights and principles to multinational tech companies producing and managing digital products and services. Constitutionalism, a concept linked to the idea of establishing and implementing the constitution, intended as the foundational framework – be it codified in a document or not - of a polity, is projected beyond the State, in the realm of private actors. A non-traditional reading of the constitutional dimension, but not a novelty per se. The anchoring of the concept of constitutionalism to the state dimension had already been subverted in the context of international law. Globalisation marked the progressive emergence of issues, ranging from international terrorism to climate change, that required the concerted intervention of a plurality of actors.[8] The State maintains a cen-

8 See Anne Peters, 'Compensatory Constitutionalism: The Function and Potential of Fundamental International Norms and Structures' (2006) 19 Leiden Journal of International Law 579.

tral role but some of its functions shift vertically, in two directions: up, to supranational actors and, down, to multinational non-state actors.[9] In a globalised world, besides regional and international intergovernmental organisations, autonomous private subsystems of society, such as media or sportive organisations, regulate themselves, establish their own constitutional norms.[10] The constitutional dimension expands its perimeter, it becomes 'multi-level' or 'hybrid'.[11] And the initial use of the concept of digital constitutionalism fits this grove, focusing in particular on the dimension of powerful multinational tech companies. As Pereira and Keller have put it more recently, we observe an 'indispensability of constitution to mitigate asymmetries of power even – and mainly – in transformative contexts generated by globalisation'.[12]

The first generation of scholars using this term did not define what actually digital constitutionalism is.[13] They focused more on the underlying phenomenon they wished this concept to denote. There was a lack of consensus in relation to the actors involved and the means adopted to pursue the aims of digital constitutionalism. Suzor was the first one to use this expression consistently to denote the project of limiting the power of private digital companies through the use of constitutional principles, with particular attention to the rule of law.[14] For Suzor, constitutional law has a twofold aim: on the one hand, to circumscribe the perimeter of action of private self-regulation, and, on the other hand, to instil its core principles – traditionally, only articulated with reference to the State – into contract law,

9 See Petra Dobner and Martin Loughlin (eds), *The Twilight of Constitutionalism?* (Oxford University Press 2010), who speak of an 'erosion of statehood' (pt 1).

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

11 See Ingolf Pernice, 'The Treaty of Lisbon: Multilevel Constitutionalism in Action' (2009) 15 Columbia Journal of European Law 349; Gunther Teubner, 'Constitutionalising Polycontexturality' (2010) 20 Social and Legal Studies 210, 246; Mauro Santaniello and others, 'The Language of Digital Constitutionalism and the Role of National Parliaments' (2018) 80 International Communication Gazette 320, 324.

12 Jane Reis Gonçalves Pereira and Clara Iglesias Keller, 'Constitucionalismo Digital: Contradições de Um Conceito Impreciso' (2022) 13 Revista Direito e Práxis 2648, 2652, authors' translation.

13 For a mapping of this first generation of scholars, see Celeste, 'Digital Constitutionalism' (n 5).

14 Nicolas Suzor, 'The Role of the Rule of Law in Virtual Communities' (2010) 25 Berkeley Technology Law Journal 1817; Nicolas Suzor, 'Digital Constitutionalism: Using the Rule of Law to Evaluate the Legitimacy of Governance by Platforms' (2018) 4 Social Media + Society 1.

the latter at its turn promoting a constitutionally-compliant development of private companies' self-regulation. Similar ideas had been previously expressed by Fitzgerald and Berman using different denominations, respectively 'informational' and 'constitutive' constitutionalism, and stressing, the first one, the constitutionalising role of private law, while, the latter, the centrality of national constitutional principles.[15]

2. Beyond the law

Within this first generation of scholars, some authors go even beyond traditional legal sources, such as constitutional and private law. They use the reference to digital constitutionalism in relation to norms that would traditionally lie outside the legal spectrum because adopted by private companies, promoted in the context of political processes or advocated by civil society actors, and thus not attaining the status of legally binding and generally applicable law.[16]

In the globalised digital society, powerful multinational companies creating, managing and selling digital products and services emerge as dominant actors beside nation States. We observe the emergence of a modern form of digital feudalism, where private rulers dictate the rules of their own virtual fiefs.[17] A stream of legal scholarship on digital technology had already observed the capability of the 'code' to act as the law – even if not in a discursive, i.e. verbal way - of the digital products and services we use.[18] The first generation of scholarship on digital constitutionalism identified another type of law related to this private sphere, this time more akin to the traditional conception of discursive legal rules. Karavas observed a trend in German case-law where the judiciary limited itself to play a guiding – 'maieutic' is the term used by the author – role vis-à-vis

15 Brian Fitzgerald, 'Software as Discourse? The Challenge for Information Law' (2000) 22 European Intellectual Property Review 47; Paul Berman, 'Cyberspace and the State Action Debate: The Cultural Value of Applying Constitutional Norms to "Private" Regulation' (2000) 71 University of Colorado Law Review 1263.

16 Celeste, 'Digital Constitutionalism' (n 4).

17 See Manuel Castells, *The Rise of the Network Society* (2nd edn, Blackwell 2000), who talks of an 'institutional neo-medievalism'; see also Bruce Schneier, 'Power in the Age of the Feudal Internet' [2013] MIND 16.

18 See Lawrence Lessig, *Code: And Other Laws of Cyberspace, Version 2.0* (Basic Books 2006); Joel Reidenberg, 'Lex Informatica: The Formulation of Information Policy Rules through Technology' (1998) 76 Texas Law Review 553.

a self-constitutionalising power of online platforms in determining their own, private 'lex digitalis'.[19] Going even beyond scholars who recognised the binding, quasi-legal character of the internal rules of social media companies, such as Bygrave who speaks of a 'lex Facebook',[20] I compared social media's Terms of Service to quasi-constitutional instruments, private bills of rights.[21]

National parliaments, which would traditionally be the depositaries of the legislative power, were studied in the context of digital constitutionalism as the promoters of political conversations on digital rights. We speak of political conversations, and not of ordinary stages of the legislative process, because the scholarship focused on outputs of parliamentary works that were the result of ad hoc commissions, often integrated by other societal stakeholders, which were not formally part of parliamentary activities. An example is the adoption of the *Declaration of Internet Rights* that was drafted by an ad hoc committee created by the then President of the Italian Chamber of Deputies and composed of politicians, academics, journalists and industry representatives.[22] Santaniello et al. analysed the specific language and content of various documents issued by similar parliamentary initiatives.[23] In particular, they highlighted that parliaments, in line with their traditional role as strongholds of democracy against the abuse of other State powers, mostly produced norms and principles of 'limitative' nature, which would aim to introduce safeguards against a potential compression of individual rights by other actors.[24] The work of these institutions in the context of digital constitutionalism is considered as a 'political process

19 Vagias Karavas, 'Governance of Virtual Worlds and the Quest for a Digital Constitution' in Christoph B Graber and Mira Burri-Nenova, *Governance of Digital Game Environments and Cultural Diversity: Transdisciplinary Enquiries* (Edward Elgar Publishing 2010); Vagias Karavas and Gunther Teubner, 'Www.CompanyNameSucks.Com: The Horizontal Effect of Fundamental Rights on "Private Parties" within Autonomous Internet Law' (2005) 12 Constellations 262.

20 Lee A Bygrave, 'Lex Facebook', *Internet Governance by Contract* (Oxford University Press 2015).

21 Edoardo Celeste, 'Terms of Service and Bills of Rights: New Mechanisms of Constitutionalisation in the Social Media Environment?' (2019) 33 International Review of Law, Computers & Technology 122.

22 Camera dei Deputati, 'Declaration of Internet Rights' <https://www.camera.it/application/xmanager/projects/leg17/commissione_internet/testo_definitivo_inglese.pdf>; See Oreste Pollicino and Marco Bassini (eds), *Verso Un Internet Bill of Rights* (Aracne 2015).

23 Santaniello and others (n 11).

24 Santaniello and others (n 11) 325 ff.

of Internet-constitution drafting', which would represent an intermediary discourse linking purely legal and societal normative processes related to the digital field.[25]

Such societal normative processes not only encompass the private law-making of tech companies mentioned above, but scholars also identified a phenomenon related to digital constitutionalism in the emergence of 'Internet bills of rights' promoted by civil society actors. Gill, Redeker and Gasser[26] and Petracchin[27] collected and analysed a number of texts published mainly by civil society organisations that advocate rights and principles addressing the challenges of the digital age. Despite their non-legally binding nature, these initiatives were regarded as a 'proto-constitutional discourse', a gradual intellectual exercise of translation of the core principles of contemporary constitutionalism into norms speaking to the actors of the digital society.[28] Scholars from various disciplines had already started investigating these 'Internet bills of rights' without specifically referring to the concept of digital constitutionalism, but focusing more on the message of this communicative effort carried out by a plurality of individuals and organisations.[29] From this point of view, we could argue that digital constitutionalism is also seen as a sort of 'movement', both of people and of thought.[30] From this perspective, the interdisciplinary character of the scholarship on digital constitutionalism emerges clearly. Digital constitutionalism is not only a legal phenomenon, but also a social and political one. Political both in terms of content, in the sense that it aims

25 Santaniello and others (n 11) 333.

26 Lex Gill, Dennis Redeker and Urs Gasser, 'Towards Digital Constitutionalism? Mapping Attempts to Craft an Internet Bill of Rights' (2015) Berkman Center Research Publication No 2015-15 <https://papers.ssrn.com/abstract=2687120>; see also a later version of this paper in Dennis Redeker, Lex Gill and Urs Gasser, 'Towards Digital Constitutionalism? Mapping Attempts to Craft an Internet Bill of Rights' (2018) 80 International Communication Gazette 302.

27 Andrea Pettrachin, 'Towards a Universal Declaration on Internet Rights and Freedoms?' (2018) 80 International Communication Gazette 337.

28 Gill, Redeker and Gasser (n 8) 3.

29 See Francesca Musiani, Elena Pavan and Claudia Padovani, 'Investigating Evolving Discourses on Human Rights in the Digital Age: Emerging Norms and Policy Challenges' (2009) 72 International Communication Gazette 359; Rolf H Weber, *Principles for Governing the Internet: A Comparative Analysis* (UNESCO 2015) <https://unesdoc.unesco.org/ark:/48223/pf0000234435>.

30 Cf. Kinfe Micheal Yilma, '"Bill of Rights for the 21st Century: Some Lessons from the Internet Bill of Rights Movement"' [2021] The International Journal of Human Rights 1.

to tackle 'fundamental political questions', but also in light of the nature of its initiatives, which are 'political interventions', 'pieces of a political conversation'.[31]

II. Development and growth

The first generation of scholarship on digital constitutionalism mainly looked at sources and actors that would not be regarded as traditionally belonging to the constitutional dimension. In this way, they stressed the power of private actors and highlighted the limitations of public power – not to say, of traditional constitutional law itself – to tackle the challenges of the digital society. In the past five years, the concept of digital constitutionalism has attracted the attention of significant number of scholars from various disciplines, giving rise to what Mendes defined a 'dynamic intellectual movement'.[32] This second generation of scholars contributed to add an analysis of more traditional constitutional actors and legal sources. This has been done by widening and further developing the concept of digital constitutionalism and by deepening the analysis of phenomena related to digital constitutionalism within traditional legal areas, such as legislation and case law, as well as in the context of the emergence of new technologies, such as quantum computing.

1. Widening

What we have called the first generation of scholarship on digital constitutionalism analysed a plurality of actors and normative sources where it was possible to observe the emergence of rights and principles targeting issues related to the digital environment. Some of these authors focused on legal sources, such as private law, others on normative instruments emerging within the private realm or simply at political and civil society level, thus devoid of any legally binding value. In light of this plural framework, I proposed a 'systematic' theoretical approach to digital constitutionalism to

31 Claudia Padovani and Mauro Santaniello, 'Digital Constitutionalism: Fundamental Rights and Power Limitation in the Internet Eco-System' (2018) 80 International Communication Gazette 295, 296–297.

32 See *Mendes/Fernandes*.

reconcile these scholarly positions and offer a wider and more encompassing definition of digital constitutionalism and its related phenomena.[33]

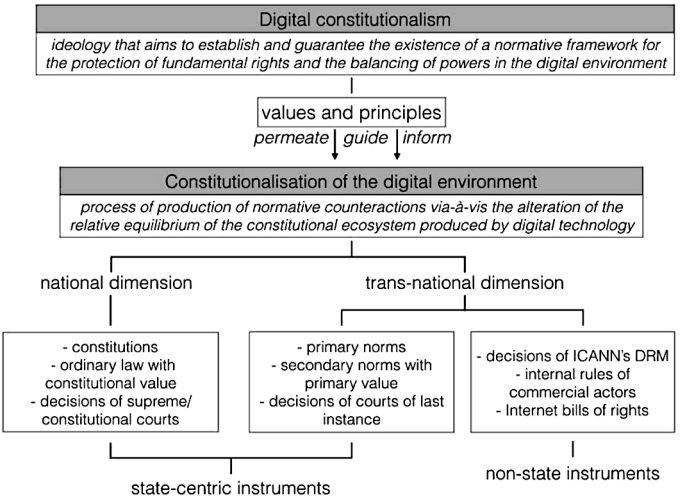
In my view, digital constitutionalism is not exclusively related to the limitation of power of private actors by legal sources acquiring a quasi-constitutional role. Nor does it exclusively denote constitutional discourses emerging in the societal sphere. It encompasses both these dimensions and goes beyond them. Digital constitutionalism is defined as the 'ideology that aims to establish and guarantee the existence of a normative framework for the protection of fundamental rights and the balancing of powers in the digital environment'.[34] In more concrete terms, such an ideology informs a variety of constitutional 'counteractions' that generalise and respecify core principles of contemporary constitutionalism to address the challenges of the digital society.[35] These counteractions, globally regarded, would constitute a composite and multilevel process of 'constitutionalisation' including normative responses emerging both within and beyond the State.[36]

The distinction between the concepts of constitutionalism and constitutionalisation assumes a core conceptual role in the context of this systematic theory, as the previous scholarship often used these two terms interchangeably. Constitutionalisation is defined as the process that is implementing the principles and values of constitutionalism.[37] I argued that a systematic theory allows us to consider the current process of constitutionalisation of the digital society as a multilevel one.[38] Multilevelism does not merely imply a fragmentation of constitutionalising inputs – there is no single constitutional 'father' in the digital society. But it is also possible to

33 Celeste, 'Digital Constitutionalism' (n 5).
34 Celeste, 'Digital Constitutionalism' (n 5) 88.
35 The concept of 'generalisation and re-specification' is borrowed from Teubner: see Teubner (n 10); for an application to the context of digital constitutionalism, see Edoardo Celeste, 'Internet Bills of Rights: Generalisation and Re-Specification Towards a Digital Constitution' (2023) 30 Indiana Journal of Global Legal Studies 25.
36 Celeste, 'Digital Constitutionalism' (n 1); Edoardo Celeste, 'The Constitutionalisation of the Digital Ecosystem: Lessons from International Law' in Angelo Golia, Matthias C Kettemann and Raffaela Kunz (eds), *Digital Transformations in Public International Law* (Nomos 2022).
37 Celeste, 'Digital Constitutionalism' (n 5).
38 Edoardo Celeste, 'The Constitutionalisation of the Digital Ecosystem: Lessons from International Law' in Angelo Golia, Matthias C Kettemann and Raffaela Kunz (eds), *Digital Transformations in Public International Law* (Nomos 2022).

talk of a set of mutually stimulating and compensating impulses.[39] In this way, despite the differences of the various elements of such a process of constitutionalisation, it is possible to recompose the puzzle – or better, to understand the anatomy, the whole significance, of this complex mosaic – by interpreting these various inputs, as if they were elements going in the same direction: each one contributing to translate and implement the core values of contemporary constitutionalism in the context of the digital society.

Fig. 1 – Mapping of the phenomenon of constitutionalisation of the digital environment[40]



An aerial view of this phenomenon allows us to single out constitutionalising inputs that emerge both within and beyond the context of the State, thus encompassing all the normative sources analysed by the first generation of scholarship and even expanding it. Indeed, one has not only to mention the adoption of the whole spectrum of 'traditional' – from a legal perspective – normative sources, such as constitutional amendments, decisions of constitutional courts, or ordinary law playing a constitutional function. One has also to observe the emergence of constitutional stimuli

39 Cf Peters (n 8); see Celeste, 'The Constitutionalisation of the Digital Ecosystem' (n 38).

40 Originally published in Celeste, 'Digital Constitutionalism' (n 5).

beyond the state dimension. In Figure 1, I listed three examples of what I called constitutional 'counteractions'[41] emerging in non-state-centric contexts: the decisions of the ICANN's Dispute Resolution Mechanism, the internal rules of multinational tech companies and Internet bills of rights.[42]

This multilevel process of constitutionalisation is not merely an academic fiction to make coherence of otherwise fragmented normative scenarios. The tesserae of this complex mosaic are not evolving in airtight silos. They influence each other. They stimulate each other and contribute to the same conversation, albeit using different normative instruments. They are 'communicating vessels'.[43] Interestingly, Internet bills of rights or the internal rules of private tech companies intentionally adopt the specific traditional language of constitutional charters. Preambles, use of the first person plural, present tenses: the constitutional jargon becomes a *lingua franca* that reconnects legal discourses otherwise occurring in contexts without institutionalised connections or ways of communication.[44] As in a puzzle, each counteraction complements each other; the emergence of one normative response can be read as the symptom of a status of 'constitutional anaemia' arising at another level of the constitutional ecosystem.[45] One normative source might struggle to address a problem of the digital environment, so another source proposes a solution, finally stimulating further reactions in the constitutional mosaic.

2. Deepening

The second generation of scholars dealing with digital constitutionalism also deepened the analysis of phenomena and normative trends related to this concept, focusing, on the one hand, on traditional legal actors, such as courts, and, on the other hand, on the latest technological developments, such as quantum computing.

41 Celeste, 'Digital Constitutionalism' (n 5); Edoardo Celeste, *Digital Constitutionalism: The Role of Internet Bills of Rights* (Routledge 2022).

42 For a more detailed analysis of these three examples, see Celeste, *Digital Constitutionalism* (n 41) ch 4.

43 See Celeste (n 15), who reuses an expression originally employed in Christoph B. Graber, 'Bottom-up Constitutionalism: The Case of Net Neutrality,' Transnational Legal Theory 7 (2016), 524, 551.

44 Celeste (n 15).

45 Celeste, *Digital Constitutionalism* (n 41) 209 ff.

Pollicino offered a comprehensive reading of recent case law of the Court of Justice of the European Union highlighting its crucial role in protecting digital rights.[46] The subtitle of his book 'Judicial Protection of Fundamental Rights on the Internet: A road towards digital constitutionalism?' exposes the question of whether a form of 'digital constitutionalism' is also achieved through a substantive contribution by the EU judiciary.[47] De Gregorio singled out and analysed a 'European digital constitutionalism', explaining how the European constitutional architecture has been and is being used, especially by courts, to progressively limit the power of private digital platforms.[48] Constitutional values are seen as an instrument to progress from a phase of 'digital liberalism', dominated by the economic interests of European actors, to a stage of digital constitutionalism, more focusing on the protection of fundamental rights in the digital environment, through an intense judicial activism.[49] Finally, this general trend was also observed in the context of specific challenges, such as the regulation of online platforms.[50]

Besides this certainly more orthodox approach to digital constitutionalism focusing on traditional legal actors, we witness a parallel deepening of the scholarship on digital constitutionalism in relation to the development of specific innovative technologies.[51] Wimmer and Moraes analysed the impact of quantum computing on the right to encryption, as emerging and framed in initiatives inspired by digital constitutionalism, with a particular focus on Brazil.[52] In November 2022, the Academy of Sciences of Hamburg, in partnership with a plurality of other European universities and research

46 Oreste Pollicino, *Judicial Protection of Fundamental Rights on the Internet: A Road towards Digital Constitutionalism?* (Hart 2021).

47 See in particular ibid 5.

48 Giovanni De Gregorio, *Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society* (1st edn, Cambridge University Press 2022).

49 See in particular ibid 2.

50 For an EU-US comparative perspective, see Giovanni De Gregorio, 'Digital Constitutionalism across the Atlantic' (2022) 11 Global Constitutionalism 297; for an analysis from a broader perspective, focusing on issues related to Internet governance, see Giovanni De Gregorio and Roxana Radu, 'Digital Constitutionalism in the New Era of Internet Governance' (2022) 30 International Journal of Law and Information Technology 68.

51 Pereira and Keller first noticed this trend in relation to quantum computing: see Pereira and Keller (n 12).

52 Miriam Wimmer and Thiago Guimarães Moraes, 'Quantum Computing, Digital Constitutionalism, and the Right to Encryption: Perspectives from Brazil' (2022) 1 Digital Society 12.

institutes, hosted a workshop on 'quantum constitutionalism'.[53] The event aimed to reflect on the implications for the constitutional dimension of a future, more consistent deployment of quantum computing. The concept of digital constitutionalism inspired the whole workshop: the advent of quantum computing was intended as the beginning of a 'post-digital' era that would have produced new issues for contemporary constitutionalism. In other words, 'quantum constitutionalism' would be regarded as the new 'digital constitutionalism': the next challenge, and consequent reaction of the constitutional ecosystem to technological innovation.

C. Approaches

From this mapping of the scholarship on digital constitutionalism, it is possible to understand that in reality the adjective 'digital' does not qualify the substantive 'constitutionalism'; it is rather an adverbial denoting the context and challenges that this strand of contemporary constitutionalism addresses. The constitutional dimension is interpreted in a broad sense. The existing scholarship does not merely focus on constitutional law *stricto sensu*, but looks more generally at the constitutional 'ecosystem', its values, principles, actors, and how it is impacted by the digital revolution.[54] In the previous section, we have used a chronological way of describing the evolution of the scholarship on digital constitutionalism. In this section, we will analyse three potential ways to categorise the conceptual approaches adopted by the existing scholarship on digital constitutionalism.

I. Substantive categorisation

Pereira and Iglesias Keller proposed a 'substantive' categorisation based on the focus adopted by scholars engaging with digital constitutionalism.[55] According to this typology, a first group of scholars looks at digital constitutionalism as a normative phenomenon. It would consist in the emergence

53 See https://www.quantumconstitutionalism.org/.

54 In this sense see Edoardo Celeste, *Digital Constitutionalism: The Role of Internet Bills of Rights* (Routledge 2022) ch 2.

55 Pereira and Keller (n 12).

of Internet bills of rights, and, more broadly speaking, of initiatives articulating rights and principles to address the challenges of the digital age.[56] A second group of scholars identifies a 'rearrangement of constitutional protections' following the digital revolution, focusing in particular on the emergence or rearticulation of new rights.[57] In this group we find scholars using these values and principles also to derive criteria for judicial review.[58] This group's view of digital constitutionalism is considered to be compatible with a 'traditional view of constitutionalism', by resulting in simple additions of layers or identification of lenses within contemporary constitutionalism, as it was done with concepts such as environmental constitutionalism.[59] A third group would instead use digital constitutionalism as a 'theoretical framework for state and non-state means of applying the law to digital technologies'.[60] The scholars mentioned in this category mainly deal with mechanisms of limitation of the power of private tech actors, both in terms of state regulation and as a form of self-constitutionalisation.[61]

56 In this group they mention: Dennis Redeker, Lex Gill and Urs Gasser, 'Towards Digital Constitutionalism? Mapping Attempts to Craft an Internet Bill of Rights' (2018) 80 International Communication Gazette 302; Claudia Padovani and Mauro Santaniello, 'Digital Constitutionalism: Fundamental Rights and Power Limitation in the Internet Eco-System' (2018) 80 International Communication Gazette 295; Celeste, 'Digital Constitutionalism' (n 5).

57 Pereira and Keller (n 12) 2669; In this group are mentioned: Oreste Pollicino, *Judicial Protection of Fundamental Rights on the Internet: A Road towards Digital Constitutionalism?* (Hart 2021); Wimmer and Moraes (n 52).

58 See Mendes and Oliveira Fernandes (n 6).

59 Pereira and Keller (n 12) 2672, translation by the authors.

60 Pereira and Keller (n 12) 2672.

61 In this group are mentioned: Nicolas Suzor, Tess Van Geelen and Sarah Myers West, 'Evaluating the Legitimacy of Platform Governance: A Review of Research and a Shared Research Agenda' (2018) 80 International Communication Gazette 385; Angelo Golia, 'The Critique of Digital Constitutionalism' <https://papers.ssrn.com/abstract=4145813> accessed 14 August 2023; Giovanni De Gregorio, *Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society* (1st edn, Cambridge University Press 2022).

II. Theoretical categorisation

Duarte et al. proposed to identify three 'theoretical' components of digital constitutionalism: a liberal, a societal and a global one.[62] Rather than a categorisation of existing theories, the authors describe what they call three approaches to digital constitutionalism, which have not to be intended as mutually exclusive, but rather as three layers of the same conceptual architecture. Digital constitutionalism would find its roots into the liberal constitutionalism emerged to protect freedoms against the intrusion of public actors. Duarte et al. rightly notice that the affirmation of private actors as dominant players besides nation States in the digital environment represents a challenge to a *liberal* constitutionalism that is anchored to the state-centric dimension. This part of the digital environment where private actors establish their own 'constitutional' rules and implement them is captured by a *societal* reading of digital constitutionalism, which relies on theories of societal constitutionalism. Within society, state-centred and private-focused constitutional inputs may collide. A way to overtake this problem is to look at digital constitutionalism from a *global* perspective. Relying on multilevel theories, constitutional collisions and different societal input can be regarded comprehensively.

III. Normative categorisation

The substantive categorisation proposed by Pereira and Iglesias Keller is useful to provide an immediate idea of the focal point of the research at stake. It emerges from an empirical analysis of the existing literature on digital constitutionalism and will certainly benefit future attempts of categorising emerging scholarship on this phenomenon, with the caveat that the three groups identified by Pereira and Iglesias Keller are not mutually exclusive. In particular, scholars falling into the third group, who are studying public and private mechanisms to enforce the law in the context of the digital environment, could well analyse how to adjust existing constitutional protections, thus equally involving elements belonging to the second group. Duarte et al.'s theoretical categorisation is equally helpful as it distinguishes the existing scholarship from the point of view of the specif-

62 Francisco de Abreu Duarte, Giovanni De Gregorio and Angelo Golia, 'Perspectives on Digital Constitutionalism' <https://papers.ssrn.com/abstract=4508600> accessed 14 August 2023.

ic, underlying approach to constitutionalism which is adopted. Once again, however, the three categories proposed are not mutually exclusive; they represent three theoretical layers that can well co-exist, one encompassing another. For example, if one adopts a global constitutionalist approach, one can well still focus their research on aspects related to a liberal conception of constitutionalism, as one assumes the emergence of constitutional responses at various levels of the constitutional ecosystem.

This paper proposes a further categorisation, which can help complement, and can be used in conjunction with, the previous ones. It presents four approaches to digital constitutionalism and it is a 'normative' categorisation. Not normative in the sense that it is prescriptive, but meaning that it is legal or juristic in nature, by distinguishing these four categories based on the normative sources they refer to. This categorisation contributes to the existing literature by isolating positions that are not fully apparent in the previous categorisations and by highlighting aspects that are key to understand some of the criticism that was addressed to the theories of digital constitutionalism. By summarising the previous categorisations and by presenting these four approaches, this paper aims to allow colleagues to position themselves in the current scholarly debate, without having necessarily to look for a univocal definition of the concept of digital constitutionalism, that might even stifle the plural and participative nature of the current academic conversation.

The present categorisation questions which normative source is considered to include elements that translate the core principles of contemporary constitutionalism in light of the challenges of the digital society. This categorisation adopts an empirical approach and disregards the labels that scholars may have adopted for their theories, if any. The first category is represented by the *traditional* constitutionalist approach. This group of scholars adopts a classical conception of the system of legal sources. Analyses related to digital constitutionalism in this first group investigate how constitutional law is reacting to the challenges of the digital revolution. The normative sources examined are those traditionally regarded as possessing a constitutional character and include: constitutions, acts of constitutional nature, decisions of courts possessing constitutional review or interpretation power. These sources can emerge both at national and at supranational level. This approach focuses on state-centric constitutional counteractions and overlaps with Pereira and Iglesias Keller's second group, which focuses on the 'rearrangement of constitutional protections' following the digital

revolution, and with Duarte's first approach of liberal constitutionalism.[63] Scholars adopting this approach include Pollicino, De Gregorio, Mendes and Oliveira.[64]

The second approach can be defined as 'functional and legal'. In this category we include scholars who looked at norms that belong to the traditional system of legal sources, but lie outside the scope of constitutional law. In this sense, this approach is still legal, but functional: it looks in an empirical way at whether a normative source performs a constitutional function despite being formally devoid of this nature. Authors such as Fitzgerald and Suzor, for example, adopt this approach by highlighting the role that private contract law can play in setting constitutional constraints to the power of private actors.[65] Equally, Floridi points at the constitutionalising role played by a series of pieces of EU regulation – the 'hexagram' in Floridi's words – that represent the pillars of EU digital law.[66] This approach echoes Pereira and Iglesias Keller's third category, which focuses on public and private means of regulating digital technology, but it is not easy to position within Duarte's et al.'s categorisation.

The third category still maintains a functional approach, but articulated in a socio-legal way. Here we go beyond the traditional system of legal sources. Norms of constitutional nature are found beyond the state dimension, in the private rules and enforcement mechanisms established by technology companies, in the decisions of ICANN's dispute resolution mechanisms, in the myriads of Internet bills of rights mainly promoted by civil society actors. This approach can be defined as 'functional and socio-legal' because it empirically looks beyond what is formally constitutional, detecting norms emerging outside the institutionalised, state-centric, legal dimension that produce constitutional counteractions to the challenges of the digital society. This approach reflects Duarte et al.'s layer of societal

63 Pereira and Keller (n 12) 2669.

64 Pollicino (n 57); De Gregorio (n 61); Mendes and Oliveira Fernandes (n 6), who in reality also acknolwedge the role of a plurality of other sources, even those emerging beyond the State, in the framework of digital constitutionalism.

65 Brian Fitzgerald, 'Software as Discourse? The Challenge for Information Law' (2000) 22 European Intellectual Property Review 47; Suzor, 'The Role of the Rule of Law in Virtual Communities' (n 14).

66 Luciano Floridi, 'The European Legislation on AI: A Brief Analysis of Its Philosophical Approach' (2021) 34 Philosophy & Technology 215, 220. With the expression 'hexagram' Floridi refers to the AI Act, the GDPR, the Digital Markets Acts, the Digital Services Act, the Data Governance Act and the European Health Data Space Regulation.

constitutionalism, while it overlaps with both the first and the third group as identified by Pereira and Iglesias Keller, respectively referring to the category of scholars studying the emergence of Internet bills of rights and that analysing non-state constitutional answers. In this group we can include scholars, such as Padovani, Redeker, Yilma, Celeste, Santaniello, Palladino and Golia.[67]

The fourth approach can be defined as 'holistic'. This category presents the most comprehensive scope of analysis. It encompasses the previous three approaches by arguing that the constitutional ecosystem reacts to the challenges of the digital revolution at multiple levels, with a plurality of counteractions. In this sense, we can observe a multilevel[68] or hybrid[69] process of constitutionalisation of the digital society: new normative responses simultaneously emerge in traditional constitutional sources, in legal sources playing a constitutional role and in a variety of normative instruments arising beyond the State, in the private fiefs of multinational tech companies or at the level of civil society. This holistic approach recognises a degree of complementarity of these normative responses. It does not downplay the importance of norms emerging outside traditional legal instruments. It argues that, like in a puzzle, each source complements each other. There is a mutual stimulation and, taking an aerial view of this phenomenon, it is possible to observe the emergence of a plural, but single-focused conversation on the constitutional answers to the digital revolution. This approach investigates the 'alarm signs' that each normative source is providing to the rest of the constitutional ecosystem. For example, by analysing the content of the multiple Internet bills of rights emerged at the level of civil society it is possible to detect areas of what I called 'constitutional anaemia' within traditional constitutional sources: traditional constitutional instruments struggle to address the challenges of the digital revolution and civil

67 See Musiani, Pavan and Padovani (n 29); Redeker, Gill and Gasser (n 56); Kinfe Micheal Yilma, 'Digital Privacy and Virtues of Multilateral Digital Constitutionalism—Preliminary Thoughts' (2017) 25 International Journal of Law and Information Technology 115; Celeste, 'Terms of Service and Bills of Rights' (n 21); Santaniello and others (n 11); Edoardo Celeste and others, *The Content Governance Dilemma: Digital Constitutionalism, Social Media and the Search for a Global Standard* (Palgrave Macmillan 2023) <https://link.springer.com/10.1007/978-3-031-32924-1> accessed 8 August 2023; Golia (n 61).

68 See Celeste, 'The Constitutionalisation of the Digital Ecosystem' (n 38).

69 See Santaniello and others (n 11).

society is advocating for an evolution of formal constitutional sources.[70] This approach is at the same time traditional, functional and socio-legal. It encompasses the three groups identified by Pereira and Iglesias Keller, and is in line with the third layer of digital constitutionalism proposed by Duarte et al, which focuses on global constitutionalism. I first proposed this holistic theory in order to offer a theoretical framework to reconcile the existing scholarly positions on digital constitutionalism.[71]

D. Criticism

After a phase of development and growth, the literature on digital constitutionalism has also been subject to criticism. The aim of this section is to systematise the main arguments moved against theories of digital constitutionalism. We can identify three macro-categories of criticism: a conceptual, a cynic and a traditional argument.

I. Conceptual argument

The analysis of the various potential approaches to digital constitutionalism has clearly shown the lack of a dogmatic, univocal definition of this concept. This plurality of views is regarded as an issue related to the clearness of the notion of digital constitutionalism. Some definitions of this concept are criticised to be inconsistent or contradictory. According to Pereira and Iglesias Keller, this is a 'problem of conceptual disarray that weakens the epistemic value of the term and jeopardises current applications'.[72] The concept of digital constitutionalism would be regarded as unclear because it covers a multitude of actors, normative sources and mechanisms.

As a consequence, digital constitutionalism theories might also be accused of lacking a clear positioning within existing constitutional theories. Duarte et al. highlighted the complex mix of constitutionalist theories – liberal, societal and global – underlying the various scholarly visions of digital

70 Celeste, *Digital Constitutionalism* (n 41) ch 13.

71 See Edoardo Celeste, 'Digital Constitutionalism: Mapping the Constitutional Response to Digital Technology's Challenges' (2018) HIIG Discussion Paper Series No 2018-02 <https://papers.ssrn.com/abstract=3219905> accessed 23 August 2018; Celeste, 'Digital Constitutionalism' (n 5).

72 Pereira and Keller (n 12) 2652.

constitutionalism.[73] Pereira and Keller speak of a 'theoretical matrix' comprising constitutional pluralism, societal constitutionalism, global constitutionalism, and we could add, transnational constitutionalism and multilevel constitutionalism. Two lines of criticism are thus possible in this regard: on the one hand, one might argue that digital constitutionalism does not receive a clear rooting among the theories evoked by scholars engaging with this concept, and on the other hand, it might not be clear how digital constitutionalism stands within recent scholarly debates on the decline of constitutionalism[74] or the emergence of new types of constitutionalism.[75]

Moreover, digital constitutionalism was criticised for its lack of a univocal ideological or political orientation. Golia specifically criticised my use of a 'sanitised' notion of ideology to denote the nature of digital constitutionalism. I indeed defined digital constitutionalism as the 'ideology that adapts the values of contemporary constitutionalism to the digital society', specifying that the notion of ideology here is used in a neutral sense, as a set of ideals and values, and not in the Marxist pejorative sense of set of deceiving beliefs.[76] Along the same lines, Griffin criticizes the absence of a clear political orientation, proposing a 'left-wing normative account of digital constitutionalism' aiming to limit the power of private technology corporations.[77]

Finally, one last critique related to the conceptual boundaries of digital constitutionalism consisted in arguing that this notion engages with new issues that are generated by the advent of the digital revolution, rather than with problems which are connatural to contemporary society.[78] It would be mistaken to think that digital constitutionalism aims to restore a heavenly

73 de Abreu Duarte, De Gregorio and Golia (n 62).

74 See Dobner and Loughlin (n 9).

75 See Ran Hirschl, *Towards Juristocracy: The Origins and Consequences of the New Constitutionalism* (Harvard University Press 2007); Stephen Gill and A Claire Cutler (eds), *New Constitutionalism and World Order* (Cambridge University Press 2014); Detlef Nolte and Almut Schilling-Vacaflor (eds), *New Constitutionalism in Latin America: Promises and Practices* (Routledge 2012); Roberto Gargarella, 'Sobre el "Nuevo constitucionalismo latinoamericano"' (2018) 27 Revista Uruguaya de Ciencia Política 109.

76 Celeste, 'Digital Constitutionalism' (n 5) 77; see also Maurice Cranston, 'Ideology' <https://www.britannica.com/topic/ideology-society> accessed 30 August 2018.

77 Rachel Griffin, 'A Progressive View of Digital Constitutionalism' (*The Digital Constitutionalist*, 14 June 2022) 2 <https://sciencespo.hal.science/hal-03940791> accessed 16 August 2023.

78 Golia (n 61) 12.

constitutional equilibrium that characterized the analogue society. Digital constitutionalism would rather aim to identify persisting constitutional questions 're-shaped by digitality'.[79]

II. Cynical argument

The second stream of criticism to digital constitutionalism can be named 'cynical' as it questions the sincerity of the reference to the constitutional dimension by private actors. In light of their significant development, social media have been compared with States. Already after half a decade of existence, Mark Zuckerberg could argue that the number of Facebook's users were the same of those of a populated country.[80] Thinking of social media platforms as virtual state entities was not only justified by these figures, but also reinforced by the use of a specific 'constitutional' language in the social media terms of service. For example, Facebook used to call its terms of service 'Statement of Rights and Responsibilities' and the Facebook's Principles used to employ the expression 'every person', which echoes the formulation of constitutional texts.[81] More recently, Facebook introduced the Oversight Board, a private jurisdictional body vested with the function of solve the most complex content moderation cases.[82] This institution has been compared to a private 'supreme court', in any case denoting a trend of institutionalization and judicialization of a private space inspired by state constitutional architecture.[83] In light of this trend, I spoke of a 'constitutional tone' that would justify the question of whether the internal rules of online platforms could be regarded as their 'bills of rights', set of norms playing a de facto constitutional role within the virtual territory of a specific social media.[84]

79 Golia (n 61) 12.

80 Jonathan Zittrain, 'A Bill of Rights for the Facebook Nation' (*The Chronicle of Higher Education*, 20 April 2009) <https://www.chronicle.com/blogs/wiredcampus/jonathan-zittrain-a-bill-of-rights-for-the-facebook-nation/4635> accessed 30 August 2018.

81 See Celeste, 'Terms of Service and Bills of Rights' (n 21) 123.

82 See Kate Klonick, 'The Facebook Oversight Board: Creating an Independent Institution to Adjudicate Online Free Expression' (2019) 129 Yale Law Journal 2418; Wolfgang Schulz, 'Changing the Normative Order of Social Media from Within: Supervisory Bodies' in Edoardo Celeste, Amélie Heldt and Clara Iglesias Keller (eds), *Constitutionalising Social Media* (Hart 2022).

83 See Celeste and others (n 67) ch 2.

84 Celeste, 'Terms of Service and Bills of Rights' (n 21).

These examples show an appropriation of the constitutional language, which is traditionally deployed in the context of nation States, by an environment that is conversely dominated by private actors. The core cynical argument moved to this trend consists in affirming that the use of this constitutional tone is merely superficial, a 'constitutional façade'.[85] Pereira and Keller speak of a 'descriptive' or 'metaphorical' employment of constitutional concepts.[86] Here the traditional language and mechanisms of state constitutional law would be transplanted into private virtual domains without any effort of adapting this normative infrastructure to the peculiarities of the online environment. This repurposed constitutional rhetoric would have a high evocative power, but unclear contours. The idea that what we could call 'constitutional appeal' generates among users would then represent a marketing tool, or in the words of Albert, a 'legal talisman', capable of disguising into constitutional a private setting devoid of basic constitutional guarantees.[87]

Hence the core danger highlighted by this cynical argument. The reference to the constitutional dimension would not only be fake, but essentially dangerous in so far it is instrumentalised to increase the legitimacy of private ruling, which is intrinsically at odds with the principles of constitutional democracy.[88] Pereira and Keller speak of 'constitutions without constitutionalism'.[89] They highlight a risk not only to 'disguise' private power, but also to 'reinforce' it, despite the original intent of digital constitutionalism to introduce limitations to the dominance of online platforms.[90]

85 See Celeste, 'Terms of Service and Bills of Rights' (n 21) 128; Pereira and Keller (n 12) 2651 and 2656, who speak of 'mere rhetorical device', 'semantic or facade constitutions'; Róisín Á Costello, '*Faux Ami?* Interrogating the Normative Coherence of "Digital Constitutionalism"' (2023) 12 Global Constitutionalism 326, 7, who speaks of a 'descriptive rhetoric of constitutionalism' .

86 Pereira and Keller (n 12) 2656.

87 Kendra Albert, 'Beyond Legal Talismans' (Berkman Klein Center for Internet & Society, Harvard University, 10 November 2016) <http://opentranscripts.org/transcript/beyond-legal-talismans/> accessed 21 December 2018; see also Celeste, 'Terms of Service and Bills of Rights' (n 21).

88 See Pereira and Keller (n 12) 2652, who speak of an 'instrumentalization of "constitutionalism" for illiberal purposes and their transposal onto supra-state or even private dynamics' (authors' translation).

89 Pereira and Keller (n 12) 2656.

90 Pereira and Keller (n 12) 2675.

III. Traditional argument

The third line of criticism moved to theories of digital constitutionalism can be defined as 'traditional', in the sense that it is anchored to a classical conception of constitutionalism and the legal system.

Constitutionalism is traditionally associated with the state dimension. It is an ideology that emerged to limit the power of the State and, subsequently, to legitimise – and by doing so, to *constitute* and organise – the power of the latter stemming from popular sovereignty.[91] Digital constitutionalism theories apply the concept of constitutionalism not only beyond the state dimension, but also to private actors. Technology companies' attempt to establish core values and principles as well as to limit their power by introducing internal control mechanisms is described in terms of 'constitutionalisation' of these private spaces.[92] Such an unorthodox approach would lead to a stretching of the concept of constitutionalism beyond its natural ecosystem. Scholars professing a constitutional purism would consider this concept dilatation as illegitimate or uncanonical per se. Constitutional scholars adopting a more pragmatic approach see here the risk of a contamination, denaturation, not to say a degradation of traditional constitutionalism. Pereira and Iglesias Keller talk of a risk of trivialization or hollowing out the concept of constitutionalism.[93] What in reality is mere private actors' self-regulation cannot be disguised as a form of constitutionalisation. The 'normative core' of constitutionalism is not there.[94] Applying the notion of constitutionalism beyond the State would amount to an offense to the constitutional dimension.

Costello argues that using the language of constitutionalism beyond the State and in the context of private actors may be 'harmful', may lead to 'confusion'.[95] Here we see this line of criticism converging with the cynical

91 See Charles Howard McIlwain, *Constitutionalism: Ancient and Modern* (Amagi, originally published by Cornell University Press, 1947, 2007); András Sajó, *Limiting Government: An Introduction to Constitutionalism* (Central European University Press 1999); András Sajó and Renáta Uitz, *The Constitution of Freedom: An Introduction to Legal Constitutionalism* (Oxford University Press 2017).

92 On the idea of using elements of constitutional law to describe dynamics of private actors see Suzor, 'Digital Constitutionalism' (n 14); Karavas (n 19); Teubner (n 10); Celeste, 'Terms of Service and Bills of Rights' (n 21).

93 Pereira and Keller (n 12) 2676.

94 Costello (n 85) 8 ff.

95 Costello (n 85) 15.

argument presented above that posits that the appropriation of the constitutional language by private entities conceals the risk of instrumentalising the appeal of constitutionalism to legitimise private practices that are all but in line with constitutional principles and values. Costello's solution is to abandon the expression 'digital constitutionalism', avoid employing the dichotomy between private and public law in this context, but rather refer to the interaction between public and private 'policy'.[96] In relation to this very last point, it is apparent here how this line of traditional criticism highlights a mistaken extension not only the concept of constitutionalism, but also of the boundaries of the legal system itself. It is possible to read a general suffering against a perceived 'pan-constitutionalism', an undue expansion of the constitutional dimension to areas that would be traditionally considered as the realm of other sources of law - such as private law, for instance – or as extra-legal fields – as in the case of private platforms' self-regulation.[97]

Finally, if the critical arguments expressed above relate to the application of constitutional labels beyond the state and in the domain of private actors, there is also a line of criticism that is moved to specific trends that implement the idea of digital constitutionalism. In particular, Yilma points out to a series of risks inherent to the emergence of a significant number of Internet bills of rights.[98] He criticises the fragmented nature of this phenomenon, questions their impact, but also analyses the issue of their 'desirability'.[99] In this regard, we find here a traditional line of criticism as Yilma speaks of a constitutional 'hypertrophy' that would derive from an 'inflation' of rights.[100] The added value of the principles advocated by the plurality of actors that adopt and promote Internet bills of rights documents would be uncertain, if not counterproductive. Traditional constitutional instruments already include general formulations of the rights and principles that can be applied in the digital environment. Therefore, a duplication, especially through non legally binding documents, is unnecessary.

96 Costello (n 85).

97 Here I am re-elaborating with my own words an argument made orally by Prof Alessandro Mantelero at the workshop '*Digital Constitutionalism. A Normative And Institutional Framework For Conflict Solving Under Construction*' (Frankfurt, 3-4 March 2023).

98 Yilma (n 67); along the same lines, see also Yilma (n 30).

99 Yilma (n 67) 125.

100 Yilma (n 67) 126.

E. A counter-critique

The last section will conclude this chapter with a personal counter-critique to the three streams of criticism moved to theories of digital constitutionalism. The aim of this section is neither to set the final word on this topic nor to defend the normative 'truth' of theories of digital constitutionalism. Further academic discussions on this topic are welcome to enhance the understanding of the phenomena we are living. Current criticism has to be taken into account in a constructive way to further refine existing theories. It is however hoped that this contribution will help calibrate emerging critical lines by relating them to specific aspects of digital constitutionalism theories, rather than negating this concept tout court. The counter-critique will follow the systematisation of the critical lines identified in the previous section.

I. Pluralism, ideological orientation and normative counteractions

The concept of digital constitutionalism was criticised for its lack of clarity and consistency. Taking together the various positions taken by the existing scholarship, we a see that a complex plurality of actors and mechanisms is put under the umbrella of digital constitutionalism. This reconstruction is undoubtedly accurate. However, if on the one hand, this mosaic of theories, viewpoints, actors and mechanisms might generate confusion, on the other hand, it is a living witness of the complexity of the analysed phenomena and of the willingness to explain this trend from a plurality of disciplinary and theoretical perspectives. Such a diversity also means that we are observing a comprehensive scholarly effort to examine the phenomena underlying digital constitutionalism. Not to mention that the underlying concept of constitution, constitutionalism and constitutionalisation have never received a univocal definition. Here, the main counter-critique moves against generalising critical tendencies; arguing that digital constitutionalism theories miss the point does not give recognition to the various approaches that have emerged in this field. It is hoped that this paper will help both scholars supporting and criticising digital constitutionalism theories to better position themselves, to properly distinguish between the concept of constitutionalism and constitutionalisation, to explicitly state which approach they are taking or criticising.

Certainly, an effort that supporters of digital constitutionalism should make is to reconstruct more clearly the relationship between their argu-

ments and pre-existing theories, which represented one of the shortcomings highlighted by criticists. This will help to clarify that digital constitutionalism is not subverting the DNA of contemporary constitutionalism. When one speaks of digital constitutionalism as an ideology, one refers to a set of values and ideals with a clear ideological positioning. Digital constitutionalism is not a new form of constitutionalism, but rather one of its layers, a development of contemporary constitutionalism. Its scholarly discourse builds and further develops 'analogue' constitutional theory.

When one speaks of constitutional 'equilibrium' before the advent of the digital revolution, one does not imply a status of constitutional heaven, devoid of issues to solve, but one rather refers to the equilibrium between constitutional norms and societal issues. The constitutional ecosystem, at its various levels, provided a *normative* – but not necessarily factual – answer to the issues of the analogue society. The digital revolution has undermined this normative equilibrium. Existing norms no longer fully speak to the variety of social actors, no longer address the multiple issues that characterise the digital society. Hence, a series of normative counteractions are emerging.[101] To allow existing constitutional norms and principles to perpetuate their message in the mutated social reality where we live today. Digital constitutionalism would advocate a translation of the DNA of contemporary constitutionalism into norms that can address the challenges of the digital society. A living constitutional ecosystem, not only understandable by specialised audiences, but clearly providing normative guidance to all involved actors.

II. Constitutionalism as a lens

The lines of criticism that we have defined as 'cynical' questions the application of the language and tools of constitutionalism to private technology companies. These multinational entities would refer to constitutionalism as a marketing tool, to exploit the sense of trust that a 'constitutional appeal' generates in the users. Nothing but a mere constitutional façade would lead to legitimisation of practices and values that are in reality arbitrarily established by private corporations for their own interests.

The application of theories of digital constitutionalism in the domain of private technology companies does not aim to defend or justify their

101 Celeste, *Digital Constitutionalism* (n 41) ch 3 ff.

practices. Constitutionalism, its values and mechanisms are here used as a 'lens' to perform a 'litmus test' to examine the development of the governance of private platforms against constitutional norms and practices established in the state dimension. These entities have emerged as dominant actors besides nation States. They have the power to similarly affect the exercise of fundamental rights by their users. The concept of constitutionalism is deployed in this domain with much caution. Indeed, one has to distinguish the use of the constitutional machinery done by online platforms themselves and that performed by the scholarship. The first could be regarded as an effort of self-constitutionalisation; platforms would employ the language of constitutionalism in order to use its mechanisms and rely on its principles. However – there is no doubt – this phenomenon also hides a 'marketing' component. Private companies need to show to their users that their platforms are safe, that fundamental rights are respected, that their violations are timely prosecuted. Yet, the scholarship resorts to digital constitutional theories not to justify or legitimise the conduct of multinationals, but rather to understand to what extent these actors are pursuing a path of constitutionalisation, which has been long studied in the context of States, both at national and at supranational level.

Differentiating between the concepts of digital constitutionalism, as a set of values and ideals, and the process of constitutionalisation, which represents the implementation of these principles, is helpful in this context to measure the developments – be they positive or negative – of private platforms. For example, Facebook once announced its willingness to let users vote on its terms of service – a promise that, if maintained, would have certainly represented a step forward in the process of constitutionalisation of this entity.[102] Facebook, once again, introduced an Oversight Board to adjudicate the most complex cases related to online content moderation, an entity that is still subject to the control of the platform, but is at least composed of external international experts. In these contexts, the reference by the scholarship to a constitutionalising trend does not imply a full constitutionalisation of this private space. Conversely, one aims to assess the progress, or lack thereof, made by the platform. The language and mechanisms of constitutionalism, at least in the academic analysis, do not contribute to legitimise arbitrary practices of private companies. Digital constitutionalism is not used as a 'legal talisman' to obfuscate the eyes of the users, as conversely companies themselves might do. The scholarship here

102 See Celeste, 'Terms of Service and Bills of Rights' (n 21).

refers to constitutional theories as a lens to measure to what extent these new private dominant actors are incorporating mechanisms of protection of fundamental rights by adapting existing constitutional values and tools that have been developed in the context of nation States.

III. New battlefield for old enemies

What in the previous section we called the 'traditional' line of criticism to theories of digital constitutionalism questions an undue stretching of the concept of constitutionalism beyond the State dimension and its unwarranted application to private actors. This circumstance would lead to a denaturation and a voiding of traditional constitutionalism as well as to a hazardous legitimisation of private power. Pereira and Keller themselves however acknowledge that these critical arguments are not new.[103] They had already been moved to the various streams of global and societal constitutionalism as well as to the underlying assumption of constitutional pluralism, which, according to these scholars, represent the 'theoretical matrix' at the basis of digital constitutionalism.[104] In other words, digital constitutionalism becomes the new battlefield of old enemies. Those adopting a traditional approach to constitutionalism reiterate the same types of critiques addressed to scholars supporting an extension of constitutionalism beyond the State.

Digital constitutionalism does not empty or dilute the meaning of constitutionalism when applying a constitutional analysis to the power of private platforms. Firstly, because the constitutional dimension is used as a lens that assess the effectiveness of private norms and mechanisms that play a function that de facto can be considered as constitutional. This does not amount to argue that a copy of what Costello calls the 'normative core' of state constitutionalism is there.[105] On the contrary, state constitutionalism is used as a litmus test to measure the level of progress of the process of constitutionalisation of private actors. State constitutionalism is a model, but this does not imply that the ideal solution would be to replicate in full what constitutionalism has achieved at state level into the realm of private

103 See Pereira and Keller (n 12) 2676 ff.

104 Pereira and Keller (n 12) 2651; for an analysis of international constitutional law, see Celeste, 'The Constitutionalisation of the Digital Ecosystem' (n 38).

105 Costello (n 85) 8.

platforms. Constitutionalism within and beyond the State can coexist, do not need to perfectly symmetrical, but rather aim to be complementary. Each compensating for the shortcomings of the other.[106]

Indeed, the projection of constitutional theories beyond the State does not negate state constitutionalism. It merely acknowledges the shortcomings of state constitutionalism and the consequent emergence of constitutional patterns beyond the State. If one takes a holistic approach to digital constitutionalism, this is even more apparent. Such a perspective allows the scholar to study the joint action of various constitutional layers that are addressing the challenges of the digital revolution. And this constitutional 'conglomerate' includes both traditional constitutional instruments and constitutional tools emerging beyond the State.[107] Theories of digital constitutionalism, by highlighting the development of a process of constitutionalisation beyond the State, indirectly show areas of constitutional anaemia of traditional state constitutionalism.[108] Failing to acknowledge this dimension would mean adopting a blind posture to existing constitutional issues as well as losing a useful theoretical lens to interpret these phenomena.

Drawing a strict equation between theories of digital constitutionalism and private self-regulation is reductive. As it would be limiting digital constitutionalism to traditional constitutional instruments. As shown in the previous sections, scholars studying digital constitutionalism adopt different perspectives. Each of these analytical angles is not mutually exclusive. And, at the same time, this does not imply a 'pan-constitutional' vision where every legal source is swallowed by the constitutional dimension. Constitutionalism is adopted as a lens beyond the traditional constitutional dimension: private law or the internal rules of private platforms will not become constitutions. However, if one adopts a functional, socio-legal approach, one can argue that they can play a constitutional function.[109] Digital constitutionalism aims indeed to study the limits of traditional constitutional law and how other normative sources are emerging to constitute the right mix that will be able to address the constitutional issues of the digital society. This does not imply a hypertrophic emergence of the constitutional discourse related to digital issues. On the contrary, this pluralism

106 On the notion of 'compensatory' constitutionalism, see Peters (n 8); for an adaptation of this theory to the digital context see Celeste, 'Internet Bills of Rights' (n 35); Celeste, 'The Constitutionalisation of the Digital Ecosystem' (n 38).

107 See Celeste, 'Internet Bills of Rights' (n 35).

108 See Celeste, *Digital Constitutionalism* (n 41) ch 13.

109 See Celeste, *Digital Constitutionalism* (n 41).

importantly highlights the absence of a single, clear, constitutional pathway to solve the challenges of the digital revolution, the consequent need to have a plural conversation to discuss legal solutions, and – luckily – the willingness of various societal actors to contribute to the conversation on which rights and principles should govern the digital society.

Bridging Legislation and Jurisprudence in Democratic Digital Constitutionalism: A Look at the Brazilian Supreme Court's Approach

Gilmar Ferreira Mendes and Victor Oliveira Fernandes

Abstract: While digital constitutionalism has traditionally centered on private governance systems, Brazil's recent jurisprudence signals reassertion of rights-based judicial review to counter threats in increasingly digitized societies. This paper analyzes how the Brazilian Supreme Court has built upon legislation encapsulating digital constitutionalism values to catalyze a paradigm shift constraining state surveillance and citizen data exploitation through renewed fundamental rights. By interpreting open-textured statutory embodiments of "proto-constitutional" internet protections, the Court has legitimized innovation as directly responsive to legislative signals. Thereby rather than substituting its own value judgments, these landmark decisions apply digital constitutionalism values to questions raised by Brazil's rights-centric internet governance regime. The analysis counters claims that digital constitutionalism broadly serves to legitimize corporate self-interest or dilute accountability through "legal talisman" rhetoric removed from genuine rights protection.

A. Introduction

Over the past decade, the digital constitutionalism movement has gained considerable recognition within academic circles. As the prevailing body of literature indicates[1], the term "ideological current" commonly refers to a

1 Edoardo Celeste, 'Digital Constitutionalism: A New Systematic Theorisation' (2019) 33 International Review of Law, Computers and Technology 76, 89; Claudia Padovani and Mauro Santaniello, 'Digital Constitutionalism: Fundamental Rights and Power Limitation in the Internet Eco-System' (2018) ("*digital constitutionalism is an effort to bring political concerns and perspective back into the governance of the Internet, deeply informed by economic and technical rationalities*") 80 International Communication Gazette 295; Meryem Marzouki, 'A Decade of CoE Digital Constitutionalism Efforts: Human Rights and Principles Facing Privatized Regulation and Multistakeholder Gov-

systematic framework defined by shared principles and guidelines aimed at recognizing, asserting, and safeguarding fundamental rights within the domain of cyberspace[2]. The label digital constitutionalism serves as a succinct representation of a dynamic intellectual movement, encompassing theoretical frameworks proposing the adaptation of foundational tenets of constitutionalism to the sphere of digital society. This school of thought advocates for the extension of traditional constitutional rights, obligations, and limitations to online interactions and virtual spaces, arguing that constitutional norms must evolve to remain relevant in an increasingly digitized world. Proponents emphasize that digital constitutionalism is essential to protect citizens' rights and regulate the powers of both state and corporate actors in the digital era. Broadly, the expression emphasizes the functioning of private self-regulatory frameworks that purportedly mirror constitutional values.

While scholars broadly agree on these core elements of digital constitutionalism concept, close inspection reveals limitations in this apparent clarity. After nearly a decade, it has become evident that the label lacks a uniform meaning and encompasses varied, potentially conflicting interpretations[3]. Some descriptive accounts have shifted the debate on platform regulation towards governmental solutions. Other scholars critique the strategic use of the term by private companies as a "marketing ploy" or "legal talisman" to divert scrutiny of unfair service terms[4]. As Costello concisely underscored, "the majority of online governance structures that have embraced constitutionalist rhetoric to self-describe should be viewed not as authentically constitutionalist, but rather as manifesting 'private policy' architectures" [5].

The prevalence of these self-legitimizing narratives from private entities highlights the need to examine the normative dimensions of digital

---

ernance' (2019) July International Association for Media and communication Research Conference (IAMCR).

2 Gilmar Ferreira Mendes & Victor Oliveira Fernandes, *Digital Constitutionalism and Constitutional Jurisdiction: A Research Agenda for the Brazilian Case*, *in* The Rule of Law in Cyberspace. Law, Governance and Thecnology Series. Volume 49 65, 67 (2022).

3 Jane Reis Gonçalves Pereira & Clara Iglesias Keller, *Constitucionalismo Digital: contradições de um conceito impreciso*, 13 Rev. Direito e Prax. 2648 (2022).

4 Edoardo Celeste, Digital Constitutionalism: The Role of Internet Bills of Rights 52 (2023). (referring to the expression adopted by Kendra Albert).

5 Róisín Á Costello, *Faux ami? Interrogating the normative coherence of ' digital constitutionalism ,'* Glob. Const. 1, 4 (2023).

constitutionalism more closely. This trend features prominently in recent European scholarship. Authors such as Gregorio[6] and Pollicino[7] have proposed that digital constitutionalism is undergoing a new democratic phase, characterized by the affirmation of novel fundamental rights via European Court of Justice (ECJ) decisions and European Parliament legislation constraining the private authority of large platforms[8].

Compared to Europe, developments in Brazil offer important insights for shaping this emergent phase of digital constitutionalism. In recent years, digital constitutionalism principles of safeguarding fundamental rights online have guided the Brazilian Supreme Court (STF) in reviewing the constitutionality of legislation. Rather than legitimizing self-regulation, this jurisprudential evolution has established constitutional duties for both state and private entities to protect rights in the digital realm. The Brazilian experience demonstrates how judicial review grounded in digital constitutionalism can delineate obligations, not just for the state, but also for non-state actors.

This paper will be structured in two main parts. Section 1 will chart the evolution of digital constitutionalism scholarship, highlighting the initial neglect of constitutional judicial review in protecting fundamental rights. It will analyze seminal works focusing on private self-regulation frameworks with limited state oversight. Section 2 will detail the Brazilian Supreme Court's recent case law demonstrating digital constitutionalism's democratic turn. It will examine landmark decisions constraining both public and private power to safeguard novel fundamental digital rights. This case law will be situated as affirming rights legislation envisioned by digital constitutionalism proponents. Finally, the conclusion will summarize how the Brazilian experience illuminates digital constitutionalism's emerging rights-centric phase with a more balanced approach to governing online spaces.

---

6 Giovanni de Gregorio, Digital Constitutionalism in Europe Reframing: Reframing Rights and Powers in the Algorithmic Society (2022).

7 Oreste Pollicino, Judicial Protection of Fundamental Rights on the Internet: A Road Towards Digital Constitutionalism? (2021).

8 Gregorio, *supra* note 6 at 65.("*two primary drivers have characterized the rise of the democratic phase of European digital constitutionalism. Firstly, the Union codified some of the ECJ's judicial lessons. Secondly, the Union introduced new limits to private powers by adopting legal instruments by increasing the degree of transparency and accountability in content moderation and data processing*").

B. The neglected role of judicial review in Digital constitutionalism early scholarship

The digital constitutionalism movement was originally meant to denote a movement to constrain the private authority of internet actors, as distinct from limiting state power[9]. In this vein, Fitzgerald[10] highlighted the existence of an "informational constitutionalism" in which both public and private entities would participate in constructing the legal order. The author's initial theorization practically restricted the state's role to issuing private law statutes (such as intellectual property and contract law) that would somehow steer private self-regulation. Similarly, Suzor first employed the term "digital constitutionalism" to emphasize that the actions of private agents would be bounded by the contractual frameworks forming virtual communities[11]. Still focused on private ordering, Karavas invoked Teubner's concept of societal constitutionalism to underline the state's inability to regulate the fragmented complexity of digital domains[12].

These foundational studies of the intellectual movement strongly neglected the role of nation-states as both regulatory actors and adjudicators. As previously highlighted, digital constitutionalism appears to have confined its analytical gaze to the implementation of fundamental rights in abstract legal planes, disregarding the function of courts and constitutional tribunals. In fact, Berman[13] seems to have been the sole pioneer of the academic movement to contemplate the subjection of private entities to constitutional review. He conceived that constitutional courts could employ the constitution as a benchmark to elaborate fundamental values and resolve politically contentious issues in cyberspace[14]. However, Berman discounted the prospect of ordinary legislation reflecting constitutional principles that

9 Mendes and Fernandes, *supra* note 2 at 66.

10 Brian F. Fitzgerald, *Software as Discourse - A Constitutionalism for Information Society*, 24 Altern. Law J. 144 (1999).

11 Nicolas Suzor, *The Role of the Rule of Law in Virtual Communities.*, Tese de doutoramento - Queensland University of Technology 1 (2010), http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=63481022&site=ehost-live.

12 Vagias Karavas, Digitale Grundrechte: Elemente einer Verfassung des Informationsflusses im Internet (2007).

13 Paul Schiff Berman, *Cyberspace and the State Action Debate: The Cultural Value of Applying Constitutional Norms to "Private" Regulation*, 759 Univ. Color. Law Rev. (2005).

14 *Id.* at 1269.

bind private actors[15]. Thus, his perspective on constitutional adjudication remained drastically circumscribed.

The studies conducted by Gill et al.[16] fail to address the significance of constitutional courts. They use the term "digital constitutionalism" to describe the increasing number of normative reactions from both national and non-national entities. These reactions play a vital role in modern constitutionalism by effectively articulating constitutional principles and beliefs in order to secure political rights and restrict authority in the online domain. Hence, it is understandable that the authors opted to employ this framework to highlight the process of developing these standards through the collective consciousness of society. Nevertheless, Gill et al.'s methodology is restricted to the rise of internet bills of rights, treating them as the exclusive and genuine source for restraining private power in the digital realm. Their focus on constitutional law is limited to the understanding that certain formal digital legislation possesses a "pre-" or "proto-constitutional" nature, serving as intellectual foundations for the interpretation of formal constitutions[17].

The increasing significance of constitutional courts' rulings in shaping the understanding of online fundamental rights, particularly in the United States and the European Union, has created a new area of research focused on studying constitutional adjudication. Works such as Morelli and Pollicino, for example, started examining the use of metaphors by courts to convey constitutional values and principles in the context of digital media. Nevertheless, these authors seem to prioritize the argumentative framework of judicial decisions rather than their influence on the governance of cyberspace.

The literature's timid approach to constitutional review can be attributed to early digital constitutionalism scholarship, which held the belief that the internet's proliferation would lead to a crisis in the traditional constitutional model. This model is deeply entrenched in the sovereign authority of nation-states and primarily concerned with power dynamics within national boundaries. Recent years have shown that the prediction of the decline of the constitutional state paradigm has been diminished, as it is now

15 Celeste, *supra* note 1 at 8.

16 Lex Gill, Dennis Redeker & Urs Gasser, *Towards Digital Constitutionalism? Mapping Attempts to Craft an Internet Bill of Rights*, 7641 Res. Publ. No. 2015-15 Novemb. 9, 2015 (2015).

17 *Id.* at 6.

recognized that traditional forms of government still play a significant role in shaping online norms. In this vein, works such as Goldsmith and Wu[18] notably demonstrated that national legislation and regulations remain pivotal sources of normativity in the internet era. Thus, even in online disputes, the territorial criterion of jurisdiction is far more significant than one might assume.

For various reasons, digital constitutionalism narratives centered on private agency have become obsolete in the face of a new "democratic" phase, as authors like Gregorio[19] have identified emerging within the context of European digital constitutionalism. As this scholar explains, the gap between public and private power exercising has recently spurred the European Union to abandon digital liberalism, based on the consensus that consolidation of private authority jeopardizes democratic systems and the rule of law principle. In this paradigmatic shift, Gregorio notes, "the ECJ's judicial activism paved the way from an early approach based on digital liberalism to a new phase of digital constitutionalism characterized by the reframing of fundamental rights and the injection of democratic values into the digital environment"[20].

The democratic aspects of digital constitutionalism shed new light on this emerging concept. Given Brazil's unique circumstances, the normative dimensions of this movement have been especially influential in shaping the recent jurisprudence of the Brazilian Supreme Court. The Brazilian case clearly demonstrates how digital constitutionalism can direct constitutional courts to articulate the boundaries of fundamental rights in the digital realm by channeling core constitutional values and principles. Through examples like Brazil, we see how digital constitutionalism provides a framework for courts to apply constitutional rights to new digital contexts.

C. Strengthening democratic digital constitutionalism: lessons from the Brazilian experience

In contrast to jurisdictions that only witnessed non-binding declarations of counter-normative reactions, Brazil incorporated digital constitutionalism

18 Jack Goldsmith & Tim Wu, Who Controls the Internet? lllusions of Borderless World (2006).

19 Oreste Pollicino & Giovanni De Gregorio, *Constitutional Law in the Algorithmic Society*, *in* Constitutional Challenges in the Algorithmic Society 3 (2021).

20 Gregorio, *supra* note 6 at 64.

general clauses directly into legislation, particularly in the Marco Civil da Internet. The law's incorporation of fundamental principles regarding privacy, autonomy, and transparency played a crucial role in facilitating subsequent judicial review.

Through the inclusion of ambiguous criteria in enforceable laws, the Brazilian Congress granted the STF the dual role of interpreting and determining the extent of digital rights safeguards. The Court willingly accepted this assigned responsibility in interpreting ambiguous legal provisions. In Brazil, the combination of legislation and STF decisions has promoted the development of digital constitutionalism. The presence of unclear laws has allowed the Constitutional Court to interpret and apply constitutional rights in a specific manner.

The Brazil's Marco Civil da Internet (MCI) established general clauses and principles to shape individual rights online that subsequently guided judicial interpretation. The law prioritized general precepts protecting freedom of expression (art. 3, item I), privacy (art. 3, item II), and preserving the participatory architecture of the network (art. 3, item VII), delineating limits on safeguarding these rights vis-à-vis both public and private entities. At the same time, the open-ended nature of the MCI and related legislation has raised constitutional questions before STF, in recent years.

Some key cases adjudicated by the STF demonstrate how Digital constitutionalism has guided the construction of constitutional standards to safeguard emerging online rights. The inherent ambiguity of the MCI legal framework has resulted in judicial review centered on digital constitutionalism principles for preserving fundamental rights in the cyberspace. Significant legal cases like ADI 6,389 (2020) and ADI 6649 have upheld independent digital rights based on the constitutional values of the MCI as interpreted through the lens of Digital constitutionalism.

I. Approaching data protection as a novel fundamental right under Brazilian Constitution

In 2020, the Court issued a landmark decision in Direct Action of Unconstitutionality (ADI) 6,389, which challenged a provisional presidential decree. This decree compelled all telecom providers to share users' personal data like phone numbers and addresses with IBGE, the national census agency. The government claimed this unprecedented data sharing was necessary to enable remote census surveys during the COVID-19 pandemic.

The STF ruled the law unconstitutional for lacking minimal safeguards on data purpose and proportionality. The rapporteur, Justice Rosa Weber, affirmed Brazil's evolving recognition of data protection as an autonomous fundamental right. She held the law violated this right by authorizing mass data sharing absent any purpose or proportionality principles.

The STF rooted data protection in safeguarding human dignity against the endless exposure of informational self-determination in modern societies. Crucially, the Court situated this new right not as judicial overreach, but rather as built upon recent Brazilian digital legislation. The MCI notably enshrined data protection among key internet use principles in Brazil. The MCI's rights-based approach reflects the counter-norm generation of digital constitutionalism. The 2018 Data Protection Law further entrenched autonomous digital rights governing public and private data processing.

Significantly, by treating the MCI and Data Protection Law as emblematic of digital constitutionalism, the STF declared data protection an autonomous right requiring constitutional protection. Thereby the Court concretized a core right of this constitutional movement. The STF leveraged these legislative symbols of constitutional values to chart an unanticipated expansion of rights online.

This reasoning countered accusations of undemocratic judicial activism detached from legislation. Instead, the Court portrayed its ruling as directly flowing from recent Brazilian law symbolizing awakening threats to fundamental rights. Rather than substituting its own values, the STF anchored expanded rights in counter-normative reactions from Brazil's democratic branches, consistent with digital constitutionalism's multi-institutional nature.

In articulating this new fundamental right, the STF stressed the diffusion of digital constitutionalism principles into jurisprudence. It characterized its ruling as judicial concretization of rights following the MCI's proto-constitutional digital rights agenda. Thereby, pioneering digital legislation in Brazil catalyzed reinterpreting enduring rights, viewed by proponents as the genesis of a new constitutional paradigm adapted to the digital age.

It is worth to mention that this decision recognized an autonomous data protection right before its formal constitutional enshrinement in 2022's Amendment 115. Hence the STF articulated a new fundamental right absent from the constitutional text, establishing jurisprudential foundations for subsequent constitutional reform.

II. Articulating constitutional data protection duties upon governmental entities

In 2021, the Court ruled a Federal Decree (Decree 10,046 of 2019) enabling unrestrained personal data sharing across Public Administration entities as unconstitutional. This Decree had instituted a "common public database," supposedly to streamline public services. It effectively created a governmental "data lake" consolidating the various personal information citizens furnish to federal agencies, including biographical, electoral, and social security data.

The STF held that indiscriminately pooling sensitive personal information failed fundamental rights protections. By enabling unrestricted state data analysis without purpose limitations or safeguards for citizens' informational autonomy, the Decree violated core data protection principles. Thereby the Court again affirmed the constitutional right of data protection in invalidating governmental data mining absent considerations of digital rights.

This case reached the STF after the government shared 76 million Brazilians' data between intelligence agencies and the National Traffic Department. The stated purpose was providing access to citizens' driver's license information for intelligence analysis. The Brazilian Bar Association consequently challenged the Federal Decree enabling this mass data pooling as unconstitutional.

The ruling filled a critical legislative gap, as Brazil's 2018 Data Protection Law only partially binds the public sector. The STF held that absent comprehensive statutory protections, data sharing and collection still requires an explicit legal basis and cannot be indiscriminate. Moreover, the Court outlined principles limiting governmental data use, including specified purposes, transparency, accountability, and proportionality. Though Brazil lacks robust public sector data protection legislation, the STF affirmed Constitutional due process principles forbid unfettered state data mining. In imposing rights-based restrictions, the Court advanced Constitutional safeguards adapted from digital constitutionalism to check governmental data collection and analysis.

The Federal Decree violated these Constitutional principles. Absent a specific legislative mandate, the broad data sharing authorized infringed on Constitutional data protection rights per Article 5, Section LXXIX. Moreover, enabling free policy-oriented data use without processing safeguards or specifications disregarded rights limitations. The lack of traceability

mechanisms for citizen monitoring further failed Constitutional due process.

Justice Gilmar Mendes' report vote concluded that the Decree failed to adequately safeguard the fundamental right to data protection, as it still relied on an antiquated logic of secrecy. The Federal Government's Decree did not establish procedural safeguards for citizen control. Instead, it simply limited the sharing of data that had been classified by other legal provisions. The Court determined that the distinction between "public" and "private" nature of the data was insignificant when compared to the fundamental right, which primarily safeguards the data owner's authority to control the data.

D. Final remarks

Digital constitutionalism has rapidly emerged as an influential framework for conceptualizing rights and regulation adapted to the digital age. While early theorization focused extensively on private governance systems and self-regulatory initiatives, the past decade's proliferation of constitutional litigation has revealed the enduring primacy of judicial review in this constitutional paradigm shift. Thereby through landmark decisions, courts are elucidating how constitutional rights, duties and proportionality standards apply within online architectures just as in analogue spaces.

As explored in this analysis, recent Brazilian Supreme Court judgments demonstrate how digital constitutionalism is catalyzing a rights-centric jurisprudence constraining both state and corporate power in cyberspace. The Court has built upon the Marco Civil da Internet's crystallization of proto-constitutional principles to affirm an autonomous right to data protection with duties applicable to public and private entities. In articulating this evolved understanding, the STF has repeatedly invoked legislative embodiments of Digital constitutionalism values to legitimize its constitutional innovation as flowing directly from Brazil's uniquely rights-focused internet governance model.

Crucially, these decisions have established proportionality tests and contextual standards that qualify the application of digital rights protections. Through purpose specifications, data minimization requirements, and transparency mechanisms, the Court has set baselines to balance privacy, autonomy, and dignity with countervailing public interests in security, innovation, and effective administration. Thereby the STF has advanced a

contextualized articulation of rights avoiding absolutist conceptions that would fail to adapt enduring constitutional guarantees to the distinct logics of online spaces.

As the first jurisdiction to constitutionalize internet principles through formal legislation, Brazil's digital constitutionalism jurisprudence provides lessons for similarly situated countries facing governance deficits in increasingly digitized societies. As the landmark decisions surveyed in this analysis attest, adapting fundamental rights to changing technological realities is no longer an aspirational academic vision but an emergent judicial practice with enormous influence potential. This opens new horizons for digital constitutionalism under a democratic judicial review approach which warrants further examination in the scholarship.

The Democratic Rule of Law in Brazil and the challenges of implementing 5G in a scenario of digital divide and hyperconnection

Gabrielle Bezerra Sales Sarlet and Ingo Wolfgang Sarlet

Abstract: The implementation of the 5G technology in a scenario of digital divide and hyper connection raises – in spite of having important positive aspects related to economic, social and human developments - several challenges to the democratic rule of law all over the world. In this context, the paper aims to approach the subject in light of the Brazilian reality and legal order, but taking into account the global environment in which regards the digital transformations and the so-called techno-authoritarianism.

A. Introductory notes

Information has been the engine of history, directly linked to the architectures of acquiring, maintaining, and expanding power, especially in contexts of increasing and perpetuating social inequalities[1]. Etymologically, it is worth noting that information evokes the idea of an action, both in the positive and negative meaning of the term, in a process of framing or, in other words, formatting, always aimed at a certain goal to be achieved[2].

Furthermore, for practical purposes, regarding to protecting personal data legislation, for example, the differentiation is no longer relevant. Information (and pieces of information) should not be confused with data, as information operates in communication processes and information architectures, which can be more or less sophisticated, depending on the case, thus presupposing trust and sharing.

1 https://g1.globo.com/economia/censo/noticia/2023/06/28/censo-2022-brasil-tem-203-milhoes-de-habitantes-47-milhoes-a-menos-que-estimativa-do-ibge.ghtml Acesso em: 21.08.2023.

2 https://itsrio.org/pt/artigos/devemos-banir-a-inteligencia-artificial-nas-eleicoes/?utm_campaign=thinktech_52&utm_medium=email&utm_source=RD+Station Acesso em: 24.08.2023.

Nowadays, the boundaries of truth and certainties seem to have eroded, as the pace of new formats and models of advertising, digitalization, and the algorithmization of everyday life have accelerated, especially concerning the apparent dissolution of social and political pacts that, in some way, sought to guarantee a greater degree of fidelity and the maintenance of knowledge validation filters[3].

In view of this, it is important to point out that this study refers mainly to algorithmization as a key term for a better understanding of the current state permeated by the use of algorithms and multiple applications of artificial intelligence[4] (henceforth AI). This terminology, as it is already well known, expresses a radical change in living conditions triggered by its widespread use, in a subtle, pervasive and disruptive way, multiplying into multiple technological solutions applicable to precariousness and problems that are sometimes considered chronic, e.g. hunger, environmental devastation, migration control and the energy crisis. Its use is also notable in health, education, and allocation of sparse public resources, as well as in the form of specific modules for new surveillance systems[5] launched by private companies and government agencies[6].

In this context - the so-called digital transformation - it is important to keep in mind that this is not just another set of technological innovations that have been emerging, but a bundle of profound changes of the most diverse kind, including in the social fabric, also causing cultural ruptures[7].

One of the main phenomena experienced in the present, it can be affirmed, is the trivialization and a kind of standardization of an algorithmic way of life, which is engulfed by socio-technical AI devices aimed at main-

3 BOURDIEU, Pierre. *Sobre o Estado*: Cursos no Collége de France (1989-92). São Paulo: Companhia das Letras, 2012, [s.p.].

4 SCHMIDT, Eric; HUTTENLOCHER, Daniel; KISSINGER, HENRY A. *A era da IA e o nosso futuro como humanos*. Vanessa Schreiner (Trad). Rio de Janeiro: Alta books, 2023, p. 44-45.

5 ZUBOFF, Shoshana. *A era do capitalismo de vigilância*: a luta por um futuro humano na nova fronteira de poder. [livro eletrônico – Kindle]. Trad. George Schlesinger. Rio de Janeiro: Editora Intrínseca. 2021.

6 DI FABIO, Udo. *Grundrechtsgeltung in digitalen Systemen*: Selbstbestimmung und Wettbewerb im Netz. München: C.H. Beck, 2016, p. 44-45. See also BIONI, Bruno; MARTINS, Pedro. *Devido processo informacional*: um salto teórico-dogmático necessário? Available at: https://brunobioni.com.br/wp-content/uploads/2020/08/Ensaio-Devido-ProcessoInformacional 1.pdf. Accessed on 02 Mar 2022.

7 HOFFMANN-RIEM, Wolfgang. *Teoria geral do direito digital*: desafios para o direito. 2. ed. Rio de janeiro: Forense, 2022, p. 98.

taining a single hegemonic technological model, with information production as its central engine, with a view to strengthening control structures and, in particular, the infinite increase in Big Techs astronomical profits[8].

As a result of that, in the digital era, despite the numerous distinctions between the global North and South's impact, human existence is being drawn into ecosystems marked by a certain comfort and the acceleration of life itself in the face of the massive production of information; on the other hand, social and political polarization is intensifying due to an increase in violence, hypersurveilance, economic disparities, the precarization of attention, the vitrification of personality and the compression of individual autonomy in a context characterized by rising levels of techno-authoritarianism[9].

On the other hand, there is a preponderance of other/new "Agoras", replacing the traditional dimensions of the public and private spheres, substantiated, and absorbed in the composition of social networks under the leadership of Big Techs in the area of information and communication technologies[10]. This evolution, however, is taking place in an environment marked by information asymmetry and digital exclusion/division at various levels, which, for a better understanding, requires an approach based on certain elements, namely complexity, speed, volume, scalability and algorithmization.

For a more precise understanding of this picture characterized by complexity, it is possible to mention the increasing (but, at the same time, increasingly subtle) use of techniques to silence individuals and certain sections of the world's population, as access to new technologies of high quality is denied while a series of parallel ecosystems, substantially marked by excessive information production, are produced and maintained, which, in short, leads to deafening noises and affects the process of subjectivation and, consequently, the exercise of citizenship, especially in the digital dimension.

In this regard, beyond the traditional methods widely used in the market, control based on algorithms is increasingly being used as a new form of

8 https://forbes.com.br/forbes-tech/2023/02/o-que-difere-as-big-techs-de-outras-empresas-de-tecnologia/ Accessed on: 28.08.2023.

9 NIDA-RÜMELIN, Julian. *Digitaler Humanismus:* Eine Ethik für das Zeitalter der künstlichen Intelligenz. München: Piper, 2018; BÄCHLE, Thomas Christian. *Digitales Wissen, Daten und Überwachung*: zur Einführung. Hambug: Junius, 2016, p. 158.

10 https://www1.folha.uol.com.br/ilustrissima/2023/02/oito-medidas-para-regular-big-techs-garantindo-liberdade-de-expressao.shtml Accessed on 21.08.2023.

governance, e.g., the collection and processing of neural data[11]. It is no coincidence that there is talk of Algorithmic Regulation and/or Algorithmic Governance. The same applies to the public sphere, i.e., digital governance supported by Big Data[12], AI and algorithms, which, in the Brazilian case, can be observed primarily after the Law 14.129/21[13], which established the

11 Cf. Caso emotiv e a Corte Constitucional do Chile em: https://drive.google.com/file/d/1wX2fUrBDTl3B1W_IK_DUOCC7neQS6Hhu/view Accessed on 09.09.2023; https://idealex.press/primera-sentencia-sobre-informacion-cerebral-genera-debate/ Accessed on 10.09.2023. In Brazil, there is a PEC (Proposed Amendment to the Constitution) that seeks to amend Article 5 to include the protection of mental integrity and algorithmic transparency among fundamental rights.

12 Five characteristics are often used to identify Big Data: the five "Vs":1 - The possibilities of accessing huge amounts of digital data ("High Volume"); 2 - Different types and quality of data, as well as different ways of collecting, storing and accessing it ("High Variety"); 3 - The high speed of its processing ("High Velocity"); 4 - The use of artificial intelligence in particular makes possible new and highly efficient ways of processing data, as well as checking its consistency and guaranteeing its quality ("Veracity"): 5 - In addition, Big Data is the object and basis of new business models and possibilities for various value-added activities ("Value").

13 Law no. 14.129, of 29 March 2021. Provides for principles, rules and instruments for Digital Government and for increasing public efficiency and amends Law No. 7.116, of 29 August 1983, Law No. 12.527, of 18 November 2011 (Access to Information Law), Law No. 12.682, of 9 July 2012, and Law No. 13.460, of 26 June 2017. Available at: www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14129.htm. Accessed on 22 May 2022. Some provisions of Law 14.129/2021, as well as Decree 10.900, of 17 December 2021, should be considered, albeit briefly. Provides for the Citizen Identification Service and the governance of the identification of natural persons within the scope of the direct, autarchic and foundational federal public administration, and amends Decree No. 8.936, of 19 December 2016, Decree No. 10.543, of 13 November 2020, and Decree No. 9.278, of 5 February 2018. Available at: www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/decreto/d10900.htm. Law no. 14.129, of 29 March 2021. Provides for principles, rules and instruments for Digital Government and for increasing public efficiency and amends Law No. 7.116, of 29 August 1983, Law No. 12.527, of 18 November 2011 (Access to Information Law), Law No. 12.682, of 9 July 2012, and Law No. 13.460, of 26 June 2017. Available at: www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14129.htm. Accessed on 22 May 2022. Some provisions of Law 14.129/2021, as well as Decree 10.900, of 17 December 2021, should be considered, albeit briefly. Provides for the Citizen Identification Service and the governance of the identification of natural persons within the scope of the direct, autarchic and foundational federal public administration, and amends Decree No. 8.936, of 19 December 2016, Decree No. 10.543, of 13 November 2020, and Decree No. 9.278, of 5 February 2018. Available at: www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/decreto/d10900.htm. Accessed on 27 Aug 2023.

pillars of a digital government, foreseeing the use of AI as a central instrument for governance[14].

Taking the Brazilian case into account, it is necessary to warn of Brazil's strategic position on the world stage of so-called data colonialism[15] and, therefore, a manifestation of techno-authoritarianism. This is due to several factors, especially the hyperconnectivity of the Brazilian population, the leniency of public authorities in the face of abuses perpetrated by Big Techs, legislative gaps in the area of technology, as well as the ample potential offered by Brazil in terms of profits and opportunities for exploitation and growth that are emerging with the implementation of 5G, which, in turn, leads to the necessary confrontation of the digital divide issue in the domestic environment[16].

Thus, based on the premise that algorithmic governance[17] implies transparency and public scrutiny, this text aims to identify and explore - with a focus on the case and the Brazilian legal system, with regard to the protection of Human and Fundamental Rights (especially the protection of personal data) in face of the challenges of implementing the fifth generation of the internet (5G) in a scenario of hyperconnection and digital divide.

14 HOFFMANN-RIEM, Wolfgang. Inteligência artificial como oportunidade para a regulação jurídica. *Direito Público*, Porto Alegre; Brasília, n. 90, nov./dez. 2019; CELLA, José Renato Gaziero; COPETTI, Rafael. Compartilhamento de dados pessoais e a administração pública brasileira. *Revista de Direito, Governança e Novas tecnologias*. Maranhão, v.3, p. 39-58, jul/dez, 2017; DONEDA, Danilo. Panorama Histórico da Proteção de Dados Pessoais. In: MENDES, Laura; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUEZ JR., Otavio Luiz (Orgs.). Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021, p. 39.

15 BRAH, Avtar. *Diferença, diversidade, diferenciação*. Caderno Pagu (26), Campinas-SP, Núcleo de Estudos de Gênero-Pagu/Unicamp, 2006, pp. 329-376; BOSKER, B. (2013). *Google's Online Ad Results Guilty Of Racial Profiling, According To New Study***.** The Huffington Post. Recuperado de https://www.huffpostbrasil.com/2013/02/05/online-racialprofiling_n_2622556.html?ec_carp=4291654031226775441. Accessed on: 28.07.2023; MENDES, L.S., MATTIUZZO, M. (2019) *Discriminação algorítmica: conceito, fundamento legal e tipologia*. Revista de Direito Público, v.16 (90), pp. 39-64.

16 Brazil tends to invest more and more in technology applied to health. Cf.: https://br.cointelegraph.com/news/government-releases-brl-616-million-for-research-and-innovation-projects-that-include-blockchain-ai-and-web3-in-health Accessed on: 10.09.2023.

17 https://drive.google.com/file/d/1WFJppEqmmR9OuSaBH_qlOlzOQeXHGK_-/view Accessed on: 20.08.2023.

The aim is to contribute to a reflection on the current technocratic hegemony and its impact on the democratic rule of law in Brazil[18].

B. The Brazilian context - implementing 5G in a scenario of digital division and hyperconnection

Among the many unusual situations that have emerged with the turn produced by the recent pandemic, due to the transformations driven by information and communication technologies (ICT), the digital divide that plagues the world, particularly the countries that make up the global South, has come to the forefront of public debate, revealing the inequality and social injustice that prevail, especially on the global periphery.

Despite a lack of precise definition about its origin, the concept of the digital divide has been used primarily to identify that participating adequately in the information society serves to expand markets, maintain psychophysical well-being, and the exchange of knowledge, preventing the concentration of wealth and the deepening of inequalities among individuals, regions, and countries.

On the other hand, appropriate access to the means and digital information resources that constitute knowledge and wealth production theoretically enables the strengthening of democracies through the development and empowerment of individuals and groups, lifting them from a subalternity and vulnerability condition, as the proper appropriation of technology and information flows has become a neuralgic dimension in world geopolitics[19].

---

18 *Dados do Censo*: BRASIL. Censo. IBGE: Brasília, 2022-3. Available at: https://cidades.ibge.gov.br/. Accessed on: 22 ago.2023. Dados do Anuário Brasileiro de Segurança Pública 2023: FORUM BRASILEIRO DE SEGURANÇA PÚBLICA. Anuário Brasileiro de Segurança Pública 2023. Disponível em: https://forumseguranca.org.br/wp-content/uploads/2023/07/anuario-2023.pdf. Accessed on: 22 ago. 2023; NIC.BR; CGI.BR; CETIC.BR. Annual Report Cetic.br. 2022. Available at: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://cetic.br/media/docs/publicacoes/9/20230530114022/Annual_Report_Cetic2022.pdf. Accessed on: 25 jul. 2023; NIC. BR.CGI.BR; CETIC.BR. Available at: *Pesquisa TIC Kids Online BRASIL 2021*. Resumo Executivo. Disponível em: https://cetic.br/media/docs/publicacoes/2/20221121120628/resumo_executivo_tic_kids_online_2021.pdf. Accessed on: 29.03. 2023.

19 https://exame.com/inteligencia-artificial/ia-ameaca-ampliar-divisao-digital-na-america-latina/ Accessed on: 21.08.2023; https://www.rollingstone.com/politics/politics-features/china-facebook-instagram-propaganda-campaign-1234813762/ Acesso em:01.09.2023.

The United Nations (UN) estimates that more than 2.7 million people, especially in developing and least developed countries, are still on the margins of a safe, responsive, resilient, and human-centered digital future, to the detriment of achieving the 17 Sustainable Development Goals (SDGs) [20]. Illustratively, the implications for digital marginalization are diverse in nature, including jeopardizing global initiatives to combat hunger, new pandemics, and environmental and climate issues.

In addition, digital exclusion leads to isolation, loss of growth and development opportunities, both at a personal and collective level, hindering access to science, the job market, healthcare services and knowledge in general, accentuating power asymmetries, discrimination and violence against historically vulnerable individuals and groups by exposing them to disinformation campaigns and hate speech.

It is worth noting that there are three ways to distinguish and categorize digital exclusion: exclusion from access, exclusion from use (having access to the Internet and digital technologies, but lacking the skills to use them properly) and exclusion related to the quality of use, which, in short, refers to making the most of the connection conditions and the internet itself, especially in terms of access to quality information[21]. It should also be noted that digital exclusion, in all three mentioned levels, affects some groups more than others, with black and brown women and girls[22] in poor countries being the most affected, reinforcing the erosion of their autonomy, discrimination and gender-based violence[23].

Especially regarding SDG 9, the UN anticipates that a number of strategies must be prioritized to tackle the digital divide, including digital literacy, holding major technology platforms accountable for designing safer and more inclusive platforms, and forming a global alliance[24] to address the issue.

Considering the domestic context, Brazil has a population of 203,062,512 people, according to the 2022 Demographic Census, with 5% of Brazilian

20 https://www.un.org/en/desa/27-billion-people-still-left-offline Accessed on: 21.08.2023.

21 https://www.iberdrola.com/compromisso-social/o-que-e-exclusao-digital Accessed on: 23.08.2023.

22 So as not to give rise to any misunderstandings, it should be noted that the terminology brown and black people is the one legally in force in Brazil, both referring to the majority Afro-descendant population group in the country.

23 https://news.un.org/pt/story/2023/03/1811282 Accessed on: 19.08.2023.

24 https://a4ai.org/ Accessed on: 31.08.2023.

cities concentrating 56% of the country's population. In total, 115.6 million people live in 319 cities[25]. With the urbanization rapidly expanding worldwide, Brazil has followed the path of population densification in urban centers, as evidenced by the current state of the southeastern states, notably São Paulo and Rio de Janeiro.

The internet, in both its oracular and mirror-like expression, reveals the gravity of inequality and social marginalization in the Brazilian case, along with a system of privileges that confines the population to a kind of caste system[26], which there is no real chance of social mobility.

In order to illustrate what is at stake, particularly with regard to digital division/exclusion and techno-authoritarianism, the focus is placed on the example of the implementation of the fifth generation of the internet, the so-called 5G, which has currently been the main target of public attention, particularly at national level. 5G technology - also in Brazil - promises to massify and diversify the Internet of Things (IoT) in sectors such as public security, telemedicine, distance education, smart cities, industrial and agricultural automation, all with the aim to increase the accuracy and efficiency of the various sectors of the economy, benefiting society[27]. This is because 5G is characterized by low latency, real-time connection capacity and, in these terms, high-speed data sharing, guaranteeing unprecedented quality in communication flows and information architectures[28].

---

25 https://g1.globo.com/economia/censo/noticia/2023/06/28/censo-2022-brasil-tem-203-milhoes-de-habitantes-47-milhoes-a-menos-que-estimativa-do-ibge.ghtml Acesso em: 21.08.2023.

26 BARRETO, Luis Fernando Britto Pereira de Mello. *Uma análise da divisão digital no Brasil através da aplicação da aprendizagem de redes bayesianas*. 2012. Dissertação (Mestrado em Administração) - Faculdade de Economia, Administração e Contabilidade, Universidade de São Paulo, São Paulo, 2012. doi:10.11606/D.12.2012.tde-18022013-175034. Accessed on: 2023-09-02.

27 https://www.gov.br/anatel/pt-br/assuntos/5G/tecnologia-5g Accessed on: 26.08.2023.

28 https://www.gov.br/anatel/pt-br/regulado/radiofrequencia/plano-de-uso-do-espectro-de-radiofrequencias Accessed on: 26.08.2023; "South Korea and Puerto Rico lead the world in 5G availability, with scores of 42.9 per cent and 48.4 per cent respectively. Impressively, given the geographical size of the market, the US is in fourth place, with 31.1 per cent 5G availability - almost a third. In the other developed markets, the scores vary widely. In Europe, Finland and Bulgaria have the joint highest 5G availability score (24.2 per cent - 24.7 per cent), but the five largest markets are lower, with France scoring 20.6 per cent, Germany 13.3 per cent, Italy 17.9 per cent, Spain 15.2 per cent and the UK a relatively low 10.1 per cent. Belgium has the lowest 5G availability in Europe, with a connected time of 4 per cent. In Asia, South Korea is chased by Singapore and Taiwan (both with 30 per cent). Singapore's

5G is the fifth generation of the mobile internet network, consisting of a structure of antennas, receivers and radio frequency bands that enables more faster, secure, and stable connections for mobile phones, tablets, and other smart devices. It demands the use of its own antennas and receivers, requiring a larger infrastructure made up of a network of antennas close together[29].

Activities such as sending and playing multimedia files, using applications, taking part in video calls, playing online games, broadcasting live streams, and performing various downloads and uploads will be faster and of twenty times better quality on average[30]. This means that, in general, people will benefit from being more and better connected[31].

In fact, 5G aims to solve the problem of signal loss by overcoming network overloads. Among the many sectors that will benefit from 5G, especially due to its speed and stability, industry and telehealth stand out[32], especially in terms of autonomous cars and remote robotic surgeries[33].

In other words, it can be said that, since 5G was first implemented in South Korea in 2019, there has been a general increase in the economy's performance and potential for income generation and benefits for the population, including a more favorable geopolitical position for countries in terms of digital sovereignty. Nevertheless, it is worth stating that the forecast for the implementation of 5G in Brazil began in Brasília in 2022

close neighbour, Malaysia, scored 20.5%, despite the relatively recent launch of 5G." In: https://www.opensignal.com/2023/06/30/benchmarking-the-global-5g-experience-june-2023 Accessed on: 26.08.2023; Para entender o panorama na América latina: https://www.gsma.com/latinamerica/wp-content/uploads/2023/06/290623-5G-in-Latam-ENG.pdf Accessed on :26.08.2023.

29 https://g1.globo.com/tecnologia/noticia/2023/07/06/5g-no-brasil-mapa-mostra-todas-as-antenas-nas-315-cidades-com-a-tecnologia-confira.ghtml Acesso em: 23.08.2023.

30 https://www.portaldaindustria.com.br/industria-de-a-z/5g-no-brasil/ Accessed on: 23.08.2023.

31 https://news.un.org/pt/story/2020/09/1726652 Accessed on: 30.08.2023.

32 STRATI. Conheça um panorama sobre o mercado da saúde para 2023! *Site Strati*, [*S.l.*], 3 nov. 2022. Disponível em: https://strati.in/mercado-da-saude/. Accessed on: 01 jun. 2023; PASSOS, Juliana. A telessaúde deve estar a serviço do SUS. Entrevista com Angélica Baptista Silva. *Site EPSJV/Fiocruz*, 05 de abril de 2023. Available at: https://www.epsjv.fiocruz.br/noticias/entrevista/a-telessaude-deve-estar-a-servico-do-sus#:~:text=Porque%20se%20voc%C3%AA%20tem%20que,um%20melhor%20acompanhamento%20do%20paciente. Accessed on: 04.05.2023.

33 https://digital.futurecom.com.br/transformacao-digital/o-5g-ja-esta-impactando-saude-no-brasil Accessed on: 13.09.2023.

and is expected to be finalized in 2029, when developed countries are likely to be installing 6G[34].

In the case of health, for example, it is important to highlight that, due to the speed of data traffic and low latency, significant investments in technology are being made to the extent of the value of biometric and psychological data in the world ranking. Among the application possibilities of 5G, one can list the potential use of techniques such as digital twins[35] and new information management formats focused on resource allocation and data security. Therefore, in this context, the medical record will increasingly become an information hub[36].

In short, digital health theoretically connects people and populations through ICTs to manage health and well-being, complemented by providers teams working in flexible, integrated, interoperable and digitally enabled care environments that must strategically manage digital tools, technologies and services to transform, integrate and democratize the provision of care and therapies in a safe, robust and reliable manner. Thus, in line with the implementation of 5G health, it has been recently enacted the Law 14.510/2022 to regulate the practice of telehealth[37], which, through a multidisciplinary scope, assigns rights and duties, and is a driver for some ongoing reflections on central points such as responsibility, cybersecurity, and equity.

However, in the Brazilian environment, as mentioned, the discrepancies regarding the 5G experience in the state capitals are still intense. Many Brazilian smartphone users have limited access to 5G networks or 5G devices, facing much slower overall mobile download speeds. Incidentally, 20.7% of Brazilian users have overall average download speeds below 10 Mbps, which makes the internet browsing on their devices much more dif-

34 https://www.uol.com.br/tilt/noticias/redacao/2023/03/07/o-que-e-6g-quando-chega-qual-velocidade-nova-rede-no-brasil-melhor-que-5g.htm Accessed on: 24.08.2023.

35 M. Alazab *et al*., "Digital Twins for Healthcare 4.0 - Recent Advances, Architecture, and Open Challenges," in *IEEE Consumer Electronics Magazine*, 2022; Thelen, A., Zhang, X., Fink, O. *et al.* Uma revisão abrangente do gêmeo digital - parte 2: funções de quantificação e otimização de incertezas, um gêmeo digital de bateria e perspectivas. *Struct Multidisc Optim* **66** , 1 (2023). https://doi.org/10.1007/s00158-022-03410-x Accessed on: 25.05.2023.

36 https://www.saudebusiness.com/colunas/cara-ou-coroa-os-dois-lados-da-inteligencia-artificial-na-saude Accessed on: 13.09.2023.

37 http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/lei/L14510.htm#:~:text=LEI%20N%C2%BA%2014.510%2C%20DE%2027,15%20de%20abril%20de%202020. Accessed on: 12.09.2023.

ficult and challenging. Despite the slow and gradual implementation of 5G, only 0.6% of smartphone users in Brazil enjoy overall average download speeds of more than 100 Mbps[38].

Regarding smartphone users, the main access mean of the mobile internet in Brazil, it is important to look at the issue of speed. In this regard, it is noted that "*20% of the population (one in five users) receives, on average, less than 10 Mb/s download speed on their mobile connection. Equally complicated is the fact that the states with the highest percentage of users with internet speeds below 10 Mb/s are Amazonas (26 per cent), Minas Gerais (27.2 per cent) and Roraima (29 per cent)*". Finally, the report provided by Opensignal also clarifies that Acre, Mato Grosso, Mato Grosso do Sul, Rondônia, Roraima and Piauí have more than 15% of the population without a signal for 10% or more of their mobile internet usage time[39].

It is also important to remember that the internet reaches 60 million homes in the country, corresponding to 80% of the total. Of these homes, 82% have a stable connection in urban areas and 68% in rural areas. In class A, 100% of homes are connected. In the other classes, the situation is completely different: class B (97%); class C (87%); D and E (60%). However, in Brazil, 36 million people do not connect to the internet, usually because of the high prices of the devices and lack of interest. Approximately 29 million live in urban areas and have studied up to primary school. Of these, 21 million are black and brown; 19 million are in classes D and E; and 18 million are aged 60 or over[40].

In the midst of the digital vacuum in some regions, situation that has a decisive impact on some very specific population groups, especially public-school students in isolated areas in the interior of Brazil, the Federal Senate approved a constitutional amendment proposal, PEC 47/2021, which aims to introduce a right to digital inclusion[41] in the fundamental rights catalogue of the Article 5 of the Federal Constitution of 1988 (henceforth

38 https://www.opensignal.com/2023/05/16/users-in-brazils-state-capitals-enjoy-5g-download-speed-exceeding-250mbps Accessed on: 12.08.2023.

39 https://www.opensignal.com/2023/08/24/brazilian-smartphone-users-observe-major-disparities-in-mobile-network-experience Accessed on: 01.09.2023.

40 CGI.br/NIC.br, Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br), Pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros - TIC Domicílios 2022. IN: https://cetic.br/media/docs/publicacoes/2/20230825143720/tic_domicilios_2022_livro_eletronico.pdf Accessed on:24.08.2023.

41 https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2326575;

CF/88). This proposal, however, is still awaiting deliberation and approval in the Chamber of Deputies of the National Congress.

In this regard, the federal executive branch launched the "Brasil Conectado" (Connected Brazil) program, which, in short, aimed to bring the internet to the most deprived regions in terms of digital inclusion, in order to promote the expansion of strategic areas such as health and education. However, for these objectives to be realized, it is essential to guarantee, on an equal basis, appropriate infrastructure, access to compatible devices and high-quality broadband internet, as well as data security through effective policies on cybersecurity, sovereignty, and digital education.

However, according to the Education Watch observatory, what has happened so far has been the thoughtless authorization of Starlink's entry[42], especially into the Brazilian Amazon region, favoring illegal mining and deforestation, as well as the increasing dominance of platform capitalism in Brazilian education[43], with Google taking the dominant position in student and teacher data storage in this opaque ecosystem, where apps are even installed without users' consent[44].

On the other hand, somewhat contradictory, Brazil can undoubtedly be described as a hyperconnected country, since 142 million of the 149 million Internet users in the country connect every day, or almost every day - with a prevalence in social classes A and B and to a lesser extent in C, D and E. Thus, Brazilians spent nine hours and thirty-two minutes per day, on average, surfing the Internet in 2022. It is important to note that the majority of Brazilian Internet users (62%) access the web exclusively via their mobile phones, which is the case for more than 92 million people[45]. In this regard, Internet use exclusively via mobile phone predominates among

---

https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2183047&filename=PEC%2047/2021%20(Fase%201%20-%20CD) Accessed on:20.08.2023.

42 https://veja.abril.com.br/economia/acordo-fechado-a-chegada-da-starlink-de-elon-musk-ao-brasil?utm_source=google&utm_medium=cpc&utm_campaign=eda_veja_audiencia_institucional&gad=1&gclid=CjwKCAjw3dCnBhBCEiwAVvLcu1JyAqjDcnyonTXxx3Z2VCCGXWsn3kvVIGIZJBmMbIqEoHxykuzcKhoC59UQAvD_BwE Accessed on: 01.07.2023.

43 https://nucleo.jor.br/reportagem/2023-08-24-como-as-big-techs-cravaram-os-dentes-na-educacao-brasileira/ Accessed on: 27.08.2023; https://gitlab.com/ccsl-ufpa/get-mx-universities/?ref=nucleo.jor.br Accessed on: 01.09.2023.

44 https://educacaovigiada.org.br/pt/mapeamento/brasil/?ref=nucleo.jor.br Acesso em: 01.09.2023.

45 https://www.opensignal.com/2023/08/24/brazilian-smartphone-users-observe-major-disparities-in-mobile-network-experience Accessed on: 01.09.2023.

women (64%), among blacks (63%) and browns (67%), and among those belonging to the D and E classes (84%)[46].

As a result, Brazil surpasses developed countries such as UK, where the average time spent on the internet is 5 hours and 47 minutes. It is noteworthy that, as a result, Brazilian population remains more connected than the global average. It is important to remember that mobile phones continue to be the most used device and messaging services, including WhatsApp, are the favorites. In the case of WhatsApp, Brazilians spend a monthly average of 28 hours connected[47].

As mentioned earlier, it cannot be ignored that data packages, as well as the quality and speed of the internet available to most of the population, along with disinformation campaigns and the exponential volume of leaks and scams on and through the network, have been serious impediments to Brazil's transition from a digital hinterland to a leading group of countries in global technology geopolitics.

C. Challenges to the Democratic Rule of Law - A look at the global environment and the Brazilian scenario regarding digital transformations and techno-authoritarianism

In the broader context of what has been termed digital constitutionalism[48], the phenomenon of techno-authoritarianism[49] has been particularly challenging, as it poses a growing and increasingly serious threat to human and fundamental rights and also, consequently, to the democratic rule of law and its institutions[50].

---

46 https://cetic.br/media/docs/publicacoes/2/20230825143348/resumo_executivo_tic_domicilios_2022.pdf Accessed on: 02.09.2023.

47 https://cetic.br/media/docs/publicacoes/2/20230825143348/resumo_executivo_tic_domicilios_2022.pdf Accessed on: 02.09.2023.

48 https://verfassungsblog.de/a-constitution-without-constitutionalism/ Accessed on: 14.07.2023.

49 ZANATTA, Rafael Augusto Ferreira. *A proteção coletiva dos dados pessoais no Brasil*: a defesa de direitos entre autoritarismo e democracia. p. 94-95-96.

50 *"We call the form of domination in which information and its processing by algorithms and artificial intelligence decisively determine social, economic and political processes an information regime"*. In: HAN, Byung-chul. Infocracia: *Digitalização e a crise da democracia*. Editora Vozes, 2022. p. 6; https://www.migalhas.com.br/depeso/388195/racismo-algoritmico-nas-relacoes-de-consumo Accessed on: 23.07.2023.

Techno-authoritarianism[51], a term that has been increasingly used in recent years, generally consists of the use of increasingly sophisticated technological resources, especially in the context of digitalization strategies and the exponential use of information and communication technologies (ICTs), in order to increase both in quantitative and qualitative terms the control exercised by the state and, in another more current twist, by a hegemonic group of technology companies, primarily through the mystical appanage[52] of the Bigtechs[53].

In view of this, it should be pointed out that society, as a system of communication and meaning, is necessarily guided by a set of principles and rules that determine people's social belonging (both individually and collectively), but also organize the behavior, feelings and thoughts of its members. In this context, it is possible to say that what is happening in this fold of human history is something unprecedented, comparable only to the power of the East India Company (EIC)[54] in the 17th century, as a handful of companies establish a new, but subtle, form of exercising authoritarian power, which, especially since the last decade of the 20th century, has subjugated - or at least constrained, to a greater or lesser extent - all other institutions (public and private) that exercise power, whether legitimate or not.

These are large technology companies that develop innovative and disruptive services, growing rapidly and superlatively and hegemonically and predatorily dominating the market and, in doing so, the democratic regime. These corporations have become part of the daily lives of billions of people around the world, particularly after the pandemic, offering technological products and solutions, many of them supposedly free of charge, while also radiating virtually unprecedented domination based on the processing of personal and non-personal data. This has had an impact on individuals

51 https://www1.folha.uol.com.br/ilustrissima/2023/02/oito-medidas-para-regular-big-techs-garantindo-liberdade-de-expressao.shtml Accessed on: 09.08.2023.

52 RODRIGUES, Jose Carlos. Ensaios em antropologia do poder. Rio de janeiro: Terra Nova, 1992. P. 22-23.

53 Auxier, B.; Anderson, M.; Perrin, A.; Turner, E. Children's Engagement with Digital Devices, Screen Time. Pew Research Cente. 2020. Disponível em: https://www.pewresearch.org/internet/2020/07/28/childrens-engagement-with-digital-devices-screentime/. Acesso em 20 mar. 2023; https://nucleo.jor.br/reportagem/2023-08-24-como-as-big-techs-cravaram-os-dentes-na-educacao-brasileira/ Accessed on:29.08.2023.

54 https://neofeed.com.br/blog/home/o-poder-das-big-tech-mudanca-comportamental-ou-nova-classe-de-ativos/ Accessed on: 29.08.2023.

and social groups by changing their understanding and experience of the privacy-identity binomial[55], altering their fears, dreams, conceptions of the world and perception of time and space[56], as well as the limits and contours of the public and private spheres.

As a result, the capacity of individuals and social groups to exercise autonomy[57] and, consequently, to resist that domination has been increasingly emptied. In this context, human and fundamental rights[58] of all dimensions such as freedoms, personality rights, equality rights, but also political, social, economic, cultural and environmental rights, are being jeopardized and even flagrantly violated[59]. Therefore, citizenship, when invested with the digital condition, has become increasingly precarious, as maneuvers like those described in the Cambridge Analytica scandal[60] are becoming increasingly frequent. The spread of such practices revealed some risks that were still hidden from the vast majority of the world's population, despite what had already been established in the Snowden case[61].

It must be emphasized that techno-authoritarianism has become a global phenomenon, meaning that it can occur in a state that is already defined and recognized to be authoritarian or even dictatorial, which only exacerbates the situation, since dictatorship is expanded and intensified through the use of technological resources[62], but it has also had an impact, to a greater or lesser extent, on many states that are or can still be considered

55 GREENFIELD, Susan. *Transformações mentais*: como as tecnologias digitais estão deixando marcas em nosso cérebro. Rafael Surgek (Trad). Rio de Janeiro: Alta Books. 2021. P. 44.

56 MAUÉS, Antonio Moreira. *O desenho constitucional da desigualdade*. São Paulo: Tirant Lo Blanch, 2023, p. 30.

57 MALONE, Hugo; NUNES, Dierle. A implementação de nudges em plataformas digitais de resolução de conflitos. *Revista de Processo*, v. 340, p. 385-405, 2023.

58 https://agenciabrasil.ebc.com.br/geral/noticia/2023-06/justica-determina-bloqueio-de-redes-sociais-de-acusadas-de-racismo?amp Acesso em: 23.08.2023; https://www.conjur.com.br/2023-mai-02/direito-digital-moderacao-conteudo-regulacao-desregulacao-ou-autorregulacao-redes Accessed on: 21.08.2023.

59 MENDES, L.S., MATTIUZZO, M. (2019) Discriminação algorítmica: conceito, fundamento legal e tipologia. *Revista de Direito Público*, v.16 (90), pp. 39-64.

60 https://brasil.elpais.com/brasil/2018/05/02/internacional/1525285885_691249.html. Accessed on: 23.08.2023.

61 https://www.cartacapital.com.br/mundo/ha-10-anos-edward-snowden-revelou-um-mundo-sitiado-pela-espionagem-americana/ Accessed on: 21.08.2023.

62 ZANATTA, Rafael Augusto Ferreira. *A proteção coletiva dos dados pessoais no Brasil*: a defesa de direitos entre autoritarismo e democracia. São Paulo: 2022, p. 44.

democratic, eroding their institutions[63], especially - to name examples that are absolutely current and known to all - through the vertiginous increase in the promotion of disinformation campaigns and hate speech. As Kakutani reminds us, "when it comes to spreading fake news and undermining belief in objectivity, technology has proven to be a highly flammable fuel".

Regarding Brazil, especially given the current state of social and political polarization[64], which is exacerbated by the strong stratification of society, Maués assertion that "increasing inequality tends to weaken democracy itself"[65] becomes relevant. In other words, the democratic regime is not sustainable in markedly unequal societies, which are becoming increasingly inflammable and inflamed, especially in the face of the growing digitalization of everyday life and its implications.

Another aspect to emphasize is that, although it can be said that the use of technology to maintain authoritarian regimes is primarily a phenomenon traditionally driven by the state[66], there is a kind of turning point, that is, a totally unprecedented techno-authoritarianism led by major technology companies, acting in a subtle, pervasive and perverse way[67], which makes the situation even worse, as can be seen from the analysis of the documents of the scandals involving Google, Facebook[68] and YouTube[69].

Moreover, beyond just the actions of big companies – despite their decisive participation –, to better illustrate the picture outlined, we only

63 Cf. BRAZIL. Law no. 14.129, of 29 March 2021. Provides for principles, rules and instruments for Digital Government and for increasing public efficiency and amends Law no. 7.166, of 29 August 1983, Law no. 12.527, of 18 November 2011 (Access to Information Law), Law no. 12.682, of 9 July 2012, and Law no. 13.460, of 26 June 2017. Brasília: Presidency of the Republic. Available at: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14129.htm. Accessed on: 18 August 2023.

64 https://doi.org/10.1590/1807-0191202228162 Accessed on: 25.08.2023.

65 MAUES, Antonio Moreira. *O desenho constitucional da desigualdade*. São Paulo: Tirant lo Blanch, 2023. p. 30-31.

66 https://www.ipea.gov.br/participacao/images/pdfs/participacao/outras_pesquisas/a%20constituio%20cidad%20e%20a%20institucionalizao%20dos%20espaos%20de%20participao%20social.pdf Acesso em: 23.08.2023; https://www2.camara.leg.br/legin/fed/lei/1960-1969/lei-4862-29-novembro-1965-369015-norma-pl.html Accessed on: 23.08.2023.

67 MOROZOV, Evgeny. *Big Tech*: a ascensão dos dados e a morte da política. Claudio Marcondes (Trad). São Paulo:Ubu, 2018, p. 43-44.

68 https://www.cnnbrasil.com.br/economia/facebook-papers-veja-o-que-os-documentos-vazados-revelam-ate-agora/ Accessed on: 23.08.2023.

69 https://mittechreview.com.br/odiou-esse-video-o-algoritmo-do-youtube-pode-empurrar-voce-para-outro-igual/ Acesso em: 23.08.2023.

have to look at the phenomenon of hate speech in individual and collective terms, the exponential increase in disinformation, as well as attacks in general on democratic institutions[70], which occur on a global scale (in the case of Brazil, there are also demonstrations for military intervention) that, for the most part, arise and are expressed within the population, although often directly or indirectly emulated by an information design based on algorithms[71].

For a better understanding, the concept of disinformation (especially what has come to be called fake news) refers to the deliberate dissemination of false, deceptive or inaccurate information, with the aim of misleading and manipulating opinions and elections[72], creating confusion and even stigmatizing and harming population groups, given that minority rights become more fragile on social media[73].

As for hate speech, it can be generally defined as verbal violence expressions that convey and express hatred, contempt or intolerance towards individuals or certain groups, especially historically vulnerable ones[74]. Regarding the linguistic vulnerability inherent in expressions of hatred, Butler explains that words hurt, potentially causing similar effects to physical pain, reason why it can be identified a metaphorical connection between physical and linguistic vulnerability[75]. Furthermore, at this point it is noticeable that there is no clear boundary between the on and offline worlds[76].

Considering all of this, it is important to emphasize that this is not just a matter of design, as social media platforms, due to their impact on

70 https://www.bbc.com/portuguese/articles/cye7egj6y1no Accessed on 24.08.2023.

71 NOBLE, Safiya Umoja. *Algoritmos da opressão*: como o Google fomenta e lucra com o racismo. Felipe Damorim (trad). Santo André: Rua do sabão. 2021, p. 159; FISCHER, Max. *A máquina do caos*: como as redes sociais reprogramaram nossa mente e nosso mundo. Erico Assis(trad). São Paulo: Todavia, 2023, p. 242.

72 https://itsrio.org/pt/artigos/devemos-banir-a-inteligencia-artificial-nas-eleicoes/?utm_campaign=thinktech_52&utm_medium=email&utm_source=RD+Station Accessed on: 24.08.2023.

73 FISCHER, Max. *A máquina do caos*: como as redes sociais reprogramaram nossa mente e nosso mundo. Erico Assis(trad). São Paulo: Todavia, 2023, p. 117.

74 Towards a conceptualisation of hypervulnerability: https://normas.mercosur.int/simfiles/normativas/85763_RES_011-2021_PT_Protecao%20Consumidor%20Hipervulneravel.pdf Accessed on: 23.08.2023.

75 BUTLER, Judith. Discurso de ódio: uma politica do performativo. Roberta Fabbri Viscardi (Trad). São Paulo: Unesp. 2021, p. 16-17.

76 HUMMEL, Patrik; BRAUN, Matthias; TRETTER, Max et al. Data sovereignty: A review. *Big Data & Society*. V. 9, n. 1, p. 1-17, 2021. https://doi.org/10.1177/2053951720982012. Accessed on: 30.11.2023.

reality through the use of algorithms and the high speed of information sharing, focusing exclusively on engagement and maintaining attention in the digital age, has exorbitantly amplified the reach of disinformation and hate speech, increasingly contributing to hindering or preventing the average citizen discernment of the information conveyed[77] and, therefore, generating instability, insecurity, polarization, compulsion, and violence[78].

Turning our eyes briefly to what is happening internationally, we cannot fail to mention that the Supreme Court of the United States has not shied away from discussing the civil liability of digital platforms either. On May 18, 2023, two decisions were published (*Reynaldo Gonzalez et al. v. Google LLC and Twitter, Inc. v. Taamneh et al.*), which, based on the facts alleged by the plaintiffs, determined the impossibility of holding digital platform providers responsible for the use of algorithms to distribute content to users, on the ground that this measure belongs to the business model proposed by such providers. In these cases, however, the issue was not whether the providers were responsible for the actions of their users, but rather for their own actions[79].

At European level, the Digital Services Act[80] is taking its first steps. On April 25, 2023 it was established which are the Very Large Online Platforms (Vlops) and the Very Large Online Search Engines (Vloses), further defining the scope of its application[81]. Still in the European context, just to illustrate the point, the Irish Data Protection Authority recently fined Meta (owner of Facebook, Instagram, and WhatsApp), on the basis of the European General Data Protection Regulation (GDPR), 1.2 billion euros (around R$6.4 billion at the current price) for sharing European users' data with the United States.

77 https://www.forbes.com/sites/daviatemin/2023/05/26/the-nobel-prize-takes-aim-against-disinformation-lies-and-fakes/?sh=635eefb822d4 Accessed on: 13.08.2023.

78 https://www.peacetechlab.org/hate-speech Accessed on: 21.07.2023; https://www.terra.com.br/noticias/brasil/plataformas-digitais-fazem-campanha-contra-pl-das-fake-news,806cb4993c243f19be4a27fda6801121d3ombqto.html Accessed on: 23.08.2023.

79 To list a few emblematic cases: the US presidential election case (2016); the Cambridge Analytica case (2018); the case of the lynching of innocent people in India (2018); the Brazilian presidential election case (2018); the COVID-19 pandemic/INFODEMIA case (2020-present).

80 https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_pt Accessed on: 02.05.2023.

81 https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2413 Accessed on: 12.07.2023.

Returning to Brazil, without neglecting references to other experiences, it is essential to mention that, having failed to approving in time to be applied in the 2022 electoral process, the debate on the so-called Fake News Bill, which is currently before the National Congress, reignited after the brutal attacks on democratic institutions in Brasilia, DF, on 8 January, as well as the tragic wave of violence in schools across Brazil in April 2023[82], especially given the inertia of platform providers in removing content posted by users that aimed to promote or encourage acts of violence. It is worth noting that, with the issuance of Ordinance No. 351 of April 12, 2023 by the Ministry of Justice and Public Security, measures were already taken to prevent the online dissemination of blatantly illegal content, aiming to combat content posted on social media platforms that is intended to promote or incite violence in schools.

Also in this context, it should be noted that, as the Brazilian Bill on Internet Freedom, Responsibility and Transparency (PL 2630 - Fake News Bill) progressed, various versions of it have been discussed, and in late March 2023, the federal government sent its own version to the Chamber of Deputies, which began to be unofficially circulated in mid-April. Since then, other versions of the bill have been drafted by Congressman Orlando Silva (PCdoB), the bill's rapporteur in the Chamber of Deputies, focusing on the creation of a supervisory body to enforce the law, which has been the target of intense campaign of resistance, opposition, and sabotage by the tech giants. [83]

Another aspect to consider is that PL 2630, currently under consideration in the Brazilian parliament, among other things, defines that application providers have an obligation to take care of published content and must act diligently to prevent or reduce criminal practices on their services, combating publications that incite offences such as hate crimes, suicide,

82 It's worth pointing out that "*the first known attack on schools in Brazil took place 21 years ago and since then there have been another 24 similar cases. In total, there have been 137 victims and 45 people have died. The data was compiled by the Sou da Paz Institute. In relation to the period of the attacks, what the institute shows is an increase in occurrences from 2019 onwards. Between 2002 and 2019, seven attacks were recorded and in the last four years, from 2019 to this year, the number has more than doubled to 17. In the first four months of 2023 alone, there were six cases, the same number recorded in the whole of last year.*" https://soudapaz.org/noticias/agencia-brasil-brasil-teve-24-ataques-a-escolas-mais-da-metade-nos-ultimos-4-anos/ Accessed on: 21.08.2023.

83 https://www1.folha.uol.com.br/poder/2023/05/big-techs-fazem-acao-suja-contra-pl-das-fake-news-diz-relator.shtml Accessed on: 31.07.2023.

crimes against children and adolescents and coups attempting. They must also provide mechanisms that make it easier for users to report illegal content and follow transparency rules, submitting to external audits and preventing and mitigating the risks of its algorithms being used to disseminate illegal content that violates freedom of expression, information and the press and media pluralism, or that undermines the Brazilian electoral process. PL 2630 also deals with the possibilities of liability for damage caused by advertising on platforms or for failure to fulfil obligations to combat such content. Finally, it provides for punishments and fines of up to R$1 million per hour if they fail to comply with court decisions to immediately remove illegal content, which can be tripled if this content has been spread through platform advertising[84].

In this regard, it is more than reasonable to recognize the exacerbated concentration of informational[85], economic and technological power and political influence in the hands of giant technology corporations. It is known that these corporations concentrate, process, and sell personal and non-personal data, monitoring and manipulating everything and everyone, all the time. What is worse - and that's why appropriate regulatory schemes are so important - is that these corporations are largely immune to control, whether by the state or by organized civil society.

D. Final remarks

It is precisely in view of this framework, which has only been sketched out here, that good algorithmic governance takes on a central role at the moment, so much so that it needs to be realized through public policies, regulatory frameworks, ethical guidelines, audit negotiations, supervision and collaboration between the different stakeholders, as well as through the

84 https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1909983 Accessed on: 24.07.2023.

85 BRAZIL. Decree No. 11,574, of 20 June 2023. Amends Decree No. 10,046, of 9 October 2019, which provides for governance in data sharing within the federal public administration and establishes the Citizen Base Register and the Central Data Governance Committee. Brasília: Presidency of the Republic, 2023. Available at: http://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11574.htm . Accessed on: 19 ago. 2023.

direct involvement of civil society. In doing so, algorithmic governance[86] seeks to ensure that algorithms are monitored and used in a safe, robust, inclusive, ethical, transparent, fair, and responsible manner[87].

Considering the above and what the future holds, it should not be forgotten that Artificial Intelligence applications, including generative ones, despite all the positive advances, pose real risks and challenges for governance, such as, among other factors, lack of transparency, improper data collection, biases, invasion of privacy, impacts on copyright and patent protection, concentration of information power, and serious repercussions on the job market.

For these reasons, it must be ensured that algorithms are understandable and that the decisions they make are explainable, establishing forms of control and accountability for the actors involved in the development, implementation and use of AI[88] applications, in order to prevent and combat issues of algorithmic discrimination (especially those that are not easily identifiable), as well as ensuring, at least to a satisfactory level, people's privacy and data protection.

Furthermore, among many other points that could be mentioned, it is crucially important to prevent algorithms from contributing to perpetuating or widening existing inequalities, especially given the digital exclusion/division issue. To make it promote equal opportunities, just to mention one recognized crucial tool, regular analyses and evaluations must be instituted to monitor the performance and effects of algorithms use, allowing for adjustments and corrections as necessary[89]. In this regard, the use of impact reports in the field of data protection and, more generally, in relation to algorithmic impacts, stands out.

An explosive confluence for the maintenance of the democratic regime is undoubtedly the constellation that unites digital illiteracy and lack of literacy, the digital divide, as well as the lack of effective measures to ensure informational separation, digital sovereignty and cyber security equivalent

86 https://drive.google.com/file/d/1WFJppEqmmR9OuSaBH_qlOlzOQeXHGK_-/view Accessed on: 18.08.2023; https://www.oxfordinsights.com/government-ai-readiness-index-2022 Accessed on: 12.08.2023.

87 https://ethics.org.au/wp-content/uploads/2018/05/The-Ethics-Centre_PRINCIPLES-FOR-GOOD-TECHNOLOGY-29JAN.pdf Accessed on: 18.06.2023.

88 TEIXEIRA, João de Fernandes. *Inteligência artificial*. Coleção como ler filosofia. São Paulo: Paulus, 2014, p. 59-64.

89 O'NEIL, Cathy. *Algoritmos de destruição em massa*: como o big data aumenta a desigualdade e ameaça a democracia. Rafael Abraham(Trad.). Santo André: Rua do sabão, 2020,p. 327-331.

to the constitutional duties assumed by the Brazilian state in its digital version in the face of the disorganized implementation of 5G. In the Brazilian case, considering the above, it does not seem enough to exclusively bet on the implementation of 5G and neglect the structural complexity inherent in the domestic ecosystem, which is now deeply densified due to the algorithmic design of the Big Tech companies.

Vanishing Normativity? Legal Theory in the Digital Age*

João Paulo Bachur

Abstract: Legal theory confronts profound challenges in the digital age, where emerging technologies redefine traditional notions of normativity. This paper explores the intersection of jurisprudence and digital society, contending that the rise of algorithms and artificial intelligence disrupts the conventional understanding of normativity.

The digital landscape blurs distinctions between online and offline realms, requiring a reevaluation of legal normativity. While some view algorithmic regulation as eroding normativity by supplanting traditional legal norms, this paper proposes a nuanced understanding rooted in Wittgenstein's language philosophy.

Drawing on Wittgenstein's concept of rule-following, this paper reconceptualizes normativity as a continuum, encompassing algorithms, models/standards, and laws/norms. It argues that legal normativity can be better understood through implicit normativity, as articulated in discussions surrounding Wittgenstein's later writings.

Moreover, this paper advocates for a methodological shift in legal theory, emphasizing the role of socialization in normativity acquisition. Insights from Norbert Elias and Bruno Latour underscore the social processes

* A first version of this paper was drafted for the Conference "Digital Constitutionalism: A Normative and Institutional Framework for Conflict Solving under Construction", held at the Frankfurt University on March 3rd and 4th, 2023. For personal and health reasons, I could not attend the Conference. Nonetheless, I kept working on the paper and presented it in the "Pre-Reflective Agency Conference" at the University of Birmingham on June 29th, 2023, as well as at the Institute for Philosophy and Social Theory of the University of Belgrade, on November 16th, 2023, and at the Max Planck Institute for Legal History and Legal Theory in Frankfurt am Main, on November 21st, 2023. On these occasions, the paper had a different title – "*Rules, Rule-Following, and Implicit Normativity: A New Paradigm for Legal Theory?*". I thank Sylvie Delacroix, Mireille Hildebrandt, Georgios Pavlakos, Margaret Martin, Petar Bojanic, Srđan Prodanović, Marjan Ivković, Milan Urošević, Michal Sladaček, Christian Boulanger, James Thompson, Gabriel Brito, and Ricardo Martins Spindola Diniz for critical comments and remarks on the previous versions of this paper. I thank Laura Schertel Mendes, Ricardo Campos, and Indra Spiecker gen. Döhmann for including this paper in this edited volume.

underpinning normativity, transcending traditional philosophical frameworks.

In conclusion, this paper highlights the imperative for legal theory to adapt to the challenges of the digital era, reimagining normativity in the context of algorithmic behavior regulation. By embracing interdisciplinary perspectives and reconceptualizing normativity, legal theory can navigate the complexities of the digital age and elucidate the evolving nature of legal frameworks.

A. Vanishing Normativity? Challenges for Legal Theory in the Digital Society

It has been frequently said that legal theory has reached a "dead end": arguably, it may have lost the capability to make progress and overcome the so-called "post-positivism", and this in such an extent, that jurisprudence seems to have become an insulated academic discourse.[1] Nonetheless, the contemporary digital society poses new challenges for legal theory, and it may even put into question the key elements of traditional jurisprudence. As a matter of fact, the main schools of thought still dwell on the same issues that gave birth to modern legal theory with Hobbes and Bentham – morality, coercion, and the source of the binding force of law, the source of normativity. These old problems are now added to new questions presented by the so-called onlife world, a world that cannot be anymore understood by the binary distinction between online and offline, for it constitutes a new hybrid space that merges the digital, the factual-empirical, the social, the discursive, and the psychological dimensions of our lives.[2]

Legal theory has not even managed to overcome its old discussions, and it must already deal with the unraveling questions posed by the increasingly spread of algorithms and artificial intelligence applications for legal purposes, including legal decision-making. The new digital technologies are profoundly and unprecedentedly changing the legal landscape: smart cities, predictive policing, smart contracts, crypto assets, gig workers, and judicial mass decisions (even in criminal law) are now reality, not science fiction imagination. Almost all areas are touched by new disruptive technologies that promise to deliver personalized, unbreachable legal settings. At the cutting edge of legal theory, enthusiasts of this new 'personalized law' cheer

1 Auer, 'What is Legal Theory?', in *Rechtsgeschichte – Legal History*, vol. 29, 2021, 30.
2 Floridi, *The Onlife Manifesto – Being Human in a Hyperconnected Era*, 2015.

granular regulation enabled by the new digital technologies, for it may help us overcome the flaws and biases of human adjudication: "*the use of big data analytics and artificial intelligence could recalibrate the relationship between law and individuality and change the foundational structures of our legal system*".[3] On the other hand, critical voices claim ethical guidance for technological applications, some level of coercive regulation, or protection by default provided by technology itself.[4]

When you replace the traditional legal system with technological behavior guidance, that is, when '*code becomes the law*'[5], you may miss all 'the rest' usually attached to the traditional rule of law within a constitutional framework – individual rights, liberal democracy, adjudication, due process guaranties, checks and balances, and so on. Just like the printing press once eroded the possibility of religious censorship, enabled the systematization of all pre-modern law (from Justinian *Corpus Juris Civilis* to ancient English Common Law), and became the technical means of positive law as adjudication, we may be experiencing an equivalent earthquake with big data analytics and artificial intelligence, but in a much faster pace – for better or worse. For we watch the new possibilities of blockchain and artificial intelligence systems as well as the rise of new far-right populism, surfing the wave of fake news and disinformation, threatening the institutional framework of liberal democracy.

When legal philosophers discuss new technologies, it usual to find the diagnosis that the algorithmic society precludes the normative character of legal institutions. Christoph Möllers for instance, a contemporary leading German scholar, sees the core of normativity in the possibility of breaking a rule: no rule can be said to be normative if you cannot choose whether to break it or not. This tight connection between rules, rule-following and normativity will be fully discussed in this paper; for now, let's just assume that normativity (in this traditional sense) presupposes: (*i*) a previous rule and (*ii*) agency from the part of the subject to choose whether to comply and follow the rule or to breach and act against the given rule. When discussing new thresholds for normativity in the digital age, Möllers argues

3 Busch & De Franceschi, 'Introduction', in *Algorithmic Regulation and Personalized Law: A Handbook*, 2021, 1. See Sunstein, *Choosing Not to Choose*, 2015, 157 ff., for an optimistic approach, but Auer, 'Granular Norms and the Concept of Law: A Critique', in *Algorithmic Regulation and Personalized Law: A Handbook*, 2021, 137-154, for a convincing counter point.

4 Hildebrandt, *Smart Technologies and the End(s) of Law,* 2015.

5 Lessig, *Code and Other Laws of Cyberspace*, 2000.

that algorithmic regulation forecloses normativity: "An algorithm excludes normativity. A community whose behavior is programmed has no room for norms".[6]

This diagnosis echoes the famous slogan "the code is the law", meaning that new digital technologies regulate behavior in such a granular and empirical way, that it becomes apart from the general standards that characterized modern law. As we know it, modern law – the positive law issued in by the political system to be applied in future cases – works articulating universals (i.e., general abstract rules) to individual cases. But does it make sense to state that algorithms exclude normativity? Mireille Hildebrandt, one of the leading scholars that deal with technological issues from the perspective of legal theory, advocates for "legal protection by design", and this solution also implies the diagnosis that algorithms overcome legal normativity – only because the normativity of general rules is insufficient, we could claim legal protection by design, that is, legal protection that is inscribed in the technology itself.[7]

But are we comparing similar phenomena? The affordances of the new digital technologies make us behave in specific ways and, in a weak sense, they can be seen as 'normative', to some extent. When we agree to cookies to visit a website, we are not consenting in a proper way, we are just doing what it takes to visit the website. When you scroll your news feed on Twitter, TikTok or Instagram, you are not consciously consenting to the profiling that is being made of you – you just cannot avoid it if you want to check up your social media. So, new technologies make us behave in certain ways, and law also makes us behave in certain ways. The question for legal theory is then the following: are algorithms and rules equally normative? Moreover: are algorithms taking the place of legal normativity, the cornerstone of jurisprudence?

This paper offers an initial answer to this question. At the heart of the problem is the question of rule-following: is it a habit or a rule-driven action? Once we understand what it means to follow a rule, we can distinguish the rule of algorithms and the rule of law. This paper will offer an alternative explanation for legal normativity inspired by the rule-following issue in Wittgenstein's *Philosophical Investigations*. As we shall see,

6 Möllers, *Die Möglichkeit von Normen*, 2015, 455: "Ein Algorithmus schließt Normativität aus. Eine Gemeinschaft, deren Verhalten programmiert wird, hat keinen Raum für Normen".

7 Hildebrandt, *Smart Technologies and the End(s) of Law*, 2015.

there is not solely one mode of normativity. The problem of traditional jurisprudence is that it absorbed only *one* normativity regime, namely the one inherited from moral philosophy. So, it is not a coincidence that the first generation of studies on the problems created by big data analytics and artificial intelligence decision-making systems usually ended in ethical claims towards tech developers within the framework of self-regulation – a naïve solution, as we now see. Section B catches up with the problem of normativity in traditional jurisprudence. Once we start with a strict bifurcation between facts and norms, normativity is given and attached to a preexistent norm. If normativity is not given from the sky, legal theory should explain its social emergence.

Section C advances the hypothesis that normativity (in general, not only legal normativity) is better understood as a *continuum*, not in a dichotomic relation to facts. I suggest to replace the 'is'/'ought' (*Sein/Sollen*) dichotomy by a *spectrum of normativity*, one that is structured by a matrix that connects normativity regimes with different types of rules. The connection between norm and legal normativity is neither the only possible nor the best way to understand how the law works. As I see it, there is a historical connection between different meanings for the concept of '*rule*', to which correspond three different normativity regimes: *algorithms*, *models/standards*, and *laws/norms* correspond each to three different modes of normativity, namely: *pseudo normativity*, *implicit*, and *explicit* normativity. We aim to show that the so-called *implicit* normativity, as it is currently understood in discussions around Wittgenstein's later writings, helps explaining legal normativity. The model for legal normativity will no longer be the moral philosophy of practical reason, but ordinary language. We will see that normativity demands *learning* and *acquiring skilled competencies*, which forces us to leave philosophy and enters the realm of socialization, an interdisciplinary mixture of sociology, psychology, and anthropology. Section D will then make this methodological shift with the help of Norbert Elias and Bruno Latour. We will show how normativity is acquired and learned in the process of socialization, at first only intuitively, guided by feelings of appropriateness and inappropriateness, allowing, with age and time, the possibility of explicit problematization of conduct in binary terms, such as right/wrong, legal/illegal. This would grant us the possibility of a bottom-up legal theory that does not start with state authority. Finally, section E will conclude, resuming the challenges presented by the digital society, for they call into question the traditional understanding of normativity considering the overwhelming presence of algorithmic behavior regulation.

B. The Problem of Legal Normativity

David Lewis opens his classic book *Convention* by stating: "It is the profession of philosophers to question platitudes that others accept without thinking twice".[8] He goes on and says that philosophy is a dangerous profession because the platitude often defeats the philosopher. Even though the platitude survives, the philosopher will have done her job by making others think twice. In this section, I will risk challenging some grounding axioms of modern legal theory: the assumption that legal normativity has nothing to do with habits and requires a previous norm to take place. It has been indeed a platitude to state that law is normative. But as we do so, we only presuppose what we should explain. And we should think twice on this matter.

The mainstream legal theory takes the normativity of law for granted. In this paper, I will use '*traditional*' or '*mainstream legal theory*' as well as '*legal positivism*' and '*analytical jurisprudence*' in a relatively interchangeable way, despite all scholastic internal divisions between legal positivism schools, for they share a common point of departure, namely, that law is already normative from the outset. As Hart puts it:

> My main objection to this reduction of propositions of law which suppresses their normative aspect [*i.e., to Ross*] is that if fails to mark and explain the crucial distinction that there is between mere regularities of human behaviour and rule-governed behaviour. It thus jettisons something vital to the understanding not only of law, but of any form of normative social structure.[9]

Even when we acknowledge the difference between Hart's take on habits and rules, including the complex discussion of his practice theory of norms and the problem of the internal point of view of rules (which I will not address in this paper), and Kelsen's *Pure Theory of Law*, which takes the cleavage between the '*is*' and the '*ought*' ('*Sein*' and '*Sollen*') realms to a categorical level, we can still trace a link between the continental and the analytical traditions: both comprehend law exclusively within the framework of a rigid difference between facts and norms.

And, of course, you may doubt that law could one day be imagined beyond this difference (as I do myself). I do not argue that practicians should

8 Lewis, *Convention*, 1969, 1.
9 Hart, *Essays in Jurisprudence and Philosophy*, 1983, 13.

or could dismiss this difference. That is hardly imaginable, of course. The problem is not the difference in itself, for the 'law in action' may never need to overcome the operational distinction between facts and norms. It is precisely this distinction that enables modern law in contemporary industrial societies, including adjudication – namely, matching claims and contentions to a previously given set of categories and rules, no matter if these rules are laid down by previous case law or state-issued legislation. In this respect, the different facts/norms remain indispensable. But jurisprudence faces serious trouble when it embraces the fact/norm distinction as deployed by barristers, judges, courts, and legal officials on an *operational* level and elevates it, on a *methodological* level, to an epistemic axiom, expressing with it an unbridgeable gap between two incommunicable worlds.[10]

The unbridgeable gap between the world of facts and the world of norms is an entirely different thing. There is indeed a massive difference between a distinction and a dichotomy: "ordinary distinctions have ranges of application, and we are not surprised if they do not always apply".[11] The distinction fact/norm grounds the routine and daily tasks of anyone who works with law, and it can never be surmounted at this operational level. Professionals have problems to solve, and the fact/norm distinction provides an excellent strategy to make social complexity operational, enabling us to classify human and non-human (i.e., corporate, institutional or technological) behavior as conform or deviant: using Luhmann's terminology, the fact/norm distinction works pretty well within legal dogmatics and doctrinal law, but jurisprudence runs on a higher, more abstract level of reflection within the legal system.[12]

Along the evolution from natural to positive law, from contract theories of the 18th century to Hegel and the codification dispute in the 19th century, reaching Kelsen and Hart, the fact/norm distinction became a methodological dichotomy that, claiming Hume's philosophical authority, became a kind of *episteme* for jurisprudence. It has been a matter of dispute whether Hume meant what legal positivists ascribe him without further questioning, but we do not need to engage in this discussion right

10 Blackburn, 'Normativity à La Mode', in *The Journal of Ethics*, vol. 5, n. 2, 2001, 140.
11 Putnam, *The Collapse of the Fact/Value Dichotomy and Other Essays*, 2002, 11.
12 Luhmann, *Das Recht der Gesellschaft*, 1993, 12, and Luhmann, *Rechtssystem und Rechtsdogmatik*, 1974, 13 ff.

now.[13] It seems hardly disputable that jurisprudence made the fact/norm distinction epistemic, meaning that this distinction has become a discursive precondition to the legal theory itself. An episteme is the set of parameters that make knowledge possible in a given culture for a given branch in the human sciences.[14] The episteme is an infrastructural foundation for conceptual thought, knowledge, and discourse. For this reason, it can be defined as a historical *a priori* internally developed in some disciplines in the human sciences. It is often described with the metaphor of a space or a region between the practical level of culture and the elaborated level of science, the hiatus that make the internal criteria of a scientific system corresponds to the intuitive knowledge of culture. Someone could do, for legal theory, what Foucault has done regarding other human sciences: in his classic book *Words and Things* (usually translated as *The Order of Things*), Foucault describes a rationalist or intellectualist turn in the human sciences from the 17th century onwards, one that transformed general grammar into linguistics, the study of the causes of wealth into political economy, and natural history into biology. These taxonomic endeavors originated scientific systems. One could redo the path from medieval commenting on Roman texts, especially the Justinian codifications, to the systematization of ancient Common Law and the conceptualization of the German Historical School, culminating in the Constitutional revolutions of the 18th century, and civil law codifications throughout the 19th century, to argue for an epistemic transition in law. From a heuristic perspective, the taxonomy of custom, case law, and Roman formulae appear to have given way to the intellectualist conception of law as a system of norms.[15]

13 Bix, 'The Normativity of Law', in *The Cambridge Companion to Legal Positivism*, 2021, 591. Definitely against the fact/value dichotomy, see once again Putnam, *The Collapse of the Fact/Value Dichotomy and Other Essays*, 2002, 14: "What Hume meant was that when an 'is' judgment describes a 'matter of fact', then no 'ought' judgment can be derived from it", "there is a distinction to be drawn (one that is useful in some contexts) between ethical judgments and other sorts of judgments. (…) But nothing metaphysical follows from the existence of a fact/value distinction in this (modest) sense" (19), and finally: "This has led a number of commentators to misread Hume (…)" (20).

14 Foucault, *Les mots et les choses*, 1966, 11 ff.

15 To my knowledge, this Foucauldian study remains to be done. For pieces of this puzzle, see Pirie, *The Anthropology of Law*, 2013, 81 ff. and 135 ff.; Haferkamp, *Die historische Rechtsschule*, 2018; and Berman, *Law and Revolution*, v. 1 (*The Formation of the Western Legal Tradition*), 1983.

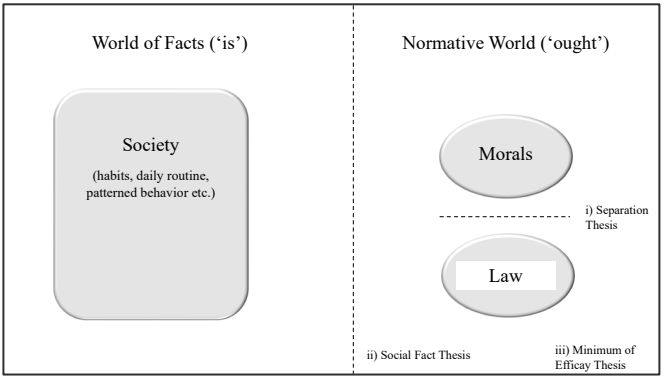
From that point onwards, law became *positive* law and should be able to ground itself without resorting to divine or natural laws. And this quest for self-foundation could be done only in a paradoxical manner, by stating that law is normative in itself, overlooking at the same time the factual, conjunctural, and political production of law (both in legislation and adjudication, i.e., as starting and end point of judicial decisions). This is indeed the point of departure for almost every mainstream legal theory: the unproblematic assumption that law is already normative from the start.[16] It may not sound as troubling as it is, but the paradox becomes unavoidable if you closely read the famous theses that make up mainstream legal positivism. Legal positivism is commonly described as a theoretical commitment to three central tenets:

i) the *separation* thesis has it that there is no necessary connection between law and morality;
ii) the *social thesis* asserts that what counts as the law is defined by social facts (or, without euphemisms, that law is the byproduct of contingent decision-making of politicians, judges, and courts), and
iii) the *minimum efficacy* thesis holds that the validity or existence of law depends on a minimum level of social compliance, for no law can be said to exist if everyone massively ignores it.[17]

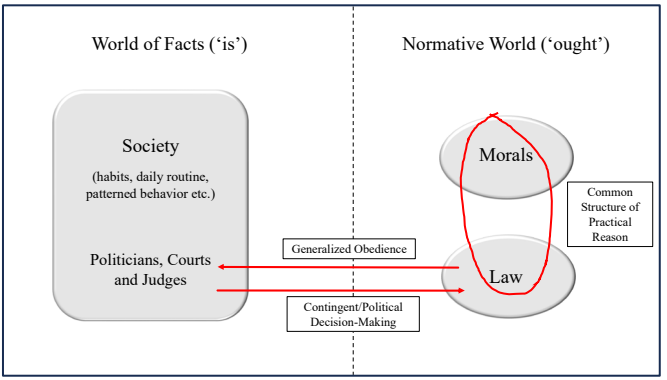
These tenets are formulated in a reasonable and almost irretrievable manner, concealing the harsh distinction between a world of facts and a world of values and norms underneath it. The following figure illustrates how these tenets should provide a clean legal system, which relies on a minimum level of social efficacy, remaining nonetheless isolated from society and separated from morality:

16 For instance, Bertea, 'Social-Practice Legal Positivism and the Normativity Thesis', in *Cambridge Companion to Legal Positivism*, 2021, 406: "From the premise that law is shaped by a collective pattern of behaviour, social-practice legal positivism derives the conclusion that, as a *social* fact, law is also a *normative* institution. The social practice on which the law fundamentally rests, in other words, includes a normative component. (…) Importantly, this normativity thesis is a thesis not about the *language* of law but about the law *itself*: It is pointing out a *property* of law (…)" – original highlights.

17 Spaak & Mindus, 'Introduction', in *The Cambridge Companion to Legal Positivism*, 2021, 7.



But we should not take these three tenets of legal positivism at their face value. In that case, we must recognize that there must be a connection between law as a social fact and law as a normative order: politicians, judges, and courts do indeed produce law, and law depends constitutively on generalized compliance. So, the law cannot be genuinely and originally normative. On the other hand, if law must be genuinely and originally normative, it will share the common ground of practical reason with morality, a feature that mitigates the separability thesis. To be separated from morality, law must rely on its social character (habitual compliance and contingent decision-making); to be completely isolated from the factual world, law must self-validate itself, just like morals. The following figure illustrates the reciprocal contamination of facts, law, and morals:



To sum up: you cannot have it both ways: law must be equivalent to morality if it is not to be derived from facts, or it must derive from facts if it is not to share the same structural features of morality. For this reason, "*[o]ne recurring objection has been that one cannot account for the normativity of law within the framework of legal positivism*".[18] The law cannot be utterly loose from morality and completely loose from society, and that is why the premises of mainstream legal positivism do not hold: "One of the key challenges for legal theory (…) is to account for law's normative dimension. As a social artefact, whence does law draw its power to bind us?".[19] If you relax the social-artefact requirement, positive law gets closer to morality. If you do not relax this requirement, it gets closer to the daily routine of legal officials and general compliance by ordinary citizens (and, therefore, closer to habits). We are left with a mystery yet to be solved, for we still have no explanation of how habits and the daily routine of those professionally in charge of making laws, filing lawsuits, and deciding cases "can ground normative conclusions about what citizens should and should not do".[20]

C. The Spectrum of Normativity and the Matrix of Rules

What does it mean to say that law is normative? How is it different from other normative orders? Why and how does it bind us in a specific manner? Legal theory has collected a series of competing answers to these questions. For instance, Kelsen's canonic *Pure Theory of Law* carries the neo-Kantian split between is/ought to its limits, and he is perhaps the most radical version of the so-called Hume's guillotine.[21] On the other hand, Hart's masterpiece, *The Concept of Law*, offers a more nuanced landscape, questioning explicitly the borders between habits and rules. But even Hart rejects the possibility of any normativity arising out of habits, placing the center of the legal system in the union of primary and secondary rules, as well as in the '*internal aspect of rules*.[22] In his turn, Shapiro states, "*Because the*

18 Spaak & Mindus, 'Introduction', in *The Cambridge Companion to Legal Positivism*, 2021, 14.

19 Delacroix, *Habitual Ethics*, 2022, 92.

20 Bix, 'The Normativity of Law', in *The Cambridge Companion to Legal Positivism*, 2021, 591.

21 Kelsen, *Reine Rechtslehre*, 2nd ed., 1960.

22 Hart, *The Concept of Law*, 1961, 56/57. We will not discuss the '*internal aspect of rules*' in this paper.

planning model replaces habits with plans, it has no problem explaining the normative nature of legal activity".[23] Brian Bix, in contrast, suggests that law has a "*sui generis form of normativity*" that prevents law from resorting to morality without dissolving law into facticity – although this suggestion is not completely convincing.[24]

All mainstream positivism begins with a given normative dimension in different variations: *Sollen* in Kelsen, rules in Hart, and plans in Shapiro. In all these cases, we can only rely on the critical reflective attitude of the individual, who access the normative character of law, evaluates the available possible courses of action, and decides how to act. In all cases, the structure of practical reasoning is presupposed, and the discussion of *legal* normativity seems to be rooted in the underlying assumption of *moral* normativity as a paradigm:

> The usual concept of morality refers to norms of a particular kind, which in one way or another will be distinguished from legal norms, for example, according to the distinction between internal and external behavioral controls. Thus, however, the concept of morality remains so closely related to that of law *on the everyday basis of norm*, that this alone creates difficulties for the imagination of a separation of law and morality.[25]

On the one hand, legal theory resists the idea that legal normativity be comprehended empirically; at the same time, it is difficult not to take moral normativity as a model: "*We can understand the concept of legal normativity only by appealing to other normative concepts*"[26] – and they are most likely to be moral. The discussion on normativity gravitates around the fact/value (is/ought) dichotomy. If we remain trapped inside this dichotomy, we must decide if normativity should be placed on the 'value' side or the 'fact' side, whether it is a given 'ought' or plain facticity. For this reason, it may be safer to reject the fact/value dichotomy in favor of a *naturalist* account, rejecting the ontologically unbridgeable gap between *is* and *ought* or between *facts*

23 Shapiro, *Legality*, 2011, 189.
24 Bix, 'Kelsen, Hart, and Legal Normativity', in *Revus: Journal for Constitutional Theory and Philosophy of Law* 34, 2018.
25 Luhmann, *Kontingenz und Recht*, 2013, 141 – my highlights.
26 Redondo, 'Legal Normativity as a Moral Property', in *Revus: Journal for Constitutional Theory and Philosophy of Law* 34, 2018.

and *norms*.[27] But, if we do so, we will claim that legal normativity has its source in *non-normative* realms, in facts (!), including daily practices and habits. That is precisely the idea.

One way to define the naturalist approach can be found in recent research on 4E cognition.[28] The so-called 4E cognition can be qualified as an interdisciplinary research area that merges pragmatism, philosophy of mind, phenomenology, and cognitive sciences, to understand cognition as the result of radically *embedded*, *embodied*, *extended,* and *enactive* processes. In a way, it is a radical rejection of the disengaged mind that has been bequeathed to us by Descartes' *cogito* and Kant's transcendental conditions as a model for knowledge and perception.[29] 17th-century rationalism elaborated what we can call a '*discontinuity thesis*' – mind, or, in the old terms, reason and nature belong to different worlds, and the only certainty that the mind can have of anything relies on its rational self-reflection. 4E cognition theories reject this discontinuity thesis in favor of a "*life and mind continuity*", according to which there can be no arbitrary disruptions between nature, mind, and (why not?) morals. That is why cognition is better understood as an *embodied* process, for the body cannot be deemed irrelevant. Cognition is also an *extended* process, for it is *embedded* in society, nature, culture, and any other extra-bodily instances, as it is also *enacted* once it cannot be reduced to the passive assimilation of the outside world but depends on some level of agency.[30]

The continuity thesis excludes the possibility of an outside force that appears in a *deus ex machina* manner, fallen from the sky:

> To this we would add not so much an emphasis on 'forces' outside the naturalistic framework but the rejection of the sudden appearance of fully independent novel levels of description – for instance, the realm of *human normativity* – without an account of *how their emergence and relative autonomy is grounded on* (understandable in terms of and

27 Delacroix, 'Understanding Normativity', in *Revus: Journal for Constitutional Theory and Philosophy of Law* 34, 2018.

28 See the collected essays in Newen, De Bruin & Gallagher (eds.), *The Oxford Handbook on 4E Cognition*, 2018. On naturalism, see also Delacroix, *Habitual Ethics*, 2022; Ginsborg, *The Normativity of Nature*, 2014; and Blackburn, 'Normativity à La Mode', in *The Journal of Ethics*, vol. 5, n. 2, 2001.

29 Damasio, *Descartes' Error*, 1994.

30 Newen, De Bruin & Gallagher, '4E Cognition: Historical Roots, Key Concepts, and Central Issues', in *The Oxford Handbook on 4E Cognition*, 2018, 6.

> interaction with) *phenomena at other levels*. This is as much a causal/historical point as it is ontological. The continuity thesis therefore proposes the need for a theoretical path that links living, mental, and social phenomena.[31]

This point of departure for jurisprudence may make the hair of an orthodox legal positivist's stand on end. According to the continuity thesis, legal normativity should derive from facts, from society, given that there is no chance to postulate a great divide between the normativity of the legal system and the non-normative existence of society. In a way, legal normativity should be rooted in practices and habits. But how is that possible?

Jurisprudence has traditionally chosen a reductive account of normativity within the fact/value dichotomy. Joseph Raz, for instance, states that the key concept for explaining norms is a reason for action, and he grounds jurisprudence in practical philosophy: "Legal philosophy is nothing but practical philosophy applied to one social institution".[32] Within this framework, law is just a specification of practical philosophy, an institutional projection of moral reasons, for morals and law share the same essential feature – they are normative in as much as they provide reasons for action: "All normative phenomena are normative in as much as, and because, they provide reasons or are partly constituted by reasons".[33]

Even though this conception is a pervasive feature of analytical jurisprudence, we can contend that his connection between legal theory and practical reasoning is contingent, not necessary. It is derived from moral philosophy, but in any case, it is not the only possible explanation for human action and its constraints – normative and otherwise. But mainstream jurisprudence sells it as the only sound explanation for the normativity of law. If positive law must validate itself without resorting to natural law, god, ancient tradition, or morality, it can only rely on the self-validation of reason. But the only kind of self-validation that the disengaged reason can provide is the one that isolates itself from the world. I want to make the point that accessing and evaluating *reasons* is by far not the only or exclusive way to act.

31 Di Paolo, 'The Enactive Conception of Life', in *The Oxford Handbook on 4E Cognition*, 2018, 74 – my highlights.
32 Raz, *Practical Reasons and Norms* [1975], 1990, 149.
33 Raz, 'Reasons, Reasons, and Normativity', in *Oxford Studies in Metaethics*, 2010, 5.

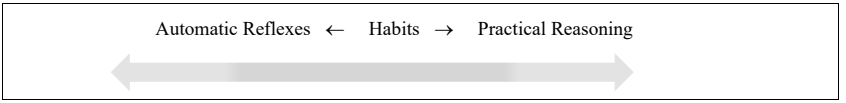
Usually, we follow the law in a semi-intuitive way, "*doing what comes naturally*", to use a famous expression.[34] Hart himself acknowledged that: "When we move a piece in chess in accordance with the rules, or stop at a traffic light when it is red, our rule-complying behaviour is often a direct response to the situation, unmediated by calculation in terms of the rules".[35] When we stop our car at a red light, we are not necessarily weighing the chances of being stopped by the police and fined. When we pay our taxes on time, we are not always calculating whether it is worth trying to evade taxes. When we sign a contract with a gym, the clauses are relatively indifferent in their details because we know how the relationship between a client and a gym works. The fact that legal theory has chosen solely and exclusively the model of practical reason to ground legal normativity becomes an artificial requirement, considering the reality of people's daily lives. On the other hand, normativity, in general, does not need that we presuppose a previously given norm, from which a command emanates and pervades the reasoning subject while she thinks and evaluates available courses of action, as well as the corresponding risks and consequences. We need to undo this strict association between *norm* and *normativity* and reframe it on a more abstract conceptual level.

We need a fresh start. If we give up, I mean, if we *really* give up the fact/value dichotomy, we cannot think of normativity in a binary relation to facts anymore. This 'either-or' scheme provided by the fact/norm difference must be replaced by a continuum, a spectrum of normativity. And you may reply, of course, that with a continuum, we will give up the possibility of clear-cut distinctions within the normativity realm. Sure. But "*Isn't the blurred sometimes exactly what we need*"?[36]

Giving up sharp artificial distinctions may help us achieve a clearer glimpse of the phenomenon we are trying to observe. The philosophy of practical reasoning had always presupposed a rational chain linking '*norm* → *reasons* → *action*'. I suggest we move to a continuum of normativity regimes, in which practical reasoning is nothing but an extreme case. Law as a whole cannot be backed by it anymore. On the other extreme point, we find automatism and reflexes: mere reactions to get along with daily affordances. They may explain some of our reactions (like when we stop at a red light), but they also cannot account for law as a whole. The middle

34 Fish, *Doing What Comes Naturally*, 1989.
35 Hart, *The Concept of Law*, 1961, 140.
36 Wittgenstein, *Philosophische Untersuchungen* [1953], 11th ed. 2022, § 71, 60.

is occupied by habits: clusters of repeated patterned behavior, including unconscious, pre-reflective, and goal-driven ones.[37] Habits lie at the heart of the normativity spectrum, and they can evolve to extremes– solidify into automatic reflexes, or detach from context into practical reasoning. So, it is not an evolution from automatism to practical reason. On the contrary, it is a continuum with a *radial* logic that spreads from the center to both ends: habits can evolve in either direction but remain at the center. None of these frontiers are positivistic ones. Automatism can dissolve, and practical reasoning can be softened back. So, we would have a continuum like this:



Each of these points corresponds to one type of rule. There is no sense in saying that habits are completely rule-free, and at the same time, even automatism does 'follow' some rules. But they are rule-driven in entirely different senses. In *Rules: A Short History of What We Live By*, Lorraine Daston offers an erudite and nonetheless synthetic, truly worth reading, history of nothing less than – *rules*.[38] Throughout human history, she has identified three ideal types of rules: tools of measurement and calculation (algorithms), models or paradigms, and regulations (laws or norms in the traditional sense). Albeit the first and the latter are well-known, she discloses the lost history of rules as standards, the most ancient rule type. She goes back to the ancient Greek word for the giant cane plant (*Arundo donax*) – '*kanon*', derived from the Semitic word '*qaneh*', that became '*regula*' in ancient Latin – and that was used as a pattern for all kinds of construction works, a standard measure for buildings. This kind of rule pervaded almost all realms of human skilled tasks. In the arts, sciences, and most different handicrafts, many manuscripts and books were written to guide navy and civil construction, rhetoric, sculpture, poetry, the routine in medieval monasteries, music composition, cooking, and science experimentation. These rules were meant to serve as ideal examples, models to

37 Habits do not equate only to automatic responses to outside stimuli, in behaviorism fashion – see Delacroix, *Habitual Ethics*, 2022, 4 ff.

38 Daston, *Rules: A Short History of What We Live By*, 2022. See also Oppel, *KANΩN: Zur Bedeutungsgeschichte des Wortes und seiner lateinischen Entsprechungen (Regula-Norma)*, 1937.

be followed, which always presupposed some implicit or tacit knowledge of the skilled practice.

Algorithms, on the other hand, became to mean "*any step-by-step procedure used in calculation or problem-solving*".[39] The English word 'algorithm' is the Latinized version of the name of a Persian mathematician, Muhammad ibn Musa al-Kharizmi (c. 780 – c. 850 CE), whose treatise on calculation was translated into Latin in the 12th century. "The modern meaning of algorithm is quite similar to that of recipe, process, technique, procedure, routine, rigmarole, except that the word 'algorithm' connotes something just a little different. Besides merely being a finite set of rules which gives a sequence of operations for solving a specific type of problem, an algorithm has five important features [finiteness, definiteness, input, output, effectiveness]".[40]

Finally, laws and norms are close to the legal positivistic understanding of rule as explicit regulation formulated in general terms. Deriving from natural laws and directly inspired by the success of natural sciences led by Newtonian physics, "Regulations are rules at their nitty-grittiest".[41]

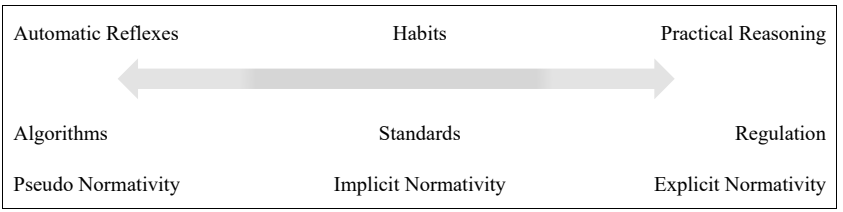
This landscape breaks with the monolithic image of legal positivism, which only considers rules as norms, in the third sense, as commands or reasons to act. Rules as regulations express an evolutionary acquisition of modernity and the Enlightenment, and there is no sense in taking this kind of rules as the only possible, ontological 'mode of existence' of rules. Indeed, there is much discussion within legal positivism as to whether the concept of rules does justice to a vast array of officially written directives.[42] The historical account of Lorraine Daston offers a much richer picture of the development of rules and seems to offer a broader frame to grasp legal phenomena as well. If the modern state-issued codified law relates more closely to rules as norms, the late Roman civil law and modern collateral agreements in financial markets and administrative legislation issued for policy implementation relate instead to rules as standards.[43] Finally, and resuming the opening questions of this paper, new digital technologies pro-

39 Ibid., 85.
40 Knuth, *The Art of Computer Programming*, vol. 1 *Fundamental Algorithms*, 1997, 4-6 – apud ibid. 85.
41 Daston, *Rules: A Short History of What We Live By*, 2022, 207.
42 And the dispute on rules and principles is but the tip of the iceberg.
43 Riles, *Collateral Knowledge*, 2011, 49; Rubin, 'Law and Legislation in the Administrative State', in: *Columbia Law Review*, vol. 89, n. 3, 1989, 371/372.

vide some behavior regulation that is closer to rules as algorithms. These three rule types vary in whether they are:

i) *thick* or *thin* in their formulation, that is, if they are granular or expressed in broad terms,
ii) *flexible* or *rigid* in the application,
iii) *general* or *specific* in the domain of application, but also in
iv) how the *core* or the essential features of the rule relate to *accidents* and *exceptions*, and
v) how they bridge the gap between *universals* and *particular* 'cases'.

Of course, these three categories may overlap and relate to each other, and they may be at the same time present, working together in a given situation. I do not mean to immobilize them in a given place; they have blurred borders. The point I would like to make is that they seem to fit the normative spectrum to explain different regimes of normativity. So, instead of sharply contrasting habits and the legal system with the help of the fact/norm dichotomy, we would have different normativity regimes relating to different types of rules. If we connect each kind of rule to the spectrum of normativity, it will look more or less like the following:



Now we begin to see why Möllers' statement that "*an algorithm excludes normativity*" is not precise. The force of algorithms expresses one kind of normativity, which is different from the normativity of general rules. But one cannot simply replace the other. There is not only one possible understanding of normativity, and no explicit norm must be presupposed for normativity to occur. These new kinds of normativity, implicit and pseudo normativity, occupy the rest of my paper. So, we move next to implicit normativity and close our reflections with the new challenges posed by the new information and communication technologies, for they may incarnates a kind of 'pseudo' normativity when the 'code becomes the law'.

D. Implicit Normativity and the Building of Expectations

The formulation of *implicit normativity* may sound like a contradiction in terms. After all, being explicitly formulated as a *recognizable command or directive* is part of the definition of a norm, at least in its traditional meaning. An implicit normativity must mean that it is not explicitly articulated – and if so, how do we recognize something like that? How can someone acknowledge this kind of normativity?

First, it is crucial to refrain from thinking of normativity again according to the model of practical reason. In our continuum, it is only the most extreme derivation from habits, not the sole mode for normative behavior guidance. Indeed, if the law is made up of society and language, legal normativity must display features equivalent to *meaning* and *social bonds*. As we saw previously in this paper, law just imported the model of practical reason from moral philosophy. In a way, legal positivism reaches beyond and falls short of natural law: it aims to provide a self-validation for law in as much as it aspires to lose itself from morality, but it has only the model of moral philosophy at hand, so it embraces *the form* of it, not the content. If we take language and society (and not morals anymore!) as paradigms for law, new modes of normativity may become visible. In this section, we will deal with two forms of implicit normativity. One is the normativity of *meaning*, and the other, the normativity of the *social*. And this kind of implicit normativity can provide us with a fresh start, for it relates to rules as standards and patterns, not to rules as norms or regulations, and it is responsible for building expectations.

Implicit normativity refers originally to a philosophical discussion around one of the most important books of the 20th century – Wittgenstein's *Philosophical Investigations*. Published a little after his death, this text is intensively debated until today, for it is placed in a tense relationship, to say the least, with Wittgenstein's *Tractatus Logico-Philosophicus*: while the latter connects to the logical positivism of the Vienna Circle, the former may be read as an anti-positivistic language philosophy. We cannot address all the complex issues involved in making sense of the *Philosophical Investigations* here, but we can derive some productive insights for a renewed jurisprudence. The book is difficult for many reasons, one being that it was written as a sequence of short aphorisms, recurring to a series of examples.

Another reason is that Wittgenstein already achieved the status of a classic, so he is much more quoted than closely read.[44]

Three key issues should be addressed: the concept of '*family resemblances*' (*Familienähnlichkeiten*), the notion of language games (*Sprachspiele*), and the trouble around 'following a rule'. Although Wittgenstein was not writing on law, and his concepts should not be automatically transplanted to jurisprudence, his take on rule-following is essential for legal scholars, for it offers a new solution to the main problem of legal theory, namely – how to avoid the infinite regress. This problem lies at the heart of modern legal thought, for Kelsen and Jellinek, as much as for Hart and Shapiro (who translate this canonic problem in the jocular formulation of a 'chicken-egg' paradox). His solution to infinite regress resorts to an implicit normativity and, at the same time, exhausts the conceptual resources of philosophy, imposing a methodological shift towards socialization, so it becomes visible how expectations and anticipation can be learned and acquired. And this may be the core of a new legal theory, one that does not start from within the framework of practical reasoning and moral philosophy but from *practices* or *habits*, because they are the locus where the building of expectations occurs.

First, it is essential to grasp that language games are a concept developed by Wittgenstein to express the impossible distinction between the linguistic and the non-linguistic realms. That was precisely what John L. Austin, in *How To Do Things With Words*, attempted to do: to isolate the speech act and the appropriate circumstances from another, so you could qualify a speech act as 'happy' or 'unhappy', and establish a catalog of verbs that could express the different functions of language (what he called 'illocutionary forces').[45] That is why the language game is not only a way of speaking but speech routines embedded in life forms, which do not make sense once they are disembedded, and that is why they are prone to infinite. There is no way to establish, once and for all, every possible language games in a closed codex.[46] Language games express the constitutive *embeddedness* of language and the impossibility of accessing meaning through the subjective intention of the speaker alone.

44 In what follows, I based my reading of Wittgenstein in Bertram, *Sprachphilosophie zur Einführung* 2011; and Staten, *Wittgenstein and Derrida*, 1985. Wittgenstein is much closer to Derrida then normally accounted for, but this remains a topic for another paper.

45 Austin, *How To Do Things With Words*, 1962.

46 Wittgenstein, *Philosophische Untersuchungen* [1953], 11th ed. 2022, § 23, 26.

Second, the concept of family resemblances expresses the impossibility of freezing the essence of language in one singled-out feature: Wittgenstein is not just saying that some phenomena resemble or overlap each other; he is saying – in a much more radical way – that there is not THE LANGUAGE in itself, and for this reason, there are also no clear boundaries for linguistic phenomena, but *only the overlapping of related phenomena*, so we cannot isolate the essence of a language without resorting to metaphysics.[47] This is the first takeaway for jurisprudence: law may not have an essence, one last particle – be it a rule, a plan, or a norm. Law can be seen as a network of overlapping legal phenomena – contracts, reflexes triggered by legal signs, adjudication, international treatises, constitutions, etc. And if so, we should not search for the essence of law but try to grasp its embeddedness in life forms instead.

Third, the rule-following issue. Wittgenstein begins by questioning why we read a signpost (*Wegweiser*) in a definite direction (for instance, reading the arrow '→' from left to right, that is, as pointing to the right).[48] The way to read this sign is not to be found in the subjective intention, nor in the sign itself, for we could imagine the possibility of someone skilled to read this same arrow '→' in the opposite direction, from right to left: "suppose what seemed the natural way of following the arrow to him [*an outsider*] was to go in the direction of the feathers and not of the point [*of the arrow*]? (We can imagine a scenario: there are no arrows in his culture, but a kind of ray gun whose discharge fans out like the feathers on our arrows)".[49] Wittgenstein holds that we cannot follow a rule just once, the same way we cannot speak any word or sentence for the very first time, for if you think of a specific rule, you will always need previous rules that establish how to follow or interpret the first rule, getting trapped in the infinite regress: "That is why 'to follow a rule' is a practice".[50] It does not convert into an infinite regress, and it is not impossible to follow rules – rule-following is but a practice.

This matter is very similar to what, in the context of Derrida's sign and language theory, has been called the 'minimal idealization' of meaning. As Wittgenstein, Derrida also criticizes traditional theories that purported to explain meaning and language as the transfer of something from one con-

47 Ibid., §§ 65-67.
48 Ibid., § 85.
49 Taylor, 'To Follow a Rule', in *Philosophical Arguments*, 1995, 165.
50 Wittgenstein, *Philosophische Untersuchungen* [1953], 11th ed. 2022, §§ 201, 202.

sciousness to another, as if meaning were a thing. As in Wittgenstein, meaning, cognition, and perception are only possible in a repetition chain (Derrida calls it '*iterability*'). And, as Wittgenstein says, the only way to make sense of a sentence, word, or sign is to contrast it with a repeated model, a pattern.[51] Both Derrida and Wittgenstein were often misread at this point. Commentators assigned to Wittgenstein a deterministic communitarian view, annihilating agency, and to Derrida, a nihilist perspective according to which no meaning is ever possible, exaggerating agency. One plausible solution to the puzzle of following rules is what Hannah Ginsborg called '*primitive normativity*': a "*normativity that does not depend on conformity to an antecedently recognized rule*".[52] Here, she is using 'rule' as norm or regulation. In the rule matrix and normativity continuum I outlined in the previous section, it gets clearer that this *primitive* normativity refers to the *implicit normativity of models, standards, and patterns*. And indeed, they do not need any prior regulation to be normative. So, implicit normativity expresses the normativity of meaning and social practices that enable us to adjust our behavior to expectations: "Profiles, patterns, expectations, and predictions all fit the same 'mechanism'; they afford anticipation".[53]

The problem here is to find the middle ground between the collective and the individual aspects, since taking part in a social practice requires both adjustment to collective requirements as well as some level of agency. It is neither deterministic nor completely free. That is the only way to escape from the teleology of social dispositions and the teleology of sovereign subjectivity. In doing so, we handle what can be called pre-reflective convictions of appropriateness and inappropriateness. When we face these collective requirements, we open up a frame for agency, and we can choose. And all this happens without returning to the reified rationality of the "*disengaged firs-person-singular self*".[54]

How does this happen? When reading Wittgenstein, one cannot help noticing two things: first, the variety of examples. Some of them are pretty intuitive, but some of them are quite unexpected. On the other hand, one notices the recurrent image of the *child*, as connected with some of these examples. And the image of the child is essential to grasp what seems to

51 Derrida, 'signature événement contexte', in *Marges*, 1972, 365-393.
52 Ginsborg, 'Primitive Normativity and Skepticism about Rules', in *The Journal of Philosophy*, vol. 108, n. 5, 2011, 233.
53 Hildebrandt, *Smart Technologies and the End(s) of Law*, 2015, 57. See also Luhmann, 'Normen in soziologischer Perspektive', in *Soziale Welt*, vol. 20, n. 1, 1969, 28-48.
54 Taylor, 'To Follow a Rule', in *Philosophical Arguments*, 1995, 169.

be the main idea of the *Philosophical Investigations*. If following a rule is a practice, that is to say, something embedded in a life form, to follow a rule requires us to master life contexts. And that is something that we can only learn through socialization:

> But whereas a dog's acquisition of a habit does not involve it in any understanding of what is meant by 'doing the same thing on the same kind of occasion', this is precisely what a human being has to understand before he can be said to have *acquired a rule*.[55]

This formulation of '*acquiring a rule*' is really insightful, for it expresses how we deal with behavior patterns, learn to deal with implicit normativity, and build expectations. At this point, we may proceed to the methodological shift we have mentioned earlier and move from philosophy to the social sciences, I mean, to sociology, anthropology, and psychology, for it is *socialization* that explains how we: i) incorporate implicit standards and behavior patterns, ii) build expectations, and iii) handle these patterns in specific situations, 'reading' the context and getting an intuitive feeling of the balance between duties, obligations, desires, and personal will, considering the available courses of action and the expectations triggered in a given situation.

Here, we must *unpack the internalization processes that cope with* "*normatively significant habits*".[56] To do so, we need to place the primary locus of the agent's understanding not in her subjective disengaged rationality, but in the practices themselves. That is precisely the turn to practices that we get from Wittgenstein's *Philosophical Investigations*. Following Charles Taylor, once we situate our understanding in the practices itself, we see how much of this understanding flows in a largely inarticulate way:

> Rather than representations being the primary locus of understanding, they are only islands in the sea of our unformulated practical grasp on the world. (...) This understanding is not, or only imperfectly, captured in our representations. It is carried in *patterns of appropriate action*, which conform to a sense of what is fitting and right. Agents with this kind of understanding recognize when they or others have put a foot wrong.[57]

55 Winch, *The Idea of a Social Science and its Relation to Philosophy*, 1958, 5.
56 Delacroix, *Habitual Ethics*, 2022, 24.
57 Taylor, 'To Follow a Rule', in *Philosophical Arguments*, 1995, 170/171 – my highlight.

Here, we exit philosophy, strictly speaking, and move to the social sciences, for "philosophy is concerned with eliminating linguistic confusions,"[58] which means, philosophy strives for clear boundaries between concepts (routine and rule, habit and agency and so on) – but we are dealing precisely with an inarticulate phenomenon whose key feature is not to have such precise contours. At this point, Charles Taylor moves to Bourdieu's notion of '*habitus*', which aims to capture this level of inarticulate social understanding. Nonetheless, Bourdieu's notion of habitus may not be the best option, for it became, through the years, closer and closer to rigid concepts like social fields and classes, becoming more dispositional and structural than before. Eventually, Bourdieu defined *habitus* this way:

> The constraints associated with a particular class of *conditions of existence* produce sets of habitus, systems of durable and transposable dispositions, structured structures predisposed to function as structuring structures, i.e., as the generating and organizing principles of practices and representations that can be objectively adapted to their purpose without presupposing the conscious aiming of ends and the express mastery of the operations necessary to achieve them.[59]

We see that Bourdieu derives the habitus from the '*conditions of existence*', impregnating this concept with deterministic assumptions. Habitus should mean the set of inculcated, pre-reflective dispositions that contextual affordances trigger for the subject, so she or he can act. In this definition, it should erase the boundaries of context and agent, and works according to 4E cognition. But as '*a system of dispositions derived from the existence conditions*' (knowing what the 'existence conditions' mean in Marxist terminology), Bourdieu's definition becomes the expression of an exogenous principle and reinstantiates causality and teleology.

The implicit normativity of practices never has this deterministic overload; it always leaves room for evaluation, so the agent can indeed choose to deviate and break expectations. As Sylvie Delacroix puts it: "This internalisation process not only entails that the performance becomes effortless; it also means we become prone to criticising deviation from those expectations. But is it also compatible with a capacity to change or deviate from that practice ourselves?" She goes on to develop that the internalization of behavior patterns takes place by providing us with senses of primitive

58 Winch, *The Idea of a Social Science and its Relation to Philosophy*, 1958, 5.
59 Bourdieu, *Le sens pratique*, 1980, 88 – my highlight.

appropriateness as well as with primitive *inappropriateness* when agents can evaluate the context without resorting back to the model of practical reasoning, that is, without becoming a '*disengaged firs-person-singular self*'. This is what she designates as a '*pre-reflective ethical intelligence*'.[60]

Many approaches have been addressing the issue of making pre-reflective decisions, such as the naturalistic decision-making studies or the heuristic and bias stance. Perhaps the most encompassing alternative would be to enlarge the habitus concept, eliminating the deterministic overload. As a matter of fact, the concept of *habitus*, as used by Norbert Elias, Marcel Mauss, and Bruno Latour, offers a promising perspective because these authors allow us to grasp how the *habitus* places itself between nature and culture, education and imitation, reflex and free will, technology and context, agent and society. At this point, we can only give general hints on this matter.[61]

Marcel Mauss, for instance, noticed what he called body techniques – the inculcation of body gestures and routines that could be learned but also voluntarily acquired, even by watching movies.[62] The technological aspect of habitus is paramount. Latour builds on Mauss' concept of habitus and goes on to advance the tech-inspired concept of *plug-in*: plug-ins are a kind of software that we 'have' in ourselves thanks to socialization, and that help us make sense of situations, almost as an 'app' for identifying affordances.[63] Plug-ins are skilled competencies that you activate in specific circumstances to render the context readable and to orient yourself. It is nothing like the disengaged rationality of practical reasoning because they are part of an *extended* cognition:

> The crucial point is that you are sustaining this mental and cognitive competence as long as you subscribe to this equipment. You don't carry it with you; it is not your own property. (…) Cognitive abilities do not reside in 'you' but are distributed throughout the formatted setting, which is not only made of localizers but also of many competence-building

60 Delacroix, *Habitual Ethics*, 2022, 29.

61 As already mentioned, this paper is a *work in progress*, and a broader concept of *habitus* still demand further development.

62 Mauss, *Sociologie et anthropologie*, 1950. This concept of 'body techniques' would be of great value to analyze digital sociability in short videos platforms, for instance.

63 Latour, *Reassembling the Social*, 2005, 209 ff.

> propositions, of many small intellectual technologies. This propagation is key to the field of distributed cognition.[64]

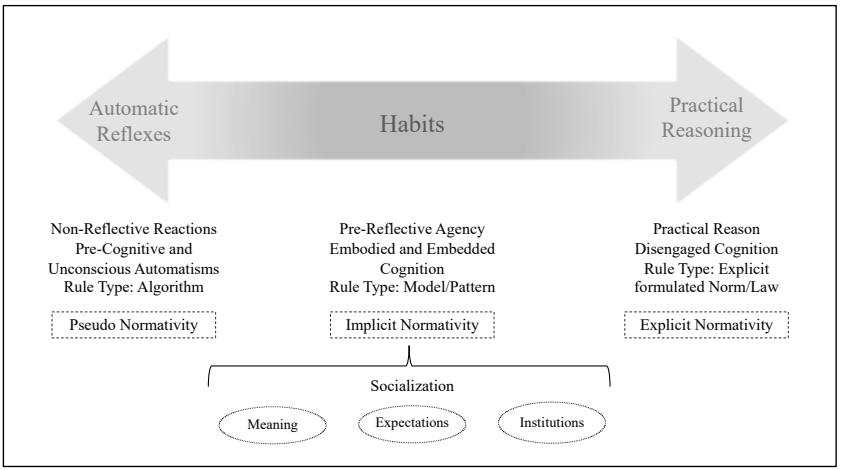
This way of observing skilled competencies requires us to rethink the boundaries of sociology and psychology. People develop mechanisms to read context affordances and behave accordingly, not only to comply (when they have a sense of appropriateness) but also to break with expectations (when they have a feeling of inappropriateness). For this reason, we can never take the individual/society dichotomy as legal positivists took the fact/value dichotomy. Following Elias, perhaps the only classic sociologist that included the *child* in his theoretical considerations, we need to erase these boundaries and see the individual as an open process, one that does not have a finish line to cross, and moreover, as a collective one, for the habitus depends not only on you and the context but also on everyone else that shares the context with you. Elias sees clearly that there is a continuity between the personality layers of the individual and the social institutions that surround the individual, and prompts us to think of society as a set of figurative formations: society is not built out of given entities like 'state' or 'social class', but out of mobile parts that, depending on the articulation, shape the meaning of each other.[65] And the key concept that links personality and society, psychology and sociology, normativity and affordances, is *anticipation* (however general it may remain):

> When we, human being, navigate our *Welt*, we are aware that others are profiling us, while we are profiling them. We develop mechanisms, institutions, norms and cultural patterns that enable us to anticipate what is expected from us.[66]

As we see, there is a kind of 'division of labor' between sociology and psychology, for they both address how people recognize *implicit normative patterns* and *inarticulate expectations* in order to know how to act (complying or deviant, meeting or frustrating expectations) – and all this without presupposing a 'basic norm' or a 'rule of recognition', not even calculating the chances to be somehow reprehended or punished by any authority. This implicit normativity takes place alongside the normativity of meaning and social figurations – it is a pulse, not a metaphysical entity inhabiting rules, norms, or 'the legal system'. That is why this normativity

64 Ibid., 210/211.
65 Elias, *Was ist Soziologie?* 1970.
66 Hildebrandt, *Smart Technologies and the End(s) of Law*, 2015, 58.

must be learned and acquired, and that is why rule-following is a practice. And that is also why we cannot isolate law completely from language and society. The 'impure' character of law must be reflected in an 'impure' – or multidisciplinary – jurisprudence. Legal theory should start with habits and implicit normativity to get a fresh look at its past achievements and troubles. The question is not to pass from habits to norms in the traditional sense but to understand that the strict entanglement of norms and practical reason is not enough anymore, especially if we consider the new challenges posed by the technological age. Before we close this paper, the last step in our normativity spectrum can be expressed in the following figure:



As we can see, the spectrum of normativity allows us to distinguish three normativity regimes: automatic reflexes, habits, and practical reasoning. The diffusion of algorithmic tools in the absence of legal regulation allowed the diagnosis that code became law. But code is never going to replace law:

> In short, law is regulation. But the reverse is not equally true: Not all regulation is law. Nor should it be. Law is the normative ultima ratio used by a society to govern conflicts or to allocate goods according to general rules. Thus, a vital part of the liberal concept of law in the philosophical

> tradition of Western Enlightenment is its design in the form of general rules.[67]

When Möllers says that algorithms exclude normativity, he is comparing two different phenomena: the pseudo normativity of algorithms and the explicit normativity of general rules. The challenged posed by new technologies to legal philosophy is that this pseudo normativity is much more efficient than the explicit normativity, because it gets inculcated in our behavior. It is not a question of compliance, but a question of affordance – people do not 'comply' with an algorithm; people use it. Jurisprudence has developed its conceptual framework exclusively for the explicit normativity. Grasping new modes of normativity may be the first step to renew legal theory.

E. Concluding Remarks

Möllers does not differentiate levels of normativity, as I did in the continuum proposed in this paper, and he has only the normativity of practical reason in mind. As we haveve already argued, not all normative phenomena are alike.[68] And that is perhaps why he comes to the awkward conclusion that digital technology should program casualty, and "Interventions in programming would have to be made practically possible for all parties involved".[69] It is not imaginable, however, how such a Habermasian requirement should ever be met in artificial intelligence industry. Can we imagine a democratic forum where '*all parties involved*' discuss the algorithms used in the recommendation systems of Twitter, Instagram or TikTok? But Möllers has a point, he expresses a familiar feeling: a technology-driven society will eventually lead us to a Black-Mirror dystopia with no room for individual agency.

This diagnosis mixes two different kinds of normativity, the two extremes of our spectrum, as we saw. It is important to make a distinction between '*regulatory power*' and '*regulation*': regulatory power (or 'code-driven normativity') relates to the kind of *pseudo normativity* we find in algorithmic

67 Auer, 'Granular Norms and the Concept of Law: A Critique', in *Algorithmic Regulation and Personalized Law: A Handbook*, 2021, 149.

68 Schmidt & Rakoczy, 'Developing an Understanding of Normativity', in *The Oxford Handbook of 4E Cognition*, 686.

69 Ibid., 455/456.

environments when we react by unconscious automatisms to get to use technology; regulation, on the other hand, express what we designated by *explicit normativity*.[70] The former relates to 'code-driven law', and the latter to 'text-driven law'.[71] Algorithms constrain our conduct, but do not regulate it properly, for they prompt us to act like someone that uses a bridge to cross a river. Regulation, on the other hand, may have algorithms as its target. In a way, the code will never be the law: the pseudo normativity of unavoidable algorithms perceived as affordances by users of digital technologies will never replace the explicit normativity of practical reason, because they run on different tracks. They are different phenomena. So, normativity is not simply vanishing, as Möllers supposes.

On the other hand, we can never deny that big data analytics and artificial intelligence are increasingly pervasive and that we can indeed be affected by invisible classifications and automated inferences that we can hardly contest and challenge. When it comes to automated legal decision-making, we have 'automated inferences'[72] that are built upon types and classifications. The risks can be analyzed in three dimensions: temporal, social, and material.

i) *Temporal* dimension: Big data analytics and artificial intelligence systems resemble legislation and adjudication in a specific way: they generate classifications and typify people according to these pre-determined categories, attaching consequences for this classification (bigger recidivism risks, higher interests or prices and so on). But there is no gap between the modeling of systems of automated inferences and they being put to use. If parliaments in liberal democracies must first approve a bill (normally after rounds and rounds of discussion), and only then this bill becomes effective, coded categories and types are developed and put into use. So, if big data says that immigrants in poor neighborhoods run higher risks of recidivism (because big data learns from the past and the past may not be the best key to interpret the future), code will reinforce inequalities. The parliamentary process allows society to discuss effects of a bill draft,

70 Delacroix, 'Beware of Algorithmic Regulation', in: *SSRN Papers*, 2019; Hildebrandt, 'Code-Driven Law: Freezing the Future and Scaling the Past', in *Is Law Computable? Critical Perspectives on Law and Artificial Intelligence*, 2020.

71 Hildebrandt, 'Code-Driven Law: Freezing the Future and Scaling the Past', in *Is Law Computable? Critical Perspectives on Law and Artificial Intelligence*, 2020.

72 Hildebrandt, 'The Artificial Intelligence of European Union Law', in: *German Law Journal*, vol. 21, 2020, 74.

and even if we cannot anticipate all possible effects, it is much better than having no clue at all.

ii) *Social* dimension: If the decision takes no time, we have not the opportunity to build expectations. While institutional decisions depend on a legal procedure, and the procedure enables all participants to re-structure their expectations and adjust them to a decision yet unknown (you may win or lose a lawsuit, but the intermediary decisions of the procedure will give you hints to what you can expect)[73], this temporal distention is not available in automated decision-making, so we cannot expect certain decisions. In institutional processes, we can observe how the other parts are behaving, and adjust our own behavior. This cannot happen in automated decisions. We may be subject to a decision (for instance, cuts in welfare benefits due to fraud suspicions) that we simply could not anticipate at all.

iii) *Material* dimension: There is no established due process to contest and challenge the merit and motives of automated decisions. Democratic decisions are discussed in their aims, costs, causes and effects. Automated decisions may be put in motion for reasons of efficiency and reducing costs, without providing a due process for contestation.

These differences express the change from a text-driven to a code-driven law: in the former, the building of general categories, the interpretation of concrete situations in which these categories apply, and the decision-making itself take time, require motivation, and can be publicly contested. In the latter, all these operations are condensed in time and invisible to society. The question, then, is how to lay down explicit regulation for digital platforms when they provide services that run 'under the radar' on the level of pseudo normativity.

New regulation strategies have been trying new mechanisms and tools to reverse the information asymmetry and better understand the new digital platforms. And the main obstacle may be in our thinking of regulation again according to the model of explicit normativity. At the heart of explicit normativity is the paradigm of criminal law when you punish deviant conduct with a sanction. Bentham inaugurated legal positivism discussing criminal policy and incarceration. This paradigm is not enough anymore for new regulation challenges, because big data analytics and artificial intelligence run with *inferences* – outputs of a process whose inputs are

73 Luhmann, *Legitimation durch Verfahren*, 1969.

unknown and indeterminable. Let us take, for instance, the NetzDG in Germany or the new regulation package in the European Union (the Digital Services Act and the Digital Markets Act). These initiatives focus on collective patterns (not on individual conduct) to establish disclosure and negotiation procedures, moving from discrete harms to systemic threats and measures.[74] But they move away from attaching a sanction to a previously given behavior. These new strategies are still under development, and a clear glance at the different normativity modes can help us in this challenging task.

74 See Eifert et al., 'Taming the Giants: The DMA/DSA Package', in *Common Market Law Review*, vol. 58, 2021, 987-1028, and Cohen, *Between Truth and Power*, 2019, 182; Auer, 'Granular Norms and the Concept of Law: A Critique', in *Algorithmic Regulation and Personalized Law: A Handbook*, 2021.

A Necessary Cognitive Turn in Digital Constitutionalism: Regulated Self-Regulation as a Regulatory Mechanism for Artificial Intelligence (AI) in Comparative Law

Ricardo Campos

Abstract: This paper argues that the debate on digital constitutionalism suffers from a deficit in the cognitive dimension of knowledge generation, focusing predominantly on normative principles and values while neglecting the significant challenge of law's capacity to generate knowledge for its own application. To address this gap, the paper examines regulated self-regulation as an effective mechanism for regulating artificial intelligence (AI) in both European and Brazilian legal contexts. The introduction outlines the growing impact of AI on citizens' rights and emphasizes the need for regulatory frameworks that balance innovation with public interest protections. The first section critiques the theoretical and practical limitations of digital constitutionalism in managing the challenges posed by AI. The subsequent section analyses how regulated self-regulation can bridge the divide between state regulation and self-regulation, using the European General Data Protection Regulation (GDPR) and Brazil's General Data Protection Law (LGPD) as case studies. In conclusion, the paper underscores the potential of regulated self-regulation to promote ethical AI development, safeguard fundamental rights, and foster innovation through adaptive governance and stakeholder collaboration, particularly by enhancing the generation of legal knowledge required for effective law enforcement.

A. Introduction

Artificial intelligence is increasingly becoming part of our daily lives. As the technology advances and gains more popularity, concerns are being raised about its impact on citizens' rights, encompassing ethical, legal, and socioeconomic questions. In recent years, efforts have been made to strike a proper balance between technological innovation and the protection of public interests and individual rights, which is reflected in a variety of regulatory approaches.

It is extremely challenging to reach a consensus that addresses the different legal perspectives associated with adopting universally applicable AI regulations. Nonetheless, certain regulatory initiatives, such as UNESCO's[1] and OECD's[2] recommendations for the development and use of technology, seem to be moving in this direction: although there are differences in content and in the form of implementation of the guidelines, respect for privacy and the protection of personal data, the need for accountability systems, and the requirements of security, transparency, explainability, and non-discrimination appear to form a common thread across various regulatory instruments[3].

The issue, however, is that these documents, while symbolizing an universal goodwill towards regulating AI, contain general and voluntary principles and obligations, which rightfully face criticism for neglecting the economic and political interests driving the current gold rush. As a result, many nation-states are also attempting to organize their own internal structures and norms according to their specific social, economic, and political characteristics, either by establishing "mere" ethical principles to guide AI development or by setting more robust and stringent rules.

The European Union, for example, has sought to develop a regulatory approach that fosters the introduction of AI while addressing its associated risks. This involves a legal framework aimed at creating an ecosystem of trust between companies and consumers while also accelerating the adoption of technology in Europe. To this end, the EU faced the challenge of defining AI in a way that is flexible enough to accommodate the technology's dynamic nature, while effectively applying a risk-based approach that considers its advantages without over-regulating it. The proposed regulation on AI – known as "AI Act" – was published in 2021[4].

---

1 Unesco, *Recommendation on the Ethics of Artificial Intelligence*, Adopted at the 41st session of the UNESCO General Conference, November 23, 2021. Accessed on October 23, 2024. https://www.unesco.org/en/articles/recommendation-ethics-artificial-intelligence.

2 OECD, *Recommendation of the Council on Artificial Intelligence*, Adopted by the OECD Council on May 22, 2019. Accessed on October 23, 2024. https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449.

3 See, in general, Floridi, L., *The ethics of artificial intelligence: principles, challenges, and opportunities*. New York, 2023, p. 57 ff.

4 This has led to various criticisms of regulation in a scenario of uncertainty amidst a new industrial revolution. For the negative impacts on the European economy, see Mario Draghi, *The Future of European Competitiveness*, 09.2024.

Unlike in the EU, regulations in the United States are generally developed in a decentralized and vertical manner at the level of individual states and sectors[5].The former US President, Joe Biden, intended to change this trend by issuing an order titled "Executive Order on the Safe and Trustworthy Development and Use of Artificial Intelligence"[6], which establishes a series of voluntary commitments that must be fulfilled by companies wishing to develop and deploy this technology in the country. However, the Executive Order has been recently revoked by Donald Trump[7].

Another example that must not be overlooked is China's[8], the country with the most stringent regulations in this area, with specific laws on issues such as algorithmic recommendations and deep manipulation of content. In contrast to the European and (the previous) American approaches, the Chinese strategy involves strong state intervention as a differentiating factor[9], which firstly promotes the strengthening of the domestic market and secondly leads to a hegemonic position in the global development of tech-

5 Williams, A. *What Could Horizontal AI Legislation Look Like In the US? Exploring the US Algorithmic Accountability Act*. In: HolisticAI Blog, January 9, 2023. Available online at: https://www.holisticai.com/blog/us-algorithmic-accountability-act, last accessed: May 7, 2024. For a comparative perspective between the American and European approaches, see: Mökander, J. et al. *The US Algorithmic Accountability Act of 2022 vs. The EU Artificial Intelligence Act: What Can They Learn from Each Other?* In: Minds and Machines, Vol. 32, No. 4, pp. 751–758, December 1, 2022.

6 U.S. White House. *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*. October 30, 2023. Available online at: https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/, last accessed: October 9, 2024.

7 Reuters, "Trump revokes Biden executive order addressing AI risks," 2025. Accessed on February 6, 2025: https://www.reuters.com/technology/artificial-intelligence/trump-revokes-biden-executive-order-addressing-ai-risks-2025-01-21/.

8 For a general overview of China's regulatory context, see: Roberts, Huw et al. *The Chinese Approach to Artificial Intelligence: An Analysis of Policy, Ethics, and Regulation*. In: *Ethics, Governance, and Policies in Artificial Intelligence*. Philosophical Studies Series, Vol. 144, Springer, 2021, pp. 47–79. Available online at: https://link.springer.com/chapter/10.1007/978-3-030-81907-1_5, last accessed on: October 9, 2024.

9 For comparative approaches between China's regulatory context and the respective American and European contexts, see: Hine, Emmie; Floridi, Luciano. *Artificial Intelligence with American Values and Chinese Characteristics: A Comparative Analysis of American and Chinese Governmental AI Policies*. In: *AI & Society*, Vol. 39, pp. 257–278, 2024. Available online at: https://link.springer.com/article/10.1007/s00146-022-01499-8, last accessed on: October 9, 2024; and Dixon, Ren Bin Lee. *Artificial Intelligence Governance: A Comparative Analysis of China, the European Union, and the United States*. Master's thesis, May 2022.

nology. The Chinese strategy involves a close alignment between the state and the country's leading AI companies, which brings us to an interesting point in the discussion about regulating this technology. According to a report by the Washington Post, during their first meeting with companies regarding algorithm regulation, state representatives showed "little understanding of the technical details," which prompted company representatives to use a combination of metaphors and simplified language to address the topic. This highlights that, from an innovation perspective, relying solely on the state apparatus to establish standards and development guidelines for AI (and other emerging technologies) can have negative consequences.

In this regard, it should be noted that in the current context of the increasing *algorithmization* of human life, the law, as a fundamental part of the normative structure of society, is now facing pressures it had not encountered until relatively recently. The recent introduction of legal regulations for the protection of personal data worldwide is an excellent example that clearly illustrates how one of the functions of modern law is to align normative (legal) levels with new technologies.[10]

This is because technological revolutions are always intertwined with the current intellectual, social, political, and economic context, deeply integrated into these aspects, and have collateral effects. Technological revolutions lead to the deconstruction of previously established concepts, paradigms, structures, and identities, contributing to their critical reassessment in light of the new stage of technological and societal development.[11] The sociologist Niklas Luhmann had already expressed theoretical doubts in the 1990s about the future development of law in a society shaped by an emerging technological revolution[12]. His works reflect a search for understanding a society that increasingly focuses on new technologies and their cross-border impacts, for which the traditional mechanisms of law and

10 V. Descombes, *Die Rätsel der Identität*, Berlin 2013, pp. 226 ff; T. Vesting, *Gentleman, Manager, Homo Digitalis. Der Wandel der Rechtssubjektivität in der Moderne*, Weilerswist 2021.

11 M. Beloy, *Post-humaner Konstitutionalismus? Eine kritische Verteidigung der anthropozentrischen und humanistischen Traditionen in der algorithmischen Gesellschaft*, in: M. Beloy (ed.), *The IT Revolution and its Impact on State, Constitutionalism and Public Law*, Oxford 2021.

12 In this regard, see, among other works, Luhmann, N, *Die Politik der Gesellschaft*, Frankfurt am Main, 2002, p. 220.

politics, centred around the nation-state, can no longer play the same role as before[13].

The connection between law and the protection of the individual (and their fundamental rights and prerogatives) therefore seems to be a more complex challenge than it was when the structuring of social norms was centred on the state as a regulator. Particularly with the emergence of new computer, information, and communication technologies, the normative structures that shape the exercise of rights can no longer be influenced or enabled solely by state actions. It is no exaggeration to say that "a state-centred view of lawmaking has become unrealistic and insufficient"[14]. This is especially true since digitalization has led to an increase in the asymmetry of knowledge between the regulatory state and private society. Increasingly, knowledge resides in private society and the great challenge for the state becomes how to create institutionalized procedures to generate knowledge for the application of the law.

In this way, new normative constructions tend to structure the scope of action for individuals, companies, and the State based on the modelling of the environment itself and the design of the business model that underlies the development of these new technologies. This, incidentally, represents the modern character of law: it deals with an indefinite and indeterminable complexity of factors, but is also a driving force for the construction of new and complex social relationships[15].

Although a number of scholars and legal practitioners have turned to the so-called "digital constitutionalism" as a legal theory capable of addressing the issues arising from the digitalization of society, I will argue in this paper that the concept is somewhat insufficient. This is because new forms of knowledge production in the digital society require actions that go beyond traditional state intervention, while also avoiding exclusive reliance on the self-regulation proposed by private actors. In this regard, I will seek to analyse how regulated self-regulation emerges as a suitable approach to guide the creation (or adaptation) of rights in response to the challenges of the digital era.

13 Luhmann, N., *Die Wirtschaft der Gesellschaft*, Frankfurt am Main, 1994, p. 170 ff.; Luhmann, N., *Die Gesellschaft der Gesellschaft*, Frankfurt am Main, 1997, p. 166 ff.

14 T. M. Hahn, *Código de conduta. Autorregulação na Lei Geral de Proteção de Dados Pessoais: conceitos, controles e projeções*, 2024, in press, p. 15.

15 R. Campos, *Metamorfoses do Direito Global: Sobre a Interação Entre Direito, Tempo e Tecnologia*, São Paulo, 2022.

B. Theoretical and practical shortcomings of digital constitutionalism

The recent reflections on what has been called *digital constitutionalism* emerge within a political, social, and economic context heavily shaped by the concept of the "Platform Society"[16]. In light of the inefficacy in applying existing regulatory frameworks and the absence of specific legal provisions for innovative practices, digital platforms have branched out without being fully subjected to the legal and social responsibilities regarding how these environments are structured and how the exercise of power within them can be limited[17]. Within this landscape, digital constitutionalism is broadly viewed as a concept employed by theories that seek to provide interpretative frameworks for public, private, and hybrid actions, with the goal of mitigating the concentration of economic and political power by these actors.

The disruptive impact of digital technologies is acting as a catalyst for a "new constitutional moment"[18] by challenging existing legal, political, and social norms. In response, societies must adapt their constitutional frameworks to accommodate the changes brought about by the digital age, resulting in potential shifts in fundamental rights and governance structures. These changes lead to an alteration of what is commonly called "constitutional balance," which would be an ideal condition produced by the application of constitutional law norms in a given legal order[19]. In other words, by affecting the protection of fundamental rights and the balance of powers, new technologies (especially digital platforms) would have promoted a disturbance of this balance, which in turn would have triggered the so-called "normative counteractions" as a response, with the purpose of restoring the previous state[20].

---

16 J. van Dijck, D. Nieborg, T. Poell, *Reframing platform power*, in: Internet Policy Review, Vol. 8, No. 2, 2019, pp. 1-18, p. 2.

17 N. P. Suzor, Digital Constitutionalism: Using the Rule of Law to Evaluate the Legitimacy of Governance by Platforms, in: Social Media + Society, Vol. 4, No. 3, 2018, pp. 1-11, p. 2.

18 "Contemporary society is experiencing a new constitutional moment, whose main catalyst is the disruptive impact of digital technology". E. Celeste. Digital Constitutionalism: a new systematic theorization. Internet Review of Law, Computers & Technology, v. 33, n. 1, p. 77.

19 Celeste, Edoardo. Digital Constitutionalism: a new systematic theorization, fn. 18.

20 Celeste, Edoardo. Terms of service and bills of rights: new mechanisms of constitutionalisation in the social media environment? Internet Review of Law, Computers & Technology, v. 33, n. 2, p. 133.

These counter-actions would consist in initiatives of integration or amendments to the existing normative framework[21], and could arguably be guided by *digital constitutionalism*, a concept that represents a set of values and principles that permeate, inform and guide the process of constitutionalization of the digital environment[22]. For digital constitutionalism, the reactions to the disturbances that new technologies have brought to the "constitutional balance" should be based on already existing constitutional principles, in a polycentric process – which has been commonly called "constitutionalization" – that may involve different instruments, either within the dimension of the States (such as legislations and decisions of constitutional courts) or outside the States (example of Internet charters of rights, even if they are not binding) [23].

For certain scholars, digital constitutionalism may manifest through advanced regulatory models. Giovanni de Gregorio, for instance, in discussing recent regulatory initiatives, identifies this manifestation within the European Union, specifically referring to the European Digital Services Act as a "reaction to new digital powers" following a period in which, in his view, the regulation of the bloc had neglected and overlooked the role of constitutionalism and constitutional law in safeguarding fundamental rights and in limiting the growth and consolidation of unaccountable powers that abuse constitutional values.[24] Another expression of digital constitutionalism — highlighting the flexibility of the concept[25] — is its connection to institutional initiatives in the realm of self-regulation. A possible example, framed within the theoretical structure provided by digital

21 "[T]hese counteractions consist in the integration or in the amendment of the existing normative framework and aim to restore a condition of relative equilibrium in the constitutional system". Celeste, Edoardo. Digital Constitutionalism: a new systematic theorization, fn. 10.

22 "[It] represents the set of values and ideals that permeate, inform and guide the process of constitutionalisation of the digital environment". Celeste, E. Digital Constitutionalism: a new systematic theorization. Internet Review of Law, Computers & Technology, v. 33, n. 1, p. 90.

23 E. Celeste, What is digital constitutionalism?, in: The Digital Constitutionalist, available at: https://digi-con.org/what-is-digital-constitutionalism/.

24 G. de Gregorio, Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society, Cambridge 2022, p. 3.

25 J. R. G. Pereira, C. I. Keller, Constitucionalismo Digital: contradições de um conceito impreciso, in: Revista Direito e Práxis, Vol. 13, No. 4, Dezember 2022, pp. 2648–2689, p. 2674, available at: https://doi.org/10.1590/2179-8966/2022/70887.

constitutionalism[26], is the Facebook Oversight Board, created by Meta in 2019 to serve as a secondary instance for reviewing content moderation decisions made on the platform.

Specifically in the Brazilian context, Saavedra and Borges argue that Brazil currently experiences a phase of digital constitutionalism[27]. This inclination toward the ideology is evidenced, first and foremost, by the broad debates surrounding internet legislation, most notably the Marco Civil da Internet (MCI), which saw significant public participation—an unprecedented occurrence at the time. There is also a growing concern for established constitutional rights, such as privacy and intimacy. Moreover, fundamental principles such as net neutrality and informational self-determination would be likewise protected, reflecting a clear trend in the country toward digital constitutionalism. In further examining the Brazilian scenario, Mendes and Ferreira suggest that, within state structures, "the principles and values of digital constitutionalism can serve as normative standards for the judicial review of internet-related legislation"[28]. According to the authors, digital constitutionalism would influence, through judicialization, the redefinition of "the essence of fundamental constitutional rights related to freedom of expression, protection of honour, and privacy" in the face of the current technological landscape[29].

Regarding the concept itself[30], Suzor conceives digital constitutionalism as a project aimed at articulating and establishing standards and legitimacy for governance in the digital age, which involves assessing the internal governance mechanisms of private platforms in light of "the principles

26 M. Miloš, T. Pelić, Constitutional Reasoning There and Back Again: The Facebook Oversight Board as a Source of Transnational Constitutional Advice, in: J. de Poorter et al. (Ed.), European Yearbook of Constitutional Law 2021: Constitutional Advice, Vol. 3, The Hague 2022, pp. 197-223.

27 G. A. Saavedra, G. O. A. Borges, Constitucionalismo Digital Brasileiro, in: Revista da AJURIS, Vol. 49, No. 152, Oktober 2022, pp. 157–180, available at: http://revistadaajuris.ajuris.org.br/index.php/REVAJURIS/article/view/1228.

28 G. Ferreira Mendes, V. Oliveira Fernandes, Constitucionalismo Digital e Jurisdição Constitucional: uma agenda de pesquisa para o caso brasileiro, in: Revista Justiça Do Direito, Vol. 34, No. 2, 2020, pp. 6-51, p. 3, available at: https://doi.org/10.5335/rjd.v34i2.11038.

29 G. Ferreira Mendes, V. Oliveira Fernandes, Constitucionalismo Digital e Jurisdição Constitucional, fn. 28.

30 Para uma visão geral sobre como diferentes autores abordam o conceito de constitucinalismo digital, cf. E. Celeste, Digital Constitutionalism: A New Systematic Theorisation, in: International Review of Law, Computers & Technology, Vol. 33, No. 1, Januar 2019, pp. 76–99, available at: https://doi.org/10.1080/13600869.2019.1562604.

of the Rule of Law" [31]. Celeste, in turn, views digital constitutionalism as a variation of modern constitutionalism, which demands the creation of normative countermeasures to address the shifts in constitutional balance brought about by the advent of digital technology, while also providing the ideals, values, and principles that guide such countermeasures[32]. In this sense, digital constitutionalism represents a "set of values and principles that influence, guide, and underpin the process of constitutionalizing the digital environment"[33]. Alternatively, the concept can be seen as "a useful shorthand to denote the theoretical strand that advocates for the translation of the core values of constitutionalism in the context of the digital society"[34].

Pereira and Keller identify two categories of issues related to the limitations and possibilities of the concept of digital constitutionalism. The first concerns the explanatory value and normative appropriateness of expanding the concept of a constitution to include legal forms that, in many respects, differ from those that shaped constitutionalism as established by modern political theory; the second relates to the risks and implications associated with broadening the concept of constitutionalism, as well as the recent uses of the category of digital constitutionalism[35]. A similar critique can be found in Trindade and Antonelo, who argue that the concept of digital constitutionalism—in a broad and superficial sense—serves merely as a "crutch" for the process of constitutionalizing the digital environment[36]. According to these authors, the concept is a dispensable support, like an accessory, as it adds nothing new, conceptually or substantively, to the idea of constitutionalism, particularly contemporary constitutionalism, and thus

31 N. P. Suzor, Digital Constitutionalism: Using the Rule of Law to Evaluate the Legitimacy of Governance by Platforms (Fn. 9), p. 2.

32 E. Celeste, Constitucionalismo digital: mapeando a resposta constitucional aos desafios da tecnologia digital, in: Revista Brasileira de Direitos Fundamentais & Justiça, Vol. 15, No. 45, 2021, pp. 63–91, p. 81.

33 E. Celeste, Constitucionalismo digital: mapeando a resposta constitucional aos desafios da tecnologia digital, fn. 33.

34 E. Celeste, Constitutionalism in the Digital Age, in: J. Pohle et al. (Ed..), Liber Amicorum for Ingolf Pernice, HIIG Book Series, 2020.

35 R. G. Pereira, C. I. Keller, Constitucionalismo Digital: contradições de um conceito impreciso (Fn. 24), p. 2676.

36 A. Trindade, A. Antonelo, Constitucionalismo digital: um convidado (in)esperado, in: Revista Brasileira de Direito, Vol. 18, No. 1, 2023, p. 13, available at: https://doi.org/10.18256/2238-0604.2022.v18i1.4816.

cannot justify the creation of a specific or segmented form of constitutionalism[37].

Even if one were to accept the concept of digital constitutionalism as a normative model or legal theory, or to endorse a possible "reconciliation" of the various conceptualizations of the ideology in question[38], at least one more critique can be raised regarding the use of digital constitutionalism as a theory capable of solving the problems arising from digitalization. In summary, digital constitutionalism seeks to expand the normative structure of traditional constitutionalism by aligning its values and principles with the rapidly changing digital environment of modern society. However, this approach exposes an inherent limitation, particularly in confronting a defining aspect of the digital era: the increasing prevalence of the cognitive dimension over the normative one[39]. Amidst this ongoing transformation, the legal framework itself is undergoing substantial changes, rendering it insufficient to rely solely on the values and principles of conventional constitutionalism. In other words, it is necessary to go beyond merely appealing to principles, aiming to reconcile the new forms of knowledge generation in the platform society with effective and efficient ways of translating these principles into practical applications[40]. As will be discussed in the following sections of this paper, one possible solution is the establishment of regulated self-regulation within the context of new digital technologies.

C. Self-Regulation Based on Experiences with the Protection of Personal Data

I. Regulated self-regulation as a mean of knowledge generation

One of the most efficient ways to enhance the new ways of knowledge generation is through regulated self-regulation. Self-regulation, which emerged

37 A. Trindade, A. Antonelo, Constitucionalismo digital: um convidado (in)esperado,fn. 36.

38 E. Celeste. "Digital Constitutionalism: A New Systematic Theorisation", fn. 18..

39 I. Augsberg, *Informationsverwaltungsrecht: Zur kognitiven Dimension der rechtlichen Steuerung von Verwaltungsentscheidungen*, 2014; R. Campos, *Metamorfoses do Direito Global, fn. 15.*

40 I. Augsberg, *Informationsverwaltungsrecht: Zur kognitiven Dimension der rechtlichen Steuerung von Verwaltungsentscheidungen*, fn. 39; R. Campos, *Metamorfoses do Direito Global, fn. 15.*

in the context of the crisis of traditional State regulation due to increasing societal complexity combined with the absorption of State functions by private activities, aimed to connect two dimensions of society: public objectives oriented towards the public interest, and sectoral knowledge from private entities for the implementation of these objectives.[41] As constitutional lawyer Dieter Grimm explains, this new institution of administrative law, situated at the intersection of procedural dimensions, state law, and social complexity, represents the most advanced form of proceduralization[42]. It is a more efficient form of regulation that essentially relies on the collaboration between the regulating state and the actors or societal sectors being regulated.[43]

Perhaps one of the institutions that best illustrates how regulated self-regulation enables the impacts of technology to be addressed through legal norms is the right to the protection of personal data, which will serve as the foundation for the discussion in this essay. We will then analyse self-regulation in the regulatory standards for AI in Europe and Brazil and compare the two approaches.

41 A. Voßkuhle, *Regulierte Selbstregulierung – Zur Karriere eines Schlüsselbegriffs*, in: *Regulierte Selbstregulierung als Steuerungskonzept des Gewährleistungsstaates: Ergebnisse des Symposiums aus Anlaß des 60. Geburtstages von Wolfgang Hoffmann-Riem*, Die Verwaltung Beiheft 4 (2001), p. 197.

42 The model of proceduralization, understood here as the third legal paradigm, differs in terms of the conditions for the production and reproduction of legal normativity in modern society from previous models of state centrality and balancing: "It differs, on the one hand, from the legacy of *quod omnes tangit* in that it does not (solely) concentrate the structures for the production and reproduction of legal normativity within the unity of a national political system. On the other hand, compared to the balancing paradigm, the model of proceduralization does not reduce the conditions for the reproduction of legal normativity to the collision of abstract principles to be resolved within the framework of constitutional adjudication. [...] Proceduralization specifically arises from the bankruptcy, or rather the insufficiency, of the two preceding models, as it incorporates the premises of both paradigms, namely the centrality of the state (*quod omnes tangit*) and the materialization of law in abstract principles mediated by constitutional adjudication (balancing)." G. Abboud; Campos, R., *A Autorregulação Regulada Como Modelo do Direito Proceduralizado*. In: G. Abboud; N. Júnior; R. Campos (Ed.): *Fake News e Regulação*, São Paulo, 2022. For more on this, see D. Grimm, *Regulierte Selbstregulierung in der Tradition des Verfassungsstaats*, in: *Regulierte Selbstregulierung als Steuerungskonzept des Gewährleistungsstaates*, Berlin, 2001,, p. 9.

43 G. Abboud; Campos, R., *A Autorregulação Regulada Como Modelo do Direito Proceduralizado* (Fn. 41).

II. Self-Regulation under the European General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) presents a detailed approach to self-regulation, primarily through the certification mechanisms described in its Articles 42 and 43. This approach, which can be referred to as a form of "regulated self-regulation," represents a combination of traditional self-regulation with stricter state oversight. The GDPR model values the advantages of self-regulation, such as sector-specific knowledge and flexibility, while simultaneously addressing common shortcomings, such as inconsistent application and a lack of effective enforcement.

In connection with the regulation, certification is no longer merely an instrument for organizations to voluntarily declare their compliance, but it has become an important regulatory tool that signals greater commitment and adherence to the standards established by the GDPR.[44] Certifications must be issued by accredited organizations that undergo strict scrutiny and are approved by national data protection authorities. These authorities play a crucial role, as they not only facilitate the process but also actively monitor and enforce the standards set by these entities, ensuring that the certification bodies are competent and well-prepared to assess compliance with the strict requirements of the GDPR.

This integration requires that the certification bodies and their procedures are aligned with the specific criteria of the GDPR, ensuring that they make an effective contribution to the overall data protection ecosystem and improve the transparency of the certification process, as certifications are overseen by data protection authorities. Certified organizations must adhere to high data protection standards, and their compliance is regularly reviewed, meaning continuous monitoring takes place. This helps reduce accountability gaps, which are often observed in purely self-regulatory structures.

In addition, the GDPR's certification process encourages organizations to adopt best practices in data protection by fostering a culture of compliance and continuous improvement, benefiting not only the organizations but also the public and the individuals whose data is processed. By structuring the certification framework, the GDPR effectively bridges the gap between self-regulation and state regulation, as it provides the flexibility and sector-

44 E. Lachaud, *The General Data Protection Regulation and the rise of certification as a regulatory instrument*, in: *Computer Law & Security Review* 34/2 (2018), pp. 244–256.

specific adaptation typical of self-regulation while ensuring that this freedom leaves no room for lax standards or non-compliance. This underscores the GDPR's commitment to maintaining high data protection standards throughout Europe and enhances both organizational accountability and the protection of personal data.

In short, in the GDPR, the regulated self-regulation through certification proposes a balanced approach that leverages the advantages of self-regulation — such as market vision, innovation, and flexibility—while ensuring robust oversight to maintain public trust and protect the rights of individuals. This model can serve as an example for other regulatory frameworks that seek to utilize the benefits of self-regulation without forgoing the oversight and accountability provided by traditional regulatory mechanisms.

III. Self-Regulation in the Brazilian General Data Protection Law (LGPD)

In Brazil, the concept of regulated self-regulation was introduced into the legal framework particularly within the General Data Protection Law (*Lei Geral de Proteção de Dados*, or LGPD), which was heavily inspired by international standards, such as the European Union's General Data Protection Regulation (GDPR).[45] According to Article 50 of the LGPD, controllers and processors responsible for data processing may, within the scope of their powers, individually or through associations, establish rules of good practice and governance. These rules define the conditions for organization, operational procedures, processes — including complaints and requests from data subjects — security standards, technical standards, specific obligations of those involved in data processing, awareness-raising measures, internal monitoring, risk mitigation mechanisms, and other aspects related to the processing of personal data. These rules of good practice and governance can be recognized and disseminated by the National Data Protection Authority (*Autoridade Nacional de Proteção de Dados,* or ANPD) in accordance with Article 50, §3 of the LGPD.

The range of topics that can be addressed within the framework of regulated self-regulation is broad and covers an exemplary spectrum of

45 In the debate surrounding the draft bill for a law on media transparency, which became known as the "Fake News Law," the decision was made to include the institution of regulated self-regulation. For more on this topic, see J. Maranhão; R. Campos, *Exercício de autorregulação regulada das redes sociais no Brasil*. In: Nery, N. Campos; Abboud, Georges (Ed.): *Fake News e Regulação*, São Paulo: RT, 2018.

possibilities that can be explored through this mechanism. These include complaints and petitions from data subjects, which provide individuals with a means to raise concerns or request corrections related to the use of their personal data. Equally important are security standards, which establish minimum requirements for the protection of data against unauthorized access or loss. Technical standards ensure compatibility and security between different systems and technologies. Awareness-raising measures are essential to inform and educate both professionals and the general public about the importance and methods of protecting personal data. Internal monitoring and risk mitigation mechanisms help organizations proactively oversee and adjust their practices to avoid data breaches. In addition to these aspects, other elements related to the processing of personal data are also considered, resulting in a comprehensive and detailed approach to the management and protection of personal information.

By allowing controllers and processors to formulate rules of good practice and governance concerning aspects of personal data processing within their respective areas of responsibility, the law brings together two legal institutions within the regulatory framework of personal data protection: "the ability of the state to recognize non-legislative normative sources, and the voluntary exercise of accountability and self-restraint by these processors, with the role of the ANPD as a security authority being to provide legal certainty and establish guidelines for these multi-stakeholder phenomena."[46]

Since the LGPD gave the ANPD considerable leeway to recognize and publish these rules without specifying the criteria for this authority, in practice there has been an "insufficient use of the mechanism by processors due to a number of questions regarding its operationalization."[47]. There was therefore "a mistrust of the institution, which went so far as to make it opaque, without attracting attention or interest compared to other LGPD topics, even in the academic field."[48]

While, on the one hand, the LGPD has satisfactorily introduced regulated self-regulation, on the other hand, with regard to seals and certifications, there is a need for stronger normative support through regulation by the national data protection authority or a legislative amendment, as this issue

46 Hahn (Fn. 14), p. 11.
47 Hahn (Fn. 14), p. 9.
48 Hahn (Fn. 14), p. 9.

is currently only addressed as a legal basis for international data transfers.[49] The ANPD could act as the accrediting body for seals and certifications on various issues related to LGPD compliance, thus paving the way for impartial audits of processors by properly accredited certifying entities, while ensuring minimal intervention and behaviour-promoting measures from the administration.

D. Regulation of Artificial Intelligence through Self-Regulatory Mechanisms

I. Initial Considerations

The governance of AI brings with it ethical, legal, regulatory, and technical challenges, which have sparked debates about when or whether a legal-regulatory framework is necessary, whether ethical or technical approaches are sufficient, and whether the existing ethical and regulatory frameworks adequately address the impacts of AI.[50] It is evident, however, that trust in AI systems and products is a fundamental criterion for the widespread adoption of AI[51], as "trust is the foundation of societies, economies, and sustainable development," and it is undeniable that "individuals, organizations, and societies will only be able to fully realize the potential of AI if trust in its development, deployment, and use can be established." [52]

In general, two major categories of self-regulatory mechanisms can be distinguished. The first category includes labels, seals, certification systems, quality seals, and trust seals. These are mechanisms that set a specific stan-

49 Chapter V of the LGPD.

50 C. Cath, *Regulierung der künstlichen Intelligenz: Ethische, rechtliche und technische Möglichkeiten und Herausforderungen*, in: *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, v. 376, n. 2133, 2018, available at: https://royalsocietypublishing.org/doi/10.1098/rsta.2018.0080 (accessed on 05.10.2023).

51 European Commission, *Proposal for a Regulation of the European Parliament and of the Council laying down requirements for artificial intelligence. Initial Impact Assessment*, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=PI_COM(2020)3896535&from=EN; European Commission, *White Paper on Artificial Intelligence: A European Approach to Excellence and Trust*, available at: https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf (accessed on 05.10.2023).

52 S. Thiebes / S. Lins / A. Sunyaev, *Vertrauenswürdige künstliche Intelligenz*, in: *Elektronische Märkte* 31 (2021), pp. 447-464, available at: https://link.springer.com/article/10.1007/s12525-020-00441-4 (accessed on 05.10.2023).

dard for AI applications and outline a set of criteria by which that standard is assessed, usually through an audit process. The second category includes codes of conduct and ethics, which can be described as declarations that establish and define requirements or principles that organizations developing or acquiring AI applications must follow. These codes aim to ensure the safe and ethical development and use of these systems, although they generally do not define measurable criteria or involve an audit process.[53]

Labelling initiatives are intended to benefit both consumers and end-users of AI applications as well as the organizations that develop them. For the first group, one of the main goals of these initiatives is to strengthen trust in AI applications by signalling technical reliability and quality[54]. Self-regulatory mechanisms can also enhance competition by creating transparency and comparability between the AI applications available on the market.[55] For companies developing AI applications, one of the main advantages of these initiatives is that they learn how to comply with emerging standards and best practices for a technology like AI[56]. A key aspect shared by most of these initiatives, in line with their intended goals, is the use of an audit process conducted by independent third parties. Similarly, codes of conduct aim to strengthen the trust of end-users and consumers and guarantee good practices in the acquisition and use of AI systems that are safe and ethically sound.[57]

D'Angelo et al. highlight several opportunities that arise from granting seals, codes of conduct, and other self-regulatory mechanisms currently being developed for AI applications. Among the most significant opportu-

53 C. D'Angelo et al., *Labelling initiatives, codes of conduct and other self-regulatory mechanisms for artificial intelligence applications: From principles to practice and considerations for the future*, Santa Monica, CA 2022, available at: https://www.rand.org/pubs/research_reports/RRA1773-1.html (accessed on 05.10.2023).

54 KI.NRW: *Designing Artificial Intelligence Secure and Trustworthy: The next Big Step towards a Certification of AI "Made in Germany"*, February 26, 2021. Accessed on December 8, 2021: https://www.ki.nrw/en/designing-artificial-intelligence-secure-and-trustworthy-the-next-big-step-towards-a-certification-of-ai-made-in-germany/.

55 S. Kelley; Y. Levin; D. Saunders, *A Code of Conduct for the Ethical Use of Artificial Intelligence in Canadian Financial Services*, Smith School of Business, Queen's University, 2018. Accessed on December 8, 2021: https://www.researchgate.net/publication/342168576_A_Code_of_Conduct_for_the_Ethical_Use_of_Artificial_Intelligence_in_Canadian_Financial_Services.

56 C. Galán, *The Certification as a Mechanism for Control of Artificial Intelligence in Europe, European Union*, 2019. Accessed on December 8, 2021: https://ec.europa.eu/futurium/en/system/files/ged/c._galan_phd_-_ai_paper.pdf.

57 D'Angelo et al. (Fn. 53).

nities is the promotion of the ethical development and use of AI products and services, which is crucial given the frequent perception of these systems as opaque. Additionally, these initiatives help build trust in AI products and services. Another important aspect is strengthening the relationships between actors in the AI supply chain during its development and implementation. Such mechanisms are also key to signalling specific standards to companies and end-users in the market, setting market standards, and enhancing global competitiveness[58]. Finally, they propose reintroducing human oversight into technological processes and emphasize the importance of human interaction in technology management.

The challenges associated with self-regulation in AI applications are numerous and multifaceted. First, due to the complexity of AI applications, it is difficult to develop and apply criteria for assessing ethical and legal principles. This complexity also requires the involvement of various stakeholders in the design and implementation of the evaluation. Moreover, the potential costs and effort involved in the evaluation may discourage participation, especially for small companies, which may perceive the process as too expensive or burdensome. In the design and implementation of self-regulation systems, there is a significant conflict between the goal of protecting consumers and promoting innovation and competition in the market. Another challenge is to ensure the legitimacy and accountability of these initiatives through transparent third-party audits. The multitude of different initiatives can confuse both companies and consumers, potentially eroding trust in these measures. Finally, promoting the adoption of voluntary self-regulation mechanisms is challenging, particularly in a competitive environment where compliance with regulations may be seen as a strategic disadvantage.[59]

These challenges highlight the complexity and the need for carefully balanced approaches to ensure that self-regulation efforts are effective and beneficial for both the AI industry and consumers. Self-regulation for AI presents a promising perspective for promoting its ethical and responsible development, and several factors can be considered to strengthen and support this approach. For example, the active involvement of a wide range of stakeholders from different disciplines in the design and development of

58 M. Haataja, *How Certification Promotes Responsible Innovation in the Algorithmic Age*, 2020. Accessed on December 8, 2021: https://bdtechtalks.com/2020/05/28/autonomous-intelligent-systems-certification-ieee/.

59 D'Angelo et al. (Fn. 53).

self-regulation instruments for AI can increase engagement and acceptance of these initiatives, allowing for the inclusion of diverse perspectives and knowledge, which enriches the process. It is also important to recognize that seeking innovative approaches is essential to address the perceived costs and burdens associated with implementing self-regulation mechanisms[60]. Furthermore, innovation provides flexibility and adaptability in the assessment of AI systems and fosters an innovation-friendly environment[61].

II. The European Experience

Although not specified in the European AI Act itself, the European Commission's White Paper on Artificial Intelligence made additional recommendations for the use of voluntary certification systems and seals[62]. In the Commission's initial impact assessment of the AI Act, an EU law to introduce voluntary labelling systems was proposed as a policy option[63]. With the goal of "strengthening user trust in AI systems and promoting the widespread adoption of the technology," the White Paper proposed voluntary labelling systems for low-risk AI, which would "allow economic operators to signal that their AI-based products and services are trustworthy [...] so that users can easily recognize that the relevant products and services meet certain objective and standardized EU-wide norms that go beyond the normally applicable legal obligations."[64] Although participation in the labelling scheme is voluntary, providers who choose to take part must meet certain EU-wide requirements (in addition to existing EU legislation) in order to carry an AI quality mark. The quality seal would demonstrate to the market that the AI application is reliable.

60 Swiss Digital Initiative, *Labels and Certifications for the Digital World: Mapping the International Landscape*, 2021. Accessed on December 8, 2021: https://a.storyblok.com/f/72700/x/73839efcca/attch-1_sdi_initiatives_final.pdf.

61 G. Myers; K. Nejkov, *Developing Artificial Intelligence Sustainably: Toward a Practical Code of Conduct for Disruptive Technologies*, 2020. Accessed on December 8, 2021: https://openknowledge.worldbank.org/bitstream/handle/10986/33613/Developing-Artificial-Intelligence-Sustainably-Toward-a-Practical-Code-of-Conduct-for-Disruptive-Technologies.pdf.

62 European Commission, *White Paper on Artificial Intelligence: A European Approach to Excellence and Trust*, available at: https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf (accessed on 05.10.2023).

63 European Commission, *Proposal for a Regulation of the European Parliament and of the Council laying down requirements for artificial intelligence* (Fn. 51).

64 European Commission, *White Paper on Artificial Intelligence* (Fn. 51).

Based on these proposals, a growing number of voluntary and self-regulatory initiatives for the ethical development of AI have been suggested by stakeholders from the private sector, civil society, as well as academia and politics. For example, the Bertelsmann Foundation has proposed the creation of an ethical quality seal for AI systems.[65] Denmark[66] and Malta[67] have recently published national AI strategies in which they propose a seal and certification program for AI products and services. Several other organizations, such as the All-Party Parliamentary Group on Data Analytics, the Institute of Electrical and Electronics Engineers (IEEE), and the World Economic Forum, have also suggested ideas for AI labelling or certification systems.[68] Most of these initiatives, however, still need to be developed and tested in practice. Similarly, a growing number of codes of conduct for AI are being developed by industry associations, academic and research institutions, corporations, and public sector organizations, such as the one for the British National Health Service (NHS).[69]

The proposed use of seal schemes and codes of conduct for low-risk AI applications is partly based on the implementation of these self-regulatory mechanisms in other industries.[70] Labels and seals are particularly ubiquitous in the food industry, where nutritional values are uniformly color-coded, and the sustainability performance of products is visually verified through standards and seals. In the context of environmental labelling and information regulations, environmental seal schemes have proven use-

65 VDE, Bertelsmann Stiftung. *From Principles to Practice: An interdisciplinary framework to operationalise AI ethics*, available at: https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/WKIO_2020_final.pdf (accessed on 05.10.2023).

66 Danish Government, *National Strategy for Artificial Intelligence*, 2019, available at: https://en.digst.dk/media/19337/305755_gb_version_final-a.pdf (accessed on 05.10.2023).

67 Malta, *Towards an AI Strategy*: *High-level policy document for public consultation*, 2019, available at: https://malta.ai/wp-content/uploads/2019/04/Draft_Policy_document_-_online_version.pdf (accessed on 05.10.2023).

68 Zeichner, Daniel; Clement-Jones, Tim; Holmes of Richmond, Chris, *An Ethical AI Future: Guardrails & Catalysts to Make Artificial Intelligence a Force for Good*. Policy Connect, June 19, 2023. Available online at: https://www.policyconnect.org.uk/research/ethical-ai-future-guardrails-catalysts-make-artificial-intelligence-force-good, last accessed on: October 9, 2024.

69 GOV.UK, *New code of conduct for artificial intelligence systems used by the NHS*, 2019, available at: https://www.gov.uk/government/news/new-code-of-conduct-for-artificial-intelligence-ai-systems-used-by-the-nhs(accessed on 05.10.2023).

70 D'Angelo et al. (Fn. 53).

ful for harmonizing countries' approaches to environmental criteria and reducing administrative costs, which can lead to an increase in trade with environmentally certified goods.[71]

While these examples are useful comparisons, the differences in labelling within the digital context must be taken into account, including industry-specific issues such as the protection of personal data, the rapid development of technology, and territoriality, which present unique challenges.[72] The same applies to codes of conduct, which, while consistent across all sectors and industries, must be adapted to the specific concerns and characteristics of AI systems. In the case of the European Union, they should meet the requirements for high-risk AI, as proposed in the AI Act.[73]

III. The Brazilian Experience

In the Brazilian context, conversely, AI regulation has almost undergone a pendulum swing, initiated by the Brazilian Strategy for Artificial Intelligence (EBIA), to which Bill 21/2020, largely principle-oriented, was added. On the other hand, Bill 2338/23, the result of the work of a commission of legal experts appointed to address the issue, was largely inspired by the AI Act model and adopts many of its rules. Additionally, a "legal framework for artificial intelligence" in Brazil was the subject of debate by the Senate's internal ad hoc committee on artificial intelligence (*Comissão Temporária Interna sobre Inteligência Artificial*, or CTIA), whose task was to review the projects attached to the final report approved by the commission of legal experts, as well as all new projects that could regulate the issue. From this debate emerged a substitute bill that intends to be a middle ground between the two main approaches that had existed until then. Among the concerns of the new AI bill are topics such as development within the age-

71 M. Klintman, *A Review of Public Policies Relating to the Use of Environmental Labelling and Information Schemes (ELIS)*, in: *OECD Environment Working Papers*, n. 105, available at: https://www.oecd-ilibrary.org/environment/a-review-of-public-policies-relating-to-the-use-of-environmental-labelling-and-information-schemes-elis_5jm0p34bk7hb-en (accessed on 05.10.2023).

72 D'Angelo et al. (Fn. 53).

73 European Commission, *Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts*, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206 (accessed on 05.10.2023).

old dilemma of innovation and regulation, the search for the ideal balance that does not exclude Brazil from the "AI gold rush" while preserving the mitigation of risks inherent in a continental country with many racial and social differences, to name a few.

As for self-regulation, the approach proposed in the CTIA's draft is remarkably integrative and cooperative, aiming to create a governance structure that connects state authorities with self-regulatory bodies. The inclusion of self-regulatory organizations in the National System for Regulation and Governance of Artificial Intelligence (SIA) is a key strategy for implementing a regulatory system that values sector-specific expertise while maintaining the oversight and control necessary to ensure compliance with ethical and legal standards. Article 40 of the draft contains definitions regarding the functioning and composition of the SIA. The text explicitly mentions the involvement of "self-regulatory bodies" as its members, indicating a model where the private sector plays an active role in the creation and implementation of behavioural standards, which can include the establishment of ethical practices, information security, and specific technical standards for the development and application of AI. "Accredited certification bodies" are also mentioned as part of the SIA, suggesting that certification will play a key role in verifying compliance with the standards set by the industry and government regulation. This reflects an approach similar to the "regulated self-regulation" model of the General Data Protection Regulation, where certification is not just a conformity seal but an active regulatory tool that promotes ongoing compliance with regulations and regular evaluations.

As per the system's objectives and foundations, the draft emphasizes the importance of assessing and strengthening the regulatory powers of agencies and regulatory bodies in line with the general guidelines of the responsible authority coordinating the system. This means an effort to align self-regulation standards with broader state regulations, ensuring that AI practices are safe, ethically sound, and responsible. In this context, the system aims for decentralized collaboration between agencies and regulatory bodies at various levels of government (federal, state, district, and municipal), which is essential for a dynamic and cross-sectoral field like AI. Additionally, harmonization with other cross-sectoral regulatory areas, such as antitrust law and consumer protection, is pursued, reflecting a holistic approach to addressing the multidimensional challenges that AI presents.

Article 41 of the draft, in turn, sets out the responsibilities and authorities of the competent body, designated as the coordinating entity of the national regulatory and governance system for artificial intelligence. This provision highlights the fundamental role of this body within the regulatory and governance structure for AI in Brazil, reflecting a governance model that encompasses both regulation and self-regulation, like the one previously discussed in relation to the General Data Protection Regulation (GDPR).

According to the draft, the responsible authority is expected to represent Brazil in international forums on artificial intelligence, ensuring that the country aligns with global practices and standards and can influence the development of international AI regulation. The authority is empowered to issue binding standards in collaboration with other regulatory bodies of the National System for the Regulation and Governance of Artificial Intelligence. These standards cover important aspects such as legally guaranteed rights, transparency requirements in the use of AI systems, certification of systems deemed high-risk, algorithm impact assessments, and procedures for reporting serious incidents. These norms are crucial to ensuring that companies dealing with AI comply with stringent standards, thereby protecting citizens' rights and the integrity of AI systems.

Additionally, the authority is responsible for issuing general guidelines, which are not binding but should orientate the development, implementation, and use of AI systems and shape responsible practices in this sector. The authority may also enter into regulatory agreements with members of the SIA to establish specific rules and coordination procedures, thereby facilitating effective collaboration between different regulatory bodies and AI sectors. Although the authority's involvement in the regulatory processes of other regulatory bodies is not binding, it is crucial to ensuring a coherent approach to AI regulation across various sectors. Furthermore, the authority holds comprehensive normative, regulatory, and sanctioning powers in economic sectors where there is no specific regulatory body or accredited self-regulatory organization, ensuring comprehensive and integrative regulation of AI across all areas of economic activity. In regulatory sandbox environments related to AI, the authority should be informed of activities and can intervene to ensure that experiments align with the goals and principles of the law. This enables controlled innovation and creates a space where new technologies and business models can be tested under regulatory supervision

Article 43 of the draft outlines the functions of the responsible authority within the already mentioned SIA, clarifying how self-regulation, codes of

conduct, and other governance practices are to be promoted and managed in the context of AI in Brazil. The responsible authority is tasked with protecting fundamental rights that may be affected by the use of AI systems and must ensure strict oversight and the implementation of protective measures. Furthermore, the authority is responsible for promoting the adoption of best practices and codes of conduct in the development and use of AI, thereby supporting behavioural standards with a focus on ethics, transparency, and accountability. It is also important that the authority be granted the power to conduct internal audits and mandate independent external audits to verify the compliance of AI systems with legal regulations, ensuring that codes of conduct and self-regulation practices are effective rather than mere formalities. The authority must also promote international cooperation to align Brazilian practices with global best practices. Additionally, it can negotiate compromises to resolve irregularities or legal uncertainties and adapt or enhance codes of conduct as needed. The accreditation of institutions to conduct audits and investigations ensures that the monitoring of AI systems is carried out by qualified entities, which strengthens the self-regulation system. Finally, the authority should be capable of handling anonymous complaints, which is essential for exposing and correcting violations without whistleblowers fearing retaliation.

For the purposes that concern us here, it should be noted that Article 44 of the draft stipulates that all regulations and standards created by the responsible authority must be preceded by a public consultation. This provision aims to ensure transparency and democratic participation in the process of formulating strategies and regulations that affect the management and use of artificial intelligence in Brazil.

E. Final Considerations

As constitutional lawyer Dieter Grimm rightly explains, self-regulation largely depends on the collaboration between the regulating state and the societal actors being regulated.[74] Regulated self-regulation is a promising way to foster the ethical and responsible development of AI while also ensuring the flexibility and adaptability needed for innovation, especially filling a gap within the concept of digital constitutionalism related to the generation of social knowledge. Several factors can be considered to

74 *Grimm* (Fn. 42).

strengthen and support this approach. The active, multidisciplinary participation of diverse stakeholders in designing and developing self-regulation instruments for AI can enhance engagement and acceptance, incorporating a wide range of perspectives and expertise to enrich the process. Additionally, adopting innovative approaches is essential to mitigate the perceived costs and burdens of implementing self-regulation mechanisms.

Instead of pursuing a supposedly universal approach, which can quickly become outdated, it is crucial to consider the diverse knowledge-building processes within today's digital society. The use of self-regulation instruments tailored to specific contexts and use cases encourages voluntary adoption while ensuring flexibility. This approach enables the adaptation of standards to the unique demands of different AI applications, fostering a regulatory environment that safeguards fundamental rights while promoting innovation and development.

II.
Data Protection and Privacy Rights in the Digital Age

Unfolding the Protected Interests of Data Subjects in Digital Constitutionalism

Marion Albers

Abstract: How to conceptualize the protected interests in data protection law is of crucial interest for digital constitutionalism, as the European Union has adopted a series of new regulations as part of its data and digital strategy. After giving an overview of this strategy to show the extent to which the legal framework is changing, this article provides an in-depth cross-jurisdictional analysis of the right to privacy, the right to informational self-determination, and the right to the protection of personal data. While the details of these rights depend on the specific legal system, their substantive and doctrinal constructions can be distinguished, and a closer analysis reveals particular achievements and weaknesses. Once the factual fundamentals – in particular, data and personal data, information, processing of data and information or knowledge – have been clarified, the need to develop approaches tailored to the characteristics of the handling of personal data and information as a specific dimension of protection becomes obvious. Multi-layered, multi-dimensional and multifaceted guarantees and rights as well as sophisticated doctrinal constructions and interplays between fundamental rights and statutory regulation must be worked out. The last part of this article presents the required doctrinal approach to data protection interests. It is constructed as a functional cooperation of fundamental rights at different levels resulting in a bundle of provisions and rights to which all fundamental rights can contribute with their substantive particularities. Such an approach can be harmonized with the changes in the legal framework brought about by the European data and digital strategy.

A. Introduction

How to conceptualize and describe the interests of individuals to be protected with respect to the handling of personal data and information, is a

key issue in the development of information and data law. The more society becomes digitalized, the more this area of law moves from the sidelines to the center of attention. At first glance, the legitimate interests covered by data protection law seem to be clear: right to privacy, right to informational self-determination, or right to the protection of personal data. But these are "umbrella terms"[1] at best. A closer analysis reveals contestable premises, pitfalls, heterogeneous notions and misconceptions. Additionally, the Internet and the social arrangements that it makes possible raise a multitude of more or less novel questions.[2] Both the subject matter and the doctrinal construction of protected interests require clarification and further elaboration.

This article will first provide an overview of the European data and digital strategy to show the extent to which the legal framework is changing, which data protection rights shape as an integral element, but in which they must also be consistently embedded. In the following third section, we will take a look at the familiar, but fuzzy concepts of data protection interests in scholarly debates and in case law. The focus is on the right to privacy, the right to informational self-determination, and the right to the protection of personal data. The in-depth analysis of the achievements and limitations of these different approaches will reveal that the idea of a "right to the protection of personal data" can offer a starting point to address substantial and doctrinal challenges. Further steps can only be reached if we get a clear understanding of the factual fundamentals of data protection, in particular, data and personal data, information, processing of data and information, or knowledge. In the fourth section, I will first explain more closely that data protection deals with a highly complex subject matter. In this light, multi-layered, multi-dimensional and multifaceted guarantees and rights as well as sophisticated doctrinal constructions and interplays between fundamental rights and statutory regulation must be developed. These insights enable us to concretize protected interests of data subjects within a multi-layered conception to which all fundamental guarantees and rights with their substantive particularities can contribute. Such an approach is a prerequisite for coordinating data protection law with other legal regulations in a reasonable way and, for example, embedding it appropriately within the overarching European data and digital strategy.

1 Cf. *Daniel Solove*, Understanding Privacy, 2008, 45.

2 See the manifold articles in *Marion Albers* and *Ingo Wolfgang Sarlet* (eds.), Personality and Data Protection Rights on the Internet, 2022.

B. Reframing Data Protection Interests in Digital Constitutionalism

Since the beginning of this decade, the European Commission has presented numerous proposals for the regulation of data, technologies and infrastructures which are partially captured under the catchword "digital sovereignty"[3]. A crucial part of the Commission's overarching strategies and policies is a comprehensive package for "shaping Europe's digital future".[4] This covers, first of all, the meanwhile implemented regulations on digital markets and digital services.[5] Their provisions concern the regulation of gatekeepers including their handling of data or obligations of online platforms, for example, with regard to user-generated illegal content. In addition, the aim of these strategies is to establish a common European data space or sector-specific data spaces, the design of which is intended to unlock the potential of digitization. Within the framework of the data strategy, the data protection regulations – above all the General Data Protection Regulation (GDPR)[6], which is supplemented by the Data Protection Direc-

3 More comprehensive on this catchword *Petra Gehring*, Datensouveränität versus Digitale Souveränität: Wege aus dem konzeptionellen Durcheinander, in: Augsberg/Gehring (eds.), Datensouveränität, 2022, 19 (19 ff.).

4 For the foundations see in particular Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "European Interoperability Framework – Implementation Strategy" of 23.3.2017, COM(2017) 134 final; "Towards a common European data space" of 25.4.2018, COM(2018) 232 final; "Shaping Europe´s digital future" of 19.2.2020, COM(2020) 67 final; "A European strategy for data" of 19.2.2020, COM(2020) 66 final; "European Commission digital strategy. Next generation digital Commission" of 30.6.2022, COM(2022) 4388 final; White Paper "On Artificial Intelligence – A European approach to excellence and trust" of 19.2.2020, COM(2020) 65 final.

5 Regulation (EU) 2022/1925 of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act) of 14.9.2022, O. J. L 265/1; Regulation (EU) 2022/2065 of the European Parliament and of the Council on a single market for digital services (Digital Services Act) of 19.10.2022, O. J. L 277/1.

6 Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) of 27.4.2016, O. J. L 119/1.

tive for Police and Criminal Justice[7], by the e-privacy Directive[8] and by further sector-specific legal acts – are classified as a first fundamental pillar intended to provide a "framework for trust in the digital environment"[9]. In the meantime, a whole series of further regulations or regulatory proposals have been added. Complementary to and distinct from the GDPR, but entirely in line with the double finality set out in Art. 1 GDPR, the guiding principle of free data flows is established for non-personal data.[10] Open data concepts, as they are increasingly being enshrined, aim to ensure that certain data sets and documents in the public sector are made available in open, machine-readable, accessible, findable and reusable formats, and may be reused in the private sector, subject to conditions if necessary.[11] This aims at enabling not only innovative data-based business models or research, but also joint government-to-business data use, for example in the fields of environmental protection or mobility. The provisions of the regulation on European Data Governance[12] are intended to promote the establishment of sector-specific data spaces, such as the already outlined

7 Directive 2016/680 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, O. J. L 119/89.

8 Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector of 12.7.2002, O. J. L 201/37. The debates on an e-privacy regulation are still ongoing.

9 Communication from the Commission "Towards a common European data space" of 25.4.2018, COM(2018) 232 final, p. 1.

10 See Regulation (EU) 2018/1807 of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union of 14.11.2018, O. J. L 303/59, and the Commission's Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union of 29.5.2019, which in particular deal with the demarcation from the regulations on personal data in the GDPR, COM(2019) 250 final.

11 Directive 2019/1024/EU of the European Parliament and of the Council on open data and the re-use of public sector information of 20.6.2019, O. J. L 172/56; for delimitation in the above context, see Art. 2(1)(h) on its scope.

12 Regulation (EU) 2022/868 of the European Parliament and of the Council on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) of 30.5.2022, O. J. L 152/1.

European Health Data Space[13]. Among other things, these regulations create a framework for "data altruism": Data subjects provide data for specified (research) purposes by means of consent. Complementing the Open Data Directive, the reuse of sensitive data is facilitated under certain conditions, first of all through the implementation of technological data protection concepts. New institutions such as data intermediaries, i.e., data sharing services that can also operate in the sense of "data trustees", and data altruistic organizations are given a key role with regard to, among other things, ensuring data protection rights. Complementary to the GDPR and the Data Governance Regulation, the Data Act revolves around ensuring that personal and non-personal data generated in the context of the Internet of Things is made available for use by various stakeholders. To achieve this goal, data owners must adhere to and ensure certain conditions for data processing. Above all, users of products or related services are to be enabled to use the data that is generated by their use (user-generated data), to share it with third parties or demand direct access for third parties. Subject to the specified criteria, data access is opened up for the benefit of public bodies. All in all, the knowledge and value creation potential of this data shall be exploited in a productive manner.[14] The Cybersecurity Act, which establishes ENISA as an institution and creates certification procedures[15], and the AI-Act, which lays down harmonized rules on artificial intelligence[16], also play an important role in connection with digitization and its regulation.

In principle, the Commission assumes that the existing data protection regulations, as one of the pillars of its data and digital strategy, can be reconciled relatively seamlessly with the new regulations.[17] A closer analy-

13 Proposal of the Commission for a Regulation of the European Parliament and of the Council on the European Health Data Space of 3.5.2022, COM(2022) 197 final. Recently, consensus has been reached in the trilogue procedure.

14 See the Regulation 2023/2854/EU of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act) of 13.12.2023, O. J. L 1/71.

15 Regulation 2019/881 of the European Parliament and of the Council on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) of 17.4.2019, O. J. L 151/15.

16 Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence […] (Artificial Intelligence Act) of 13.6.2024, O. J. L, 12.7.2024.

17 Cf., for example, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of

sis, however, reveals various inconsistencies, incompatibilities and reform requirements. To a certain extent, the GDPR sticks to traditional patterns of data protection and is path-dependent.[18] However, not all of the traditional patterns of thought are convincing and compatible with other regulatory approaches the EU data and digital strategy chooses. Irrespective of this, it becomes clear how importantly and carefully the law governing the handling of personal data and information needs to be embedded in overarching contexts and coordinated with other regulations. In view of the role of data in a digitized society and in view of the new normative models such as open data, the potential of data to create knowledge and value, and common data spaces, the law itself is dependent on dynamic updating. The necessity to develop novel regulatory patterns in data protection requires more clarity about how to conceive of the protected interests.

C. Familiar, but Fuzzy and Manifold Foundations of Data Protection Interests

Among the familiar foundations of data protection interests are the right to privacy, the right to informational self-determination, and the right to the protection of personal data. Rights to privacy are the bedrocks of broad debates and judicial decisions in the U.S. as well as in some other countries such as Canada, India, or South Africa. The understanding of the scope of protection of Art. 8 ECHR, the right to respect for private life, home, and correspondence, has been gradually extended to include data protection interests. The right to informational self-determination is a German peculiarity, but one that has attracted worldwide attention. The European Charter of Fundamental Rights – as a more recent codification that endeavors to meet the needs of modern society – guarantees everyone the right to the protection of personal data concerning him or her. The following sections analyze these legal foundations with a view to scholarly debates as well as case law and aims at identifying their achievements, weaknesses, and challenges. Last but not least, it will be shown that the

---

the Regions "A European strategy for data" of 19.2.2020, COM(2020) 66 final. See also Art. 1 III Data Governance Act, Art. 1 III Data Act.

18 Following the path taken by the Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data from 1981 and the EU Data Protection Directive from 1995, see also *Raoul-Darius Veit*, Einheit und Vielfalt im europäischen Datenschutzrecht, 2023, 103 ff.

legal concepts are always characterized by substantive as well as doctrinal and methodological considerations.

I. Right to privacy

In many countries, privacy is at the center of debates in various scientific disciplines and public discourse. It seems to be a familiar term, but "privacy" has always been a very heterogeneous concept both in the overarching or academic debates and in case law that recognizes it, in some form, as a constitutionally protected interest.

1. Traditional patterns of thought

A rough overview can highlight some patterns of thought that have been influential in western philosophy, social sciences and jurisprudence. In this context, the traditional understanding of privacy has been shaped by several basic dichotomies[19]: The first of these dichotomies is the contrasting of privacy and the state, which is constitutive for liberal thought. The second dichotomy is the differentiation between privacy and publicness, wherein the concept of "publicness" is conceived in a variety of ways.[20] The third is the differentiation between the individual's private matters and the spheres of decision and influence (also) open to others. This differentiation is linked to one's individuality but is not identical to it. At first sight, these guiding dichotomies seem easy to comprehend, but a closer scrutiny quickly reveals the numerous premises and the complexity of the converse terms. Nonetheless, a basic understanding emerges: "Privacy" assigns something to a person or a group of persons as their own concern and establishes limits to others' access to it. Due to the complexity of the guiding dichotomies and ideas in the background, this basic notion takes on various nuanced shades of meaning depending on the context and the scientific lens, and privacy touches upon a broad spectrum of topics. Varying across cultures

19 Cf. *Marion Albers*, Privatheitsschutz als Grundrechtsproblem, in: Halft and Krah (eds.), Privatheit. Strategien und Transformationen, 2013, 15 (20).

20 See *Jeff Weintraub*, The Theory and Politics of the Public/Private Distinction, in: Weintraub and Kumar (eds.), Public and Private in Thought and Practice. Perspectives on a Grand Dichotomy, 1997, 1 (1 ff.); *Norberto Bobbio*, The Great Dichotomy: Public/Private, in: Bobbio, Democracy and Dictatorship, 1989, 1 (17).

and historical epochs[21], they include the body, facets of the personality, religious convictions and conscience, spaces such as place of residence, property, close relationships such as partnership and family, or confidential documents and communications.[22] Over time and in a more controversial way, the mechanisms of allocation as one's own and the concept of access have also been understood just as abstractly and broadly. The latter includes invasions of spaces and the body, determination of decisions by third parties, processes of surveillance, or dissemination through the media, and this means that it comprises informational measures.[23] Likewise, "limits to access" are not only spatial in nature. They include physical boundaries, but also boundaries based on social expectations of expectations. Meanwhile, and in response to societal change, privacy has become a more and more differentiated concept which is fleshed out not only by substantial but also by functional approaches.[24] Against this background, it is understood as an "umbrella term".[25]

Classical concepts of privacy and traditional notions of fundamental rights are closely intertwined at several levels. This is true even for basic levels. Liberal thought on fundamental rights presupposes a differentiation between bourgeois or private society and the state. In addition, the structure of fundamental rights provisions reflects the differentiation between private matters of the individual, which *prima facie* enjoy protection based on fundamental rights, and the interests of other citizens or the general public, which can only take effect through passing a law. The protected persons, in turn, can subject state action to judicial review employing the standard of fundamental rights. Thus, we may say that the form of law itself guarantees privacy in the form of subjective rights. Besides these basic levels, there are

21 There is "no *single* history about what is private", *Beate Rössler*, Der Wert des Privaten, 2001, 15.

22 Cf. with a broad historical overview the contributions in *Philippe Ariès* and *Georges Duby*, Histoire de la vie privée, Vol. 5, 1985–1987.

23 See the description of *privacy* by *Sissela Bok*, Secrets – On the Ethics of Concealment and Revelation, 1983, 10 f.: "the condition of being protected from unwanted access by others – either physical access, personal information, or attention".

24 Cf., for example, *Ruth Gavison*, Privacy and the Limits of Law, 89 Yale Law Journal 421, 440 ff. (1980); *Helen Nissenbaum*, Privacy in Context. Technology, Policy, and the Integrity of Social Life, 2010, 74 ff.

25 *Solove* (n 1). Cf. also more closely *Bert-Jaap Koops, Bryce Newell, Tjerk Timan, Ivan Skorvanek, Tom Chokrevski* and *Maša Galič*, A Typology of Privacy, 38 University of Pennsylvania Journal of International Law, 483, 491 ff. (2017); *Sohail Aftab*, Comparative Perspectives on the Right to Privacy, 2024, 39 ff.

numerous thematic overlaps. Fundamental rights cover different protected goods which have often been classified under an overarching concept of privacy. This includes the inviolability of home or correspondence, freedom of religion or freedom of thought, or property.

As there are all these different strands covering a rich tradition, the development of a general right or more specific "rights to privacy" is quite suitable for consensus. The heterogeneous framings and the shifting meanings of privacy make it easier to refer to seemingly established viewpoints, just as they are often the reason for talking past one another. On closer analysis, it depends, of course, on the specific legal system and codification how to interpret constitutional provisions in terms of a "right to privacy". Sometimes such a right is derived on the basis of methodologically substantiated arguments; sometimes there are explicit textual anchors. Our overview of case law begins with the U.S., a cradle of a "right to privacy".

2. Approaches and developments in case law

To what extent "privacy" is a suitable description of protected interests and how rights to "privacy" must then be conceptualized in detail, is part of a broad debate in the U.S. In reaction to media intrusions, the famous article by Warren and Brandeis in 1890 advocated the recognition of a right to privacy, shaped as a "right to be let alone"[26], as part of tort law and thus put the idea on the map. While the term "privacy" is not explicitly used in the text of the U.S. Constitution, there are various approaches in the jurisdiction to anchor its more or less specified protection with regard to guarantees of primarily the First[27], Fourth[28], Fifth[29], and Fourteenth[30] Amendments in a

26 *Samuel D. Warren/Louis D. Brandeis*, The Right to Privacy, 4/5 Harvard Law Review 193 (1890).

27 "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances."

28 "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

29 "No person shall […] be deprived of life, liberty, or property, without due process of law […]."

30 "[…] nor shall any State deprive any person of life, liberty, or property, without due process of law […]."

way that these guarantees have privacy as their underlying idea, and that this, in turn, lends itself to a methodologically broad interpretation of their subject matter and scope.[31]

In several judgments of the U.S. Supreme Court, these possible approaches have been worked out with regard to more closely specified individual decisions and relationships "lying within the zone of privacy created by several fundamental constitutional guarantees [...]"[32]. In the landmark judgment *Roe v Wade*, the Court held that "a right of personal privacy, or a guarantee of certain areas or zones of privacy, does exist under the Constitution".[33] This hereafter acknowledged "right of personal privacy includes the interest in independence in making certain kinds of important decisions".[34] Such decisional privacy is not assigned solely to liberty[35] because it is not about freedom of decision as such, but about an even stronger protection for the "most intimate and personal choices a person may make in a lifetime, choices central to personal dignity and autonomy"[36]. The allocation of decision-making options is linked to certain spaces or topics and is inspired by the traditional differentiation between the individual's private matters and the spheres of decision and influence (also) open to others.

Privacy as a protected interest has been further outlined by interpreting the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures", established in

31 Methodologically partly with references to the Ninth Amendment: "The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people." See Justice *Goldberg* Concurring Opinion in *Griswold v Connecticut* 381 US 479, 489 ff. (1965).

32 *Griswold v Connecticut* 381 US 479, 485 (1965).

33 *Roe v. Wade*, 410 U.S. 113, 152 (1973), and the Court stated in the following (at 153) that this "right of privacy, whether it be founded in the Fourteenth Amendment´s concept of personal liberty and restrictions upon state action, as we feel it is, or, as the District Court determined, in the Ninth Amendment´s reservation of rights to the people, is broad enough to encompass a woman´s decision whether or not to terminate her pregnancy." Recently, this decision has been overruled by the U. S. Supreme Court´s judgment of June 24, 2022, *Dobbs v. Jackson Women Health Organization*, with as yet not fully foreseeable ramifications.

34 *Whalen v. Roe* 429 U. S. 589, 599 f. (1977); *Carey v Population Services International* 431 U.S. 678, 684 (1977).

35 See, however, the sophisticated argumentation with some well-justified criticism of *Jeffrey Bellin*, Pure Privacy, 116 Northwestern University Law Review 463, 477 ff., 481 ff. (2021).

36 *Planned Parenthood of Southeastern Pa. v. Casey*, 505 U.S. 833, 851 (1992).

the Fourth Amendment, and by specifying which spaces and objects are protected against what. The protection of the (relative) inviolability of the home as the spatial sphere of private life which is delineated in terms of its functions as well as physical boundaries (for example walls or fences) is a classic paradigm case. The protection of the secrecy of telecommunications can also be captured by using spatial metaphors which address the network of communication relationships that are created via the use of certain communications technologies and services. Over time, the jurisdiction has moved away from restricting the protected good to "material things – the person, the house, his papers, or his effects [...]"[37] characterized by corporeal, material, or physical features and boundaries and regularly existing possibilities of control. Likewise, the understanding of what "searches and seizures" are, has been dissociated from the notion that an "entry of the houses"[38] would be required for the approval of a relevant encroachment. In response to changes in the way society communicates, the U.S. Supreme Court reached the landmark decision *Katz v United States*[39]: An enclosed public telephone booth is an area where a person has a constitutionally protected reasonable expectation of privacy and eavesdropping activities of governmental agencies constitute a "search and seizure" within the meaning of the Fourth Amendment that extends as well to the recording of oral statements. For the subsequent case law, profound rearrangements, abstractions and novel key concepts are crucial, especially the argumentation that "the Fourth Amendment protects people, not places"[40], along with

37 In *Olmstead v United States* 277 U. S. 438 (1928), the question before the Court was whether the use of evidence of private telephone conversations, intercepted by means of wiretapping, amounted to a violation of the Fourth and Fifth Amendments. In a 5:4 decision, it was held that there was no violation of the Fourth and Fifth Amendments. Chief Justice *Taft* wrote the majority judgment, holding that (at 464): "The Amendment itself shows that the search is to be of material things – the person, the house, his papers, or his effects ...".

38 See for the "trespass doctrine" *Olmstead v United States* 277 U. S. 438, 464 (1928). See also the dissent of Justice *Brandeis* in this respect.

39 *Katz v. United States*, 389 U.S. 347 (1967). Charles Katz was a gambler who used a public telephone booth to transmit illegal wagers. Unbeknownst to Katz, the FBI which was investigating Katz's activity, was recording his conversations via an electronic eavesdropping device attached to the exterior of the phone booth. Subsequently, Katz was convicted based on these recordings. He challenged his conviction, arguing that the recordings were obtained in violation of his Fourth Amendment rights.

40 *Katz v. United States*, 389 U.S. 347, 351 (1967).

the "reasonable expectation of privacy" test[41] which places the emphasis on social relationships as well as on the boundaries that arise through them, and the extended understanding of encroachments. Substantive approaches based on traditional images of the safeguarded person or house are supplemented by functional approaches: the protective function is the guarantee of privacy and what fulfills the functions of such privacy under the given social conditions, based on expectations of privacy that society acknowledges as reasonable, should be safeguarded. On the one hand, this leads to flexibility, but on the other hand, to a loss of legal certainty. This is because descriptions of social contexts and functional relations depend on the predefined theoretical framework and theoretical assumptions, for example a theory of the individual and individuality.[42] The extension of the scope of protection goes hand in hand with an expanded understanding of "search and seizures". To a certain extent, the permissibility of these encroachments has always indicated that fundamental rights can include a protection against data collection, however, their traditional understanding was linked to certain activities against which a high level of protection is explainable due to the intrusiveness of the methods or the risks of their use regarding protected interests.[43] A more abstract understanding of search and seizures makes it possible to include new activities and methods made possible by technological developments as well as further encroachments of an informational nature. In turn, this leads to a loss of criteria that limit the spectrum of encroachments covered and of legal certainty. The subsequent case law illustrates the adaptability to social and technical developments as well as constant discussions regarding both the underlying legal approaches and the subsumption of the specific circumstances of the

41 In the following, the "reasonable expectation of privacy" has become a pivotal pattern of argumentation and been relied on by various other jurisdictions while developing the right to privacy.

42 Cf. *Gavison* (n 24), 445.

43 Cf. also the dissent of Justice *Alito*, joined by Justice *Thomas*, *Carpenter v United States*, 585 U. S. ____ (2018), p. 10 f.

cases.[44] This becomes particularly evident in *Carpenter v United States*.[45] In this landmark ruling, the majority highlighted that the conception of the Amendment has been expanded "to protect certain expectations of privacy" which could be positively assessed for cell site location information in light of their informative content and regardless of the fact that this data is held and retrieved by the wireless carrier.[46] The four dissents presented a variety of arguments which spanned from fundamental criticism of the *Katz* test[47] to the insistence on "accepted property principles as the baseline for reasonable expectations of privacy"[48] up to the proposal to revisit the "kind of legal interest" that "is sufficient to make something *yours*" and "the source of law that determines that" in order to also give room for legislative participation[49].

Beyond the Fourth Amendment, the informational dimension of the right to privacy is addressed to a certain extent by using the idea of a zone of privacy created by several fundamental constitutional guarantees. The judgment *Whalen v Roe* was the starting point for differentiating kinds of interests which are covered by this protection[50], even though the grounds of this judgment were fluctuating when locating these interests within

44 For example, whether "reasonable expectations of privacy" can be recognized, is addressed in *United States v Miller*, 425 U.S. 435 (1976), in *Minnesota v Olson*, 495 U.S. 91 (1990), or in *Minnesota v. Carter*, 525 U.S. 83 (1998). Whether there is a "search" under the Fourth Amendment, is discussed with regard to an installation and use of a pen register in *Smith v Maryland*, 442 U.S. 735 (1979), to the thermal imaging of the house in *Kyllo v. United States*, 533 U.S. 27 (2001), or to a GPS tracking device on a vehicle in *United States v Jones*, 565 U.S. 400 (2012). See also *Riley v California*, 573 U.S. 373 (2014), for the search and seizure of digital contents of a cell phone.

45 Timothy Carpenter was charged with several crimes after wireless carriers handed over the cell site location information generated by his phone to the FBI and these data supported the suspicion that he had been involved in these crimes, *Carpenter v United States,* 585 U. S. _____ (2018).

46 *Carpenter v United States,* 585 U. S. _____ (2018), p. 5; cf. for the protection of "a person´s expectation of privacy in his physical location and movements" pp. 7 ff. and for the discussion of the former "third-party doctrine" pp. 9 ff.

47 See the dissent of Justice *Thomas* in *Carpenter v United States,* 585 U. S. _____ (2018).

48 Dissent of Justice *Kennedy*, joined by Justice *Thomas* and Justice *Alito*, *Carpenter v United States,* 585 U. S. _____ (2018), p. 22.

49 Dissent of Justice *Gorsuch*, *Carpenter v United States,* 585 U. S. _____ (2018), p. 13.

50 *Whalen v. Roe*, 429 U.S. 589 (1977) dealt with obligations of health care providers to store the private information of patients who received prescriptions for drugs.

the Constitution.[51] Besides the interest in independence in making certain kinds of important decisions, the individual interest in avoiding disclosure of personal matters was identified.[52] In the following, the informational dimension of privacy was of broader relevance in *NASA v Nelson*, a case that dealt with NASA's background checks of contract employees.[53] The majority judgment chose to assume that a privacy interest of constitutional significance was at stake, but considering the legal safeguards, it concluded that there was no violation.[54] This line of reasoning was sharply criticized by the concurring opinions.[55] Their findings instead were that there is no constitutional right to "informational privacy".

Despite the recognition of different kinds of interests in the case law of the U.S. Supreme Court, "privacy" offers only limited, mostly accessory informational protection. Although some of the decisions address digital devices or advanced surveillance methods[56], there is little success in developing sophisticated concepts of the protection that is constitutionally guaranteed. As the grounds of the recent judgment *Dobbs v. Jackson Women Health Organization* may illustrate[57], the reasons for this have to do with the limits of the legal anchors and the methodological strategies. Catchphrases such as "dignity versus liberty"[58] cannot capture the entire background and would be an exaggeration.

---

51 *Carmel Shachar* and *Carleen Zubrzycki*, Informational Privacy After *Dobbs*, 75 Alabama Law Review 1, 12 ff. (2023).

52 *Whalen v. Roe*, 429 U.S. 589 (1977), at 598 f. See also, with partly different considerations, *Nixon v Administrator of General Services,* 433 U.S. 425(1977), at 457.

53 *NASA v. Nelson*, 562 U.S. 134 (2011).

54 A lot of questions remain unclear in the grounds, cf. *Christina P. Moniodis*, Moving from *Nixon* to *NASA*: Privacy´s second strand – A right to informational privacy, 15 Yale J. L. & Tech. 139, 157 ff. (2012).

55 Concurring opinion of Justice *Scalia*, joined by Justice *Thomas*.

56 See, for example, the reasoning in *United States v Jones*, 565 U.S. 400 (2012), in *Riley v California*, 573 U.S. 373 (2014), and in *Carpenter v United States,* 585 U. S. _____ (2018).

57 *Dobbs v. Jackson Women Health Organization*, judgment of June 24, 2022. The majority judgment emphasizes that the reasons for overruling *Roe v Wade* and *Planned Parenthood v Casey* are partly of substantial nature, but above all, it is the methodological approach that is being subjected to a fundamental criticism, with as yet not all impacts predictable. For the discussion see, for example, *Sam Kamin*, Katz and Dobbs: Imagining the Fourth Amendment Without a Right to Privacy. 101 Texas Law Review Online 80 (2022).

58 Cf. *James Q. Whitman*, The Two Western Cultures of Privacy: Dignity versus Liberty, 113 Yale L.J. 1151 (2004).

A more elaborated development of a constitutional right to privacy can be found in the case law of the Canadian Supreme Court. This is true although the guarantees this Court refers to – most notably Section 8 and also Section 7 of the Canadian Charter of Rights and Freedoms[59] – are quite similar to those in the U. S. The understanding of the Charter as a "purposive document"[60] whose spirit "must not be constrained by narrow legalistic classifications based on notions of property"[61] leads to an abstract and broad understanding of Section 8 in the sense of a "right to privacy"[62] that is shaped by the "underlying values of dignity, integrity and autonomy"[63]. The pattern of "reasonable expectations of privacy" has been essential for this understanding[64] and normatively assessed with a view to the "totality of circumstances"[65]. The approach is sufficiently flexible to allow a distinction to be made between "types of privacy interests – territorial, personal, and informational".[66] Informational privacy interests are then described primarily as interests in the confidentiality, non-disclosure, non-dissemination or individual control of information, especially but not only in case of intimate details on the individual's lifestyle and personal choices.[67] Recent judgments go further, differentiating privacy as secrecy, as control and as anonymity[68], and pointing to "informational self-determination".[69] Some cases give rise to the development of more

59 Section 8 states: "Everyone has the right to be secure against unreasonable search or seizure." Section 7 guarantees that "Everyone has the right to life, liberty and security of the person and the right not to be deprived thereof except in accordance with the principles of fundamental justice."

60 See the methodological considerations in *Hunter et al. v. Southam Inc.*, [1984] 2 S.C.R. 145, pp. 155 ff., 156 (for the citation).

61 *R. v. Dyment*, [1988] 2 S.C.R. 417, at 15.

62 See as a landmark decision *Hunter et al. v. Southam Inc.*, [1984] 2 S.C.R. 145, pp. 155 ff.

63 *R. v. Plant*, [1993] 3 S.C.R. 281.

64 *Hunter et al. v. Southam Inc.*, [1984] 2 S.C.R. 145, pp. 155 ff.; *R. v. Dyment*, [1988] 2 S.C.R. 417, at 15; *R. v. Plant*, [1993] 3 S.C.R. 281.

65 *R. v. Tessling*, 2004 SCC 67, at 31 ff.

66 *R. v. Spencer*, 2014 SCC 43, at 35; see also *R. v. Dyment*, [1988] 2 S.C.R. 417, at 19 ff.; *R. v. Tessling*, 2004 SCC 67, at 20 ff.

67 *R. v. Dyment*, [1988] 2 S.C.R. 417, at 31 ff.

68 *R. v. Spencer*, 2014 SCC 43, at 38.

69 *R. v. Jones*, 2017 SCC 60, at 39, quoting *R. v. Dyment* and the report of the Task Force, Privacy and Computers, 1972, p. 13, "all information about a person is in a fundamental way his own, for him to communicate or retain for himself as he sees fit". See also *R. v. Bykovets*, 2024 SCC 6, at 32. See further *R. v. Tessling*, 2004 SCC 67, at 23, quoting *Alan F. Westin*, Privacy and Freedom, 1970, p. 7: "the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent

specific considerations which reflect the characteristics of information. The landmark decision *R. v. Dyment* notes that if "the privacy of the individual is to be protected, we cannot afford to wait to vindicate it only after it has been violated."[70] It also highlights that "situations abound where the reasonable expectations of the individual that the information shall remain confidential to the persons to whom, and restricted to the purposes for which it is divulged, must be protected"[71], implying a pivotal role of purpose specification and purpose limitation in the processing of data and information. Cases on the Internet have led to a further differentiation of informational privacy in interests such as secrecy, control, or anonymity. The recent judgment *R. v. Bykovets* underlines that the subject matter of the protection revolves around information, not just data, and the dispute between majority opinion and dissents centers on the problem of determining the information content of IP addresses.[72] Nevertheless, the informational protection is repeatedly referred back to the underlying, albeit highly abstractly interpreted "protection against unreasonable search and seizure". All in all, specific patterns and limitations shape the "right to privacy" derived from Section 8 of the Canadian Charter of Rights and Freedoms, even if the Canadian Supreme Court goes considerably further in developing informational protection as compared to the U. S. Supreme Court.

The recognition of a constitutional right to privacy in the jurisprudence of the Supreme Court of India also provides some insight. The text of the Constitution of India does not explicitly mention "privacy". Nevertheless, following an open methodological approach, including "borrowing", the Supreme Court has derived a multi-layered and multi-dimensional right to privacy in its comprehensive *Puttaswamy-I*-verdict and reaffirmed this recognition in the *Puttaswamy-II* case.[73] Both judgments dealt with the constitutionality of the Aadhaar project, a centralized nation-wide identifi-

information about them is communicated to others". Cf. for the jurisdiction of the German FCC section C. II. of this article.

70 *R. v. Dyment*, [1988] 2 S.C.R. 417, at 23: "This is inherent in the notion of being *secure* against unreasonable searches and seizures."

71 *R. v. Dyment*, [1988] 2 S.C.R. 417, at 22, 29 ff. In this case, the appellant had a traffic accident. A doctor collected a vial of free-flowing blood for medical purposes without the appellant´s knowledge or consent. Later on, he handed the blood sample over to a police officer. The appellant was subsequently charged and convicted of impaired driving.

72 *R. v. Bykovets*, 2024 SCC 6.

73 *Justice K.S. Puttaswamy (Retd) vs Union Of India*, Judgment on 24 August 2017, Writ Petition (Civil) No 494 of 2012; (2017) 10 SCC 1; AIR 2017 SC 4161; and *Justice K.S.*

cation system based on biometric technology. The Court highlights that privacy "constitutes the foundation of all liberty" and "lies across the spectrum of protected freedoms".[74] In its conclusions, it anchors the right to privacy on a broad foundation: "Privacy is a constitutionally protected right which emerges primarily from the guarantee of life and personal liberty in Article 21 of the Constitution. Elements of privacy also arise in varying contexts from the other facets of freedom and dignity recognized and guaranteed by the fundamental rights contained in Part III."[75] Different strands are covered, among others, informational privacy.[76] It is in line with the multi-layered and broad approach that the right to privacy is not only conceptualized as a right of defense against encroachments. It also includes duties of the state and mandates it to "put in place a positive regime".[77] Since the Aadhaar project raises many questions that are genuine data protection issues beyond common notions of privacy, it is particularly interesting that the Court, after addressing the characteristics of data and information, notes that "apart from safeguarding privacy, data protection regimes seek to protect the autonomy of the individual [...] and the principle of non-discrimination".[78]

What shape does a right to privacy take when it is explicitly enshrined in constitutional codifications? Textually and systematically, it is usually placed in more traditional contexts of home, correspondence, or property as well as search and seizures. An example of this is Section 14 of the Bill of Rights in the Constitution of the Republic of South Africa, 1996.[79] However, the anchoring of the right to privacy in the form of a general term – in conjunction with doctrinal and methodological considerations – allows the Constitutional Court of South Africa to develop this right rela-

---

Puttaswamy (Retd) vs Union Of India, Judgment on 26 September 2018, AIR 2018 SC (SUPP) 1841, 2019 (1) SCC 1, (2018).

74 *Puttaswamy-I*, Part R (p. 243, 244).

75 *Puttaswamy-I*, Part T (p. 266). Already in earlier case law, the right to life enshrined in Article 21 of the Constitution has been interpreted as a basic right to a decent existence. Cf. also regarding the jurisdiction of the Supreme Court of Pakistan *Aftab* (n 25), 99 ff.

76 See *Puttaswamy-I*, Part S (p. 246 ff.).

77 *Puttaswamy-II*, Part G (p. 232); cf. also *Puttaswamy-I*, Part S (p. 254).

78 *Puttaswamy-I*, Part S (p. 246 ff., 252).

79 Section 14 of the Bill of Rights provides that everyone has the right to privacy, which includes the right not to have (a) their person or home searched; (b) their property searched; (c) their possessions seized; or (d) the privacy of their communications infringed.

tively independently. The Court underlines the interrelationships between privacy, dignity, autonomy, and equality as well as, in some cases, other freedom rights that are also affected, for example the rights to freedom of expression and the media.[80] Nevertheless, "privacy" implies certain patterns of thought, such as the juxtaposition of privacy and publicity, the differentiation of more or less personal realms, or the emphasis on an individual right to decide on disclosure. To a certain extent, such thinking patterns are also at work when it comes to issues of protection of personal data.[81]

Art. 8 of the European Convention on Human Rights (ECHR) expressly provides for the right of everyone to respect for his or her private life and correspondence.[82] Since the European Court of Human Rights (ECtHR) sees itself as the pivotal European court in the field of international law and as part of a network between the signatory states' and the European courts within which these courts and their decisions increasingly interact[83], it has moved away from the traditional understanding of the ECHR in terms of international minimum standards. According to its case law, Art. 8 ECHR protects a broad spectrum of interests. Besides the protection of personal activities, decisions or spatial areas, which always included social relationships and public activities to a certain extent, protection was gradually developed with regard to the handling of personal information and data. The initial judgments dealt with traditional cases of phone surveillance

80 Cf. *Amabhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others; Minister of Police v Amabhungane Centre for Investigative Journalism NPC and Others* (CCT 278, 279/19) [2021] ZACC 3, at 112 ff.

81 Cf. the judgments *Bernstein and Others v Bester NO and Others* (CCT 23/95) [1996] ZACC 2, at 56 ff.; *NM and Others v Smith and Others* (CCT 69/05) [2007] ZACC 6, at 32 ff.; *Amabhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others; Minister of Police v Amabhungane Centre for Investigative Journalism NPC and Others* (CCT 278, 279/19) [2021] ZACC 3, at 23 ff.

82 "Everyone has the right to respect for his private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

83 *Marion Albers*, Höchstrichterliche Rechtsfindung und Auslegung gerichtlicher Entscheidungen, in: Grundsatzfragen der Rechtsetzung und Rechtsfindung, VVDStRL Bd. 71, 2012, 257 (272 ff., 287 ff.).

and, thus, the right to respect for correspondence. In such cases, first guidelines were developed, for example that business connections are covered by protection if reasonable expectations of privacy protection can be recognized, or that an impairment does not depend on whether and to what extent recordings are subsequently used or whether concrete disadvantages have arisen – an argumentation pattern that has always existed in cases of telecommunications surveillance as typifying approach. The informational protection of the right to respect for the "private life" was to some extent based on these initial guidelines, not least because the data processing steps that followed the interception were subsumed under this right.[84] The protection extends to data that originates within a private sphere. To a certain extent, it can also cover data that is publicly accessible, for example, in the event of systematic collection and storage by public authorities, or in the case of a compilation, use or other form of processing of personal data that the data subject would not reasonably expect. In the subsequent case law, the focus has increasingly shifted from the private sphere as the source of the data to its informational content. A wide range of data has been classified as belonging to private life, such as tax data, medical data and information or the IP address, but also photos and video recordings or DNA samples as data carriers.[85] Data processing steps are differentiated and, if necessary, independently assessed as an intrusion.[86] In principle, the Court upholds the presumption that the collection, recording, use or publication of private life can constitute an impairment, regardless of whether the data is sensitive or whether the data subject has suffered specific disadvantages.[87] However, potentially detrimental consequences do play

84 Cf. ECtHR, No. 27798/95, 16.2.2000 – *Amann*, Rn. 44 ff., 64 ff.

85 Cf. ECtHR, No. 20383/04, 12.12.2013 – *Khmel*, Rn. 41 ff., 49; No. 931/13, 27.6.2017 – *Satakunnan*, Rn. 133 ff.; No. 66490/09, 27.2.2018, - *Mockutė*, Rn. 93 f.; No. 62357/14, 24.4.2018 – *Benedik*, Rn. 100 ff., 107 ff.; No. 50001/12, 30.1.2020 – *Breyer*, Rn. 76 ff.; No. 75229/10, 14.4.2020 – *Dragan Petrović*, Rn. 69, 79.

86 ECtHR, No. 20383/04, 12.12.2013 – *Khmel*, Rn. 40 ff.; No. 42788/06, 26.1.2017 – *Surikov*, Rn. 75, 84 ff.; No. 931/13, 27.6.2017 – *Satakunnan*, Rn. 134 ff.

87 ECtHR, No. 28 341/95, 4.5.2000 – *Rotaru*, Rn. 42 ff.; No. 44 647/98, 28.1.2003 – *Peck*, Rn. 57 ff.; No. 62 332/00, 6.6.2006 – *Segerstedt-Wiberg*, Rn. 69 ff.; No. 30 562/04, 4.12.2008 – *S. and Marper*, Rn. 58 ff.; No. 11519/20, 4.7.2023 – *Glukhin*, Rn. 67 ff. See also for a legal obligation of Telegram to decrypt Internet communications if they are encrypted No. 33696/19, 13.2.2024 – *Podchasov*, Rn. 58.

a role in the overall assessment of protection.[88] When such effects are taken into account, other freedoms may become relevant as well, for example the freedom of expression.[89]

The ECtHR specifies more detailed requirements for the necessary legal basis in a very differentiated manner, depending on the context and dimension of protection, while recognizing the more or less far-reaching margin of appreciation of the signatory states. For example, state surveillance measures, especially if they are secret at certain stages, require a series of coordinated minimum legal precautions.[90] And the state does not adequately fulfill its duty to protect unless it ensures respect for private life among private individuals by creating a legal framework that takes account of the different protection interests in a particular context.[91] Art. 8 ECHR can also provide (limited) rights of knowledge, such as the right to information or access to files with regard to personal data or documents held by the authorities.[92]

3. Achievements and weaknesses of privacy as protected interest

Irrespective of whether the constitutional protection of (respect for) privacy is explicitly enshrined or derived from other fundamental rights, its long tradition as an idea makes it easier to address it as a subject matter of fundamental rights protection at different levels and in different contexts. How this is done in detail depends on the legal system and culture, as well as on the role and self-understanding of the courts, and not only on substantive, but also on doctrinal and methodological considerations. Nevertheless, some achievements and weaknesses of privacy as protected interest when it comes to constitutionalizing the protection of personal data can be identified which emerge as issues across jurisdictions.

88 ECtHR, No. 931/13, 27.6.2017 – *Satakunnan*, Rn. 137; No. 50001/12, 30.1.2020 – *Breyer*, Rn. 74 ff.; No. 11519/20, 4.7.2023 – *Glukhin*, Rn. 65 ff.; No. 33696/19, 13.2.2024 – *Podchasov*, Rn. 51 ff.

89 See ECtHR, Nos. 58170/13, 62322/14 and 24960/15, 25.5.2021 – *Big Brother Watch*, Rn. 442 ff.

90 ECtHR, No. 47143/06, 4.12.2015 – *Zakharov*, Rn. 228 ff., Nos. 58170/13, 62322/14 and 24960/15, 25.5.2021 – *Big Brother Watch*, Rn. 322 ff.; No. 33696/19, 13.2.2024 – *Podchasov*, Rn. 63 ff.

91 Cf. ECtHR, No. 61496/08, 5.9.2017 – *Bărbulescu*, Rn. 115, 120 ff.

92 ECtHR, No. 10 454/83, 7.7.1989 – *Gaskin*, Rn. 37; No. 62 332/00, 6.6.2006 – *Segerstedt-Wiberg*, Rn. 99 ff.

In terms of content, it is a particular achievement that the right to (respect for) privacy can be applied to very different and wide-ranging subject matters of protection. On the one hand, this is due to its level of abstraction. In line with the basic dichotomies that have shaped the traditional understanding of privacy, some lines of reasoning take a very fundamental approach by emphasizing that privacy is a crucial value for a liberal society and, in the sense of a pre-condition, essential for the exercise of other freedoms.[93] On the other hand, the concept of a private "sphere" can cover different facets of protection, for example, personal decisions, particular spatial areas, and also the content of conversations or data that arise in or can be attributed to that private sphere. As we have seen: "Privacy" assigns something to a person or a group of people as their own concern and sets limits on others' access to it. The attribution already made in the concept – in particular: of data to the individual[94] – reduces the burden of giving reasons for protection needs. Just as the protected interests do not have to be specified in detail, it is not necessary to specify impairments and to break down precisely to what extent the person in question is actually exposed to disadvantages. As we have seen, the ECtHR even emphasizes that an impairment does not depend on whether concrete disadvantages have arisen. The data subject as fundamental right's holder has a protected negative-liberty-status based on the principle of non-interference in the private sphere, which can be applied to various forms of intrusions, including the acquisition of data, information and knowledge about the right-holder. Such an approach does not need to be more closely aligned with the characteristics of this particular subject matter to which the protection is extended. Provided that more detailed aspects of protection or of impairments are addressed, particularly in the balancing of interests, interdependencies between the protection of personal data and freedoms of decisions or behavior that might be protected by specific fundamental

93 See, for example, the Supreme Court of Canada, *R. v. Dyment*, [1988] 2 S.C.R. 417, at 17 (quoting *Alan F. Westin*, Privacy and Freedom, 1970, p. 349 f.): "[…] society has come to realize that privacy is at the heart of liberty in a modern state […] Grounded in man's physical and moral autonomy, privacy is essential for the well-being of the individual."; and the Supreme Court of India, *Puttaswamy-I*, Part R (p. 243, 244).

94 Cf. the dissent of Justice *Gorsuch*, *Carpenter v United States,* 585 U. S. ____ (2018), p. 13, with the proposal to revisit the "kind of legal interest" that "is sufficient to make something *yours*".

rights show up.[95] In this sense, the right to privacy always points beyond itself.

Following traditional patterns for the development and justification of the protection of personal data has its disadvantages as well. Insofar as some courts, due to their doctrinal and methodological approach, are rather reluctant to make more extensive interpretations, the protection with regard to the handling of data and information is understood as an extension and more or less accessory to traditionally protected freedoms or at best one facet of protection among others. It is not explicitly information- and data-oriented but rather based on the assumption that data shares the privacy of the personal sphere from which they originate. Consequently, it is more or less designed as a sphere-related "defense formula". Difficulties arise already, if data acquires an informational content that calls for protection only in the context of its further processing or use, for example, through the linking of data or additional knowledge. The paradigm of a private sphere directs attention primarily to the collection of data (as an intrusion into the personal sphere) and the requirements for its justification, for example a search warrant. The subsequent data processing steps receive only limited attention and are not appropriately assessed in terms of their own potentially detrimental consequences. Insofar as other courts understand their role to be an active one and the relevant codification in the sense of a "living constitution", they arrive at very sophisticated multi-layered and multi-dimensional conceptions, which also set a demanding task for the legislator. While the lines of reasoning are problem-oriented, they may be criticized for not being sufficiently grounded in the provisions, especially since the concept of privacy itself is under constant criticism.[96] In addition, to some extent, traditional patterns of thought still have an impact on the conceptions. The focus on "privacy" runs the risk of failing to adequately develop the protected interests of data subjects and data protection law. References to informational self-determination, such as we find in some of the court decisions, are not surprising.

At this point we can move on to the right of personality and the right to informational self-determination. In the jurisprudence of the German

95 For example: Constitutional Court of South Africa, *Amabhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others; Minister of Police v Amabhungane Centre for Investigative Journalism NPC and Others* (CCT 278, 279/19) [2021] ZACC 3, at 112 ff.; ECtHR, Nos. 58170/13, 62322/14 and 24960/15, 25.5.2021 – *Big Brother Watch*, Rn. 442 ff.

96 See, for example, *Jeffrey Belley*, Pure Privacy, 116 Nw. U. L Rev. 463 (2021).

Federal Constitutional Court, this right has been developed not least in response to the weaknesses of the formerly recognized right to respect for privacy. It is tailored to the purpose of providing protection to the individual with regard to the handling of personal data and information.

II. Right to personality and informational self-determination

German law is famous for the development of a protected interest that has attracted worldwide attention: "informational self-determination". I would prefer to call it "informational autonomy" because "informational self-determination" is just a poor translation. However, this term is established and therefore, I will stick to it.

1. Approaches and developments in case law

The Federal Constitutional Court derived the "right to informational self-determination" from Art. 2 (1) in conjunction with Art. 1 (1) of the Basic Law[97] in its decision concerning the census (*Volkszählungsurteil*) taken in 1983.[98] The wording of these fundamental rights does not explicitly provide for a "right to informational self-determination". Instead, it refers to the protection of the free development of one's personality and to the inviolability of human dignity.

In our context, it is of particular interest that Art. 2 (1) in conjunction with Art. 1 (1) of the Basic Law have long been interpreted in the case law of the Federal Constitutional Court primarily as a "right to respect for privacy". Scholarly contributions and an inspirational glance at American case law have contributed to the derivation of this right. In its early case law, the Federal Constitutional Court originally conceived "privacy" employing the spatial imagery of areas of retreat walled off from the outside world or situations for interaction and communication which are to remain, in principle, free of undesired inspection. Subsequently, issues were included that are typically classified as "private" due to their information content. As a result, the right to respect for privacy has covered many constellations:

97 Article 2 GG: "Everybody shall have the right to the free development of his or her personality [...]"; Article 1 GG: "Human dignity shall be inviolable. To respect and to protect it shall be the duty of all state authority."

98 Decisions of the FCC, Vol. 65, 1.

the protection of medical files stored at the doctor's workplace from access by security authorities,[99] the use of secret tape recordings in a civil court proceeding,[100] the publishing of a fictitious interview about private matters in the press,[101] or a television movie about a murder in which the criminal, who has since been released, can be identified (the famous *Lebach*-case)[102].

But then the *Eppler*-case resulted in a turning point.[103] In this case of an alleged public statement on a public matter, the FCC reached the conclusion that "the right to respect for privacy" was not a suitable approach to grasp the problems of the case appropriately. Instead, the "general right of personality" was derived from Art. 2 (1) in conjunction with Art. 1 (1) of the Basic Law.[104] This development is facilitated by the fact that the wording of Article 2 (1) of the Basic Law promises everyone the right to freely develop their personality. In the *Eppler*-decision, the Court held that, in principle, individuals should be able to decide for themselves how they wish to present themselves to third parties or to the public, and whether and to what extent third parties may dispose of their personality.[105] Although the case was about statements falsely attributed to one's person, this description of the scope of protection has been understood as if the general right of personality provided a right that people see you the way you want to be seen. This paved the way for the right to informational self-determination.

According to the *Census*-judgment, the right to informational self-determination confers on the individual the authority to, in principle, determine for himself or herself the disclosure and use of his or her personal data.[106] Individuals have the right to decide themselves whether and how their personal data is to be revealed and used, in other words: a right to self-determination about processing of data relating to them. How did the Federal Constitutional Court arrive at this subject matter to be protected? An analysis of the broader background, previous case law and scientific

99 Decisions of the FCC, Vol. 32, 373; Vol. 44, 353.
100 Decisions of the FCC, Vol. 44, 238.
101 Decisions of the FCC, Vol. 34, 269 – *Soraya*.
102 Decisions of the FCC, Vol. 35, 202 – *Lebach*.
103 Decisions of the FCC, Vol. 54, 148 – *Eppler*. Erhard Eppler, a well-known member of the Social Democratic Party of Germany, was blamed for making a public statement on a public matter which he proved he had not made in this way and requested injunctive relief.
104 Decisions of the FCC, Vol. 54, 148, 153 ff.
105 Decisions of the FCC, Vol. 54, 148, 155.
106 Decisions of the FCC, Vol. 65, 1, 43. Analyzing the decision and its background *Marion Albers*, Informationelle Selbstbestimmung, 2005, 151 ff.

debate can explain this very well. The precursor of the right to informational self-determination, the right to respect for privacy, drew the same criticism in Germany as it did in the U.S.-American privacy debate. The first point of criticism emphasized the relativity of the sphere of personal privacy: it could be described only in terms "relative" to those receiving information.[107] Therefore, what was to be protected was not a predetermined sphere, but the capacity of the individual to decide to whom to disclose which information. Alan Westin formulated this idea in these terms as early as 1972.[108] The second point of criticism highlighted the fact that the need for protection was less about the private sphere as the context in which certain data emerges but rather about which information could be derived from data obtained and how that information could be used.[109] In other words, what is decisive is not the context data originates from but rather the context in which the information is used. The Federal Constitutional Court responded to these central points of criticism by developing a right with a scope of protection which centers on individual decision capacities as well as on the context of use of personal data.[110] It also took up the acknowledged constitutionally protected goods of autonomy and freedom of decision and action, arguing as follows: free decision and action are possible only under certain circumstances. If people are unsure whether deviating behaviors may be stored as information and used to their disadvantage, they will try not to attract attention by such behavior and are no longer free to act at will.[111] That is why the protection of fundamental rights must cover the protection against information and data processing by the state. The Federal Constitutional Court concluded that, just as people can decide about their actions, they also have the right to determine how "their"

107 See *Bernhard Schlink*, Das Recht der informationellen Selbstbestimmung, Der Staat 25 (1986), 233, 242; *Daniel Solove*, The digital person, 2004, 212 f.

108 *Alan F. Westin*, Privacy and Freedom, 6th ed. 1970, p. 42.

109 See *Spiros Simitis*, Chancen und Gefahren der elektronischen Datenverarbeitung, NJW 1971, 673, 680.

110 For literary sources of the Court´s decision see *Hermann Heußner* (former judge at the FCC preparing the Census Decision), Das informationelle Selbstbestimmungsrecht in der Rechtsprechung des Bundesverfassungsgerichts, Die Sozialgerichtsbarkeit (SGb) 1984, 279, 280 f. Amongst others, the ideas of *Westin* have been received by the members of the Court, see *Ernst Benda* (former President of the FCC participating at the Census Decision), Privatsphäre und "Persönlichkeitsprofil". Ein Beitrag zur Datenschutzdiskussion, in: Leibholz, Faller, Mikat and Reis (eds.), Menschenwürde und freiheitliche Rechtsordnung, 1974, 23, 32.

111 Decisions of the FCC, Vol. 65, 1, 43.

personal data will be processed. The protected persons also have the right to know by whom and for what purposes personal data referring to them are processed[112], but that right is accessory in the context of the concept.

In the course of its case law, the FCC has developed a multitude of requirements statutory law has to comply with. These include the principles of purpose specification and purpose limitation, thresholds for the permissibility of data processing steps, or data security standards. Particular requirements can usually be traced back to the challenges raised by the case. The doctrinal reference point is often the principle of proportionality, although it may not be the most appropriate reference point for some requirements.

In the aforementioned version of a right of individuals to decide whether and how "their" personal data is to be disclosed and used, the right to informational self-determination was quite firmly established for a long time. But meanwhile, this version is in flux. It already has been modified to a certain extent. The FCC has thus reacted to scholarly criticism as well as to changes in its own case law on the right to respect for privacy and the general right of personality.[113] For instance, the Court clarified in its *Caroline I*-judgment that "[…] the general right of personality does not confer to the individual the right to be portrayed by others only as he or she views him- or herself or only as he or she wants to be perceived […] Such a broad protection would not only exceed the aim of protection, i.e. to avoid risks to the development of an individual's personality, but would also extend far into third parties' sphere of freedom."[114] Thereby a pattern of argumentation has been abandoned that contributed to the definition of the scope of protection of the right to informational self-determination.[115] In relation to the state, the problem has arisen in cases such as electronic profiling and searches or automatic license plate recognition that personal data is collected but quickly automatically sorted out and deleted, raising the question of whether this is relevant to the scope of protection and may amount to an encroachment. In such cases, the Court has partially modified the protective functions and the scope of protection of the right to informa-

112 Decisions of the FCC, Vol. 65, 1, 46.

113 For these changes see Decisions of the FCC, Vol. 97, 125, 146 ff.; 97, 391, 403 ff.; 101, 361, 382; 120, 180, 199.

114 FCC, Judgment of 15 December 1999, 1 BvR 653/96 – *Caroline I*, para. 70, https://www.bverfg.de/e/rs19991215_1bvr065396en.html.

115 Cf. *Marion Albers,* Grundrechtsschutz der Privatheit, DVBl 2010, 1061, 1065 f.

tional self-determination in a more or less well thought-out manner.[116] In the *Right to be Forgotten I*-Judgment of 2019, the Court has undertaken significant changes: Between private parties[117], the right to informational self-determination provides the individual "the possibility of influencing, in nuanced ways, the context and manner in which their data is accessible to and can be used by others, thus affording the individual considerable influence in deciding what information is available on them"[118]. Further elaboration of the right to informational self-determination continues to progress.

2. Achievements and limitations of informational self-determination as protected interest

The right to informational self-determination reaches far beyond the classical understanding of the right to respect for privacy. Its core element is a relatively abstract individual right to make decisions ranging from disclosure of data to their processing and to their use. This scope of protection is characterized by an approach that places the handling of personal data and information as such at the center of attention. The protection provided is no longer derived from and no longer dependent on otherwise protected interests – such as "privacy" – that have particular definitions and delimitations. It is an area in its own right. This opens up the possibility that the protection is being tailored appropriately to the subject matter. The protection directly aimed at the handling of personal data and information and the possible extension to a wide range of protection requirements that already exist or may arise in the future are an important step forward that the right to informational self-determination has brought.

116 See Decisions of the FCC, Vol. 115, 320, 342 ff.; 120, 378, 398; 150, 244, Rn. 41 ff.

117 The relationship between private parties is covered by fundamental rights via acknowledged third-party effects ("Drittwirkung"), however, an individual right to decide on the disclosure and use of personal data has always created substantial and doctrinal problems. See *Laura Schertel Mendes*, Schutz vor Informationsrisiken und Gewährleistung einer gehaltvollen Zustimmung, 2015, 44 ff. Cf. also for the doctrine of the "Drittwirkung" *Marion Albers*, L'effet horizontal des droits fondamentaux dans le cadre d'une conception à multi-niveaux, in: Hochmann and Reinhardt (eds.), L'effet horizontal des droits fondamentaux, 2018, 177 ff.

118 FCC, Order of 6. November 2019, 1 BvR 16/13 – *Recht auf Vergessen I*, Headnote 3 and Rn. 83 ff., https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2019/11/rs20191106_1bvr001613en.html.

Despite these achievements of the novel approach to protection requirements, there are shortcomings in the FCC's definition of the scope of protection. As explained, the approach opens up the possibility that the protection is being tailored appropriately to the subject matter. But this is precisely what the Court fails to do. The Court adheres to traditional patterns of thought with regard to both content and doctrine. In terms of content, the Court is guided by the familiar patterns used to describe freedom of decision and action, or property rights. After all, these patterns of free decision and action have been referred to in the argumentation of the census judgment's grounds in order to support the development of the right to informational self-determination. Additionally, even though the right to informational self-determination is derived from the right to the free development of personality and from human dignity, its scope of protection is to a certain extent shaped likewise a property right.[119] Similar to some U. S.-American conceptions of privacy, informational self-determination is primarily thought of as a right of control over personal data.[120] Such an approach does not do justice to the distinct categoriality and characteristics of data, information and knowledge. It entails ontic ideas, as if data or even information were a kind of ball that can be held or passed on and that does not change in the process. It is no coincidence that the scope of protection of "informational" self-determination relates to data, not information. The fact that others, be they government agencies or private individuals, are structurally involved with their own activities of interpreting, processing and creating constantly changing data and information is lost. In terms of doctrine, the Court is guided by the familiar patterns of protection against encroachments. That means that the fundamental right's scope of protection is interpreted as safeguarding individual freedom (traditionally understood in a liberal way) against any impairments unless they are covered by statutory provisions which meet the principle of the clarity and

119 Sometimes it is emphasized that the FCC also stated: "The individual does not have a right in the sense of an absolute, unlimitable mastery over 'his/her' data; he/she is rather a personality that develops within a social community and is dependent upon communication", Decisions of the FCC, Vol. 65, 1, 43, 46. However, these grounds refer to the reservation allowing to limit the scope of protection by means of statutory rules. They do not alter the shaping of the scope of protection.

120 The ideas of *Alan F. Westin*, Privacy and Freedom, 6th ed. 1970, 42, which the FCC adopted, have also been cited in some rulings of the Canadian Supreme Court. See also *Charles Fried*, Privacy, 77 Yale Law Journal 475, 482, 483 (1968): "Privacy […] is the *control* we have over information about ourselves […] is control over knowledge about oneself."

certainty, the principle of proportionality, and all other relevant constitutional requirements. This doctrinal approach results in specific forms of describing the subject matters or interests which are to be protected by fundamental rights as well as in specific functions and features regarding the statutory provisions. In particular, the idea is lost that an appropriate regulation of the handling of personal information and data must be multilayered as well as manifold and requires a multitude of regulatory tools.

The right to informational self-determination is quite popular in other countries' jurisdictions, as well as in the international scientific community. But we must be aware that the FCC has meanwhile revised its approach, only to a limited extent in the state-citizen relationship, but significantly in the relations between private individuals. The description of the scope of protection in these relations has been left rather vague and the sharp distinction between the statements on the state-citizen relationships and those on the relations between private parties reveals an overly traditional understanding of the state. The interplay with the Charter of Fundamental Rights of the European Union, which is not only based on factual influences, but is meanwhile also doctrinally justified[121], opens up opportunities for the necessary further development of fundamental rights.

III. Right to the protection of personal data

Aiming at being a modern charter covering contemporary challenges, Art. 8(1) of the Charter of Fundamental Rights of the European Union (CFR) offers everyone a specific right to the protection of personal data concerning him or her.[122] Art. 8(2) and (3) CFR point in part to the possibility of shaping or restricting the fundamental right via statutory regulations and in part contain guidelines for such regulations.[123] The explicit

121 Cf. *Albers* (n 83), 287 ff.

122 Art. 8(1) CFR states: "Everyone has the right to the protection of personal data concerning him or her." The right to the protection of personal data concerning him or her is also anchored in Art. 16(1) TFEU. The difficulties in reconciling Art. 16(1) TFEU, Artt. 8, 52(1) and 52(2) CFR can be resolved by a teleological reduction of Art. 52(2) CFR. Cf. ECJ (Grand Chamber) of 26 July 2017, Opinion 1/15, *PNR*, Rn. 120.

123 These sections read: "(2) Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been

enshrinement of a right to the protection of personal data has been the model for the new similar anchor in Art. 5 LXXIX of the Constitution of the Federative Republic of Brazil.[124] Art. 8(1) CFR stands alongside the protection of Art. 7(1) CFR, the right to respect for private and family life, home and communications. Does that novel fundamental right advance the constitutional landscape and offer answers to the question of how to unfold the protected interests of data subjects?

1. Approaches and developments in case law

In its initial decisions, the ECJ stated that Art. 8 CFR was "closely linked" to Art. 7 CFR[125], and did not differentiate in more detail between the two fundamental rights.[126] Specific difficulties in distinguishing between the scope of protection of Art. 7 CFR on the one hand and Art. 8 CFR on the other arise for doctrinal reasons: Art. 52(3) CFR grants the rights of the Charter the same meaning and scope as the corresponding Convention rights and Art. 7(1) CFR corresponds to Art. 8(1) ECHR which is the foundation of data protection in the case law of the ECtHR. It was the landmark *Tele2 Sverige*-judgment that partially addressed this problem and at least emphasized the distinct nature of Art. 8 CFR. As long as the European Union has not acceded to the ECHR, the ECJ explains, that "Art. 52(3) CFR does not preclude Union law from providing protection that is more extensive than the ECHR" and that Art. 8 CFR "concerns a fundamental

collected concerning him or her, and the right to have it rectified. (3) Compliance with these rules shall be subject to control by an independent authority."

124 According to the amendment of this article in 2022, "under the terms of the law, the right to protection of personal data is ensured, including in digital media". See for the preceding development until the landmark ruling of the Brazilian Supreme Court in May 7, 2020, that paved the way for Congress to pass the constitutional amendment *Ingo Sarlet*, The Protection of Personality in the Digital Environment, in: Albers and Sarlet (n 2), 133 (137 ff.).

125 ECJ, Judgment (Grand Chamber) of 9.11.2010, C-92, 93/09, *Schecke*, Rn. 47.

126 See ECJ, Judgment (Grand Chamber) of 9.11.2010, C-92, 93/09, *Schecke*, Rn. 45 ff.; Judgment (Grand Chamber) of 24.11.2011, Rs. C-468, 469/10, *ASNEF/FECEMD*, Rn. 41 ff. For more in-depth analyses of earlier case law *Paul De Hert* and *Serge Gutwirth*, Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action, in: Gutwirth et. al. (eds.), Reinventing Data Protection?, 2009, 29 ff.

right which is distinct from that enshrined in Article 7 of the Charter and which has no equivalent in the ECHR".[127]

However, the Court's interpretation of the scope of protection under Art. 8 CFR does not provide much substance. The *Digital Rights Ireland*-judgment indicates that Art. 7 CFR protects private life in a substantive sense, while Art. 8 CFR focuses on the processing of personal data in a way that is not limited to private life and sets its own requirements, for example, in terms of data security or in terms of protecting personal data against the risk of abuse and against any unlawful access and use.[128] The constituent elements of Art 8(1) CFR are "personal data" and their processing, irrespective of whether the information that can be obtained from the data is of sensitive nature or whether any detrimental effects have been suffered.[129] Data processing phases are differentiated and assessed separately – not in isolation, however, but as relatively independent elements of a processing sequence.[130] In a closer context, the protected interests of data subjects are occasionally specified, such as the need for protection against comprehensive profiling or constant surveillance, against expectation-mediated constraints on actually protected behavior, against the undermining of professional secrecy or informant protection, or against data misuse.[131] When developing these protected interests, the ECJ takes into account other fundamental rights of the European Charter as well as interests protected under secondary or national law.[132] This is quite convincing if we associate Art. 8 CFR with a bundle of protected interests

127 ECJ, Judgment (Grand Chamber) of 21.12.2016, C-203/15 u. C-698/15, *Tele2 Sverige*, Rn. 129.

128 ECJ, Judgment (Grand Chamber) of 8 April 2014, C-293/12 and C-594/12, *Digital Rights Ireland Ltd*, Rn. 29 f., 40, 54.

129 ECJ, Judgment (Grand Chamber) of 6 October 2020, C-511, 512 u. 520/18, *Quadrature du Net*, Rn. 115; Judgment (Grand Chamber) of 6 October 2020, C-623/17, *Privacy International*, Rn. 70.

130 ECJ, Judgment (Grand Chamber) of 8 April 2014, C-293/12 and C-594/12, *Digital Rights Ireland Ltd*, Rn. 34 f.; Judgment (Grand Chamber) of 24 September 2019, *GC and Others*, C-136/17, Rn. 36; Judgment (Grand Chamber) of 21 March 2024, *RL*, C-61/22, Rn. 70 ff.

131 Cf. ECJ, Judgment (Grand Chamber) of 13 May 2014, *Google Spain,* C-131/12, Rn. 80; Judgment (Grand Chamber) of 24 September 2019, *GC and Others*, C-136/17, Rn. 36; Judgment (Grand Chamber) of 6 October 2020, C-511, 512 u. 520/18, *Quadrature du Net*, Rn. 106 ff.; Judgment (Grand Chamber) of 6 October 2020, C-623/17, *Privacy International*, Rn. 50 ff.

132 See ECJ, Judgment (Grand Chamber) of 6 October 2015, *Schrems I*, C-362/14, Rn. 72; Judgment (Grand Chamber) of 6 October 2020, C-511, 512 u. 520/18,

and with requirements that are first and foremost directed at legislation, which must consistently develop an appropriate data protection regime and coordinate it with other legal regimes. It is in line with this approach that the ECJ recognizes different dimensions of protection, i.e. besides rights of defense against encroachments also duties to protect or, not quite clearly, an indirect horizontal effect in the relationship between private individuals.[133]

Where appropriate, the ECJ points to the provisions of Article 8 (2) and (3) of the CFR for guidelines. In addition, it bases many requirements on the principle of proportionality, from which it takes a limitation of the restrictions on the protection of personal data "to what is absolutely necessary"[134] – a catchword from which a range of different precautions to be defined in the event of restrictions is then developed in a not necessarily stringent deduction. The requirements and precautions range from system design provisions and thresholds for the respective processing phase, to reservations for judicial review, or data security requirements, to the right of notification in case of intervention.[135]

The case law of the ECJ thus reveals a multi-dimensional and multi-faceted conception of the statements of Art. 8 CFR, without these already being substantively and doctrinally established. However, a coherent concept cannot be expected either. Not only does the ECJ often remain apodictic in its reasons for its decisions against the background of the different legal cultures in the Member States, but it also cannot take on a role that is completely centralized and hierarchical. There is a need for interplays between the courts in the multi-level system. This is due to the fact that the statements of the fundamental right to the protection of personal data need to be contextualized as soon as we seek to fill it with substance.

Quadrature du Net, Rn. 87 ff.; Judgment (Grand Chamber) of 6 October 2020, C-623/17, *Privacy International*, Rn. 30 ff.

133 For the problem of horizontal effects see *Jörn Reinhardt*, Realizing the Fundamental Right to Data Protection in a Digitized Society, in: Albers and Sarlet (n 2), 55 (58 ff.).

134 Settled case law, for example, ECJ, Judgment (Grand Chamber) of 2 March 2021, C-746/18, *H. K.*, Rn. 38 ff.

135 ECJ, Judgment (Grand Chamber) of 8 April 2014, C-293/12 and C-594/12, *Digital Rights Ireland Ltd*, Rn. 53 ff., 68; Judgment (Grand Chamber) of 6 October 2015, C-362/14, *Schrems I*, Rn. 91 ff.; Judgment (Grand Chamber) of 24 September 2019, *GC and Others*, C-136/17, Rn. 49 ff.; Judgment (Grand Chamber) of 6 October 2020, C-511, 512 u. 520/18, *Quadrature du Net*, Rn. 105 ff.; Judgment (Grand Chamber) of 2 March 2021, C-746/18, *H. K.*, Rn. 51 ff.; Judgment (Grand Chamber) of 21 March 2024, *RL*, C-61/22, Rn. 75 ff.

2. Achievements and challenges of the right to the protection of personal data as protected interest

The right to the protection of personal data places the handling of data and information at the center of its scope of protection. As a novel right that responds to the challenges of modern society, it is hardly surprising that it has triggered extensive debates among the legal community. Since these debates are to some extent guided by substantial and doctrinal preconceptions that differ from one Member State to another, they vary and diverge quite widely.

On the basis of the previous analysis, it can be stated that the right to the protection of personal data anchored in Art. 8 CFR is a relatively independent right and not exhausted by a reference to the protection of the respect for private life provided by Art. 7 CFR. It is also not analogous to the right to informational self-determination. It is not based on the idea of control as an underlying concept and does not provide blanket protection for "control over one's own data". Nor is it primarily to be understood as a prohibitive right. On the contrary, it is formulated in such a way that it allows us to move away from the traditional substantive and doctrinal patterns of thought and to break new ground. As a right to protection, Art. 8(1) CFR can be developed multifariously, as is also shown by paras. 2 and 3. It points to the need for shaping and the multifunctional role of legislation, but also to the role of those involved in its implementation. Although it is true, that existing secondary data protection legislation has played a certain role in the genesis of the right to the protection of personal data[136], its references to legislation need to be understood dynamically. It is suitable for initializing a complex legal framework that is also designed to be constantly adapted.

However, Art. 8 CFR remains relatively vague in terms of the protected interests. Its wording merely points to the individual's right to the protection of personal data concerning him or her and offers some more or less eclectic guidelines in para. 2 and 3. The vagueness of the guidelines, together with the fact that activities are shifting increasingly to the Internet and conflicts are becoming datafied, is leading to an ever-expanding scope of protection in case law. Against this background, the right to the protection of personal data has a tendency to turn into a "super-fundamental

136 Cf. the Explanations on Art. 8, Explanations relating to the Charter of Fundamental Rights, 14 December 2007, O. J. C 303/17.

right" within the realm of a "law of everything"[137]. To avoid this, there have been numerous attempts by jurisprudence and scholarship to clarify what exactly is meant by data protection and what the right to the protection of personal data aims to achieve in contrast to other rights. If, for example, Art. 7 CFR is interpreted in the case law of the ECJ as protecting private life in a substantive sense, while Art. 8 CFR focuses on data security or risks of unlawful access and abuse of personal data, or if the right to the protection of personal data is conceptualized as a procedural right, solutions are sought in a functional combination of both rights. But this combination is usually conceived as an additive juxtaposition. Such an additive juxtaposition is not feasible and falls short because it does not succeed in convincingly distinguishing between the scopes of protection of privacy on the one hand and protection of personal data on the other. Furthermore, it is recognized that the right to the protection of personal data also has close interdependencies with other freedoms that contribute substantive aspects, so that it is no longer clear how privacy and other substantive freedoms relate to each other.

The right to the protection of personal data offers the opportunity to work out the content of the protection and the protected interests of the data subjects independently in terms of content and doctrine, and thus in accordance with the subject matter. For this to succeed, it is first necessary to reach an understanding of both the factual bases and the essential consequences that must be considered in legal approaches. The right to the protection of personal data can then be convincingly developed and embedded in an appropriate overarching concept.

D. Shaping Data Protection Interests as a Bundle of Provisions and Rights

I. Factual fundamentals

1. What is data?

Although personal data is a core element of data protection, it is far from sufficiently clear what the concept of data is and what is or is not covered by it. Due to technical developments, and also due to the extension of

137 *Nadezhda Purtova*, The law of everything. Broad concept of personal data and future of EU data protection law, 10 Law, Innovation, and Technology 40 (2018).

data protection law itself, uncertainties are reflected in numerous problems: How does the law deal with the manifold descriptions in the various scientific disciplines? Are the terms "data" and "information" synonymous or should they be strictly differentiated? Or is this question, from a practical point of view, of no importance? Which entity can be delimited as a data unity when we step out of the familiar terrain and are not dealing with easily describable situations, but with, for example, big data or AI-contexts? Is data a suitable reference point for the desired legal protection at all?

The etymological root, with regard to which data presents itself as something "given", creates an extraordinarily broad starting point for the understanding of the term "data". On a very abstract level, data can be understood against the background of the possibilities of differentiation.[138] Such an approach can capture different levels of abstraction and reference points as well as a wide range of applications for the concept of data: the distinguishability of real-world phenomena, physical parameters measured by standards, numbers, letters, texts, communication elements, or binary digital units. The heterogeneity of this non-exhaustive list reveals that the concept of data is a construction that varies according to historical epoch, perspective, and framing. While in a certain phase "data" was often linked to the evolution of science, experimentation and measurement, today they are a multifaceted element of the "onlife"-world. Additionally, the storage forms and data formats in which data is embodied are shaped by the technologies, media and infrastructures.

As the concept of data is a construction, the various scientific disciplines each take their own approach. Concepts of "data", as well as of "information", are described in multifarious and discipline-dependent ways.[139] The law does not simply borrow descriptions like those approaches in computer science might use. Instead, it builds on different types of description patterns to cover the spectrum of regulatory needs and cases, takes them up in a legally specific way and reformulates them with a view to the legally justified need for protection. What is meant by "data" in the juridical context, is to a certain extent a legal construction in itself. Since the concept of data is such an abstract one, there may be different descriptions even in

138 *Luciano Floridi*, Information. A Very Short Introduction, 2010, 23: "[…] the general definition of a datum is: Dd) datum = def. x being distinct from y, where x and y are two uninterpreted variables and the relation of 'being distinct', as well as the domain, are left open to further interpretation."

139 *Floridi* (n 138), 19 ff.

different areas of law such as data protection law, copyright law, or patent law.

The aim of data protection law is not the protection of data but of the persons to whom the data refers. This is reflected in its focus on "personal data".[140] How data is to be understood in data protection law must be approached by simultaneously considering "personal data".

2. What is personal data?

Personal data is, as Art. 8(1) CFR describes, data concerning the individual. That means that its content refers to a particular natural or, depending on the legal system, also other legal person. However, such content is neither an intrinsic property of data nor is it attached to it like a label. It is an achievement attributing meaning to data. Two key questions are hidden in the "person-relatedness": When does data refer to a *specific* person and when does data *refer* to a person?

Data protection law addresses these questions by defining that the data must relate to either an identified or an identifiable person.[141] Data such as the personal name and data that is regularly linked to it, such as the address, date of birth, marital status, social security and tax identification numbers, fingerprints or portrait photographs are illustrative examples. Even with these simple examples, it quickly becomes clear that it must be answered which identifiers specify a person and that, if necessary, a connection between particular data and identification data must be drawn. Such a connection may be readily available in a given situation, but it may also only be possible by means of a number of steps, the relevance of which must be legally assessed with regard to the identifiability of a person. Prior or additional knowledge that some people might have can enable them to associate data that is not readily assignable on its own with a specific person.[142] If a reference to the person to be protected can only be

140 See, e. g., Art. 2(1) GDPR.

141 Art. 4 no. 1 GDPR.

142 See also the breadth of the term "personal data" ECJ, Judgment of 19 October 2016, C-582/14, *Breyer*, Rn. 32 ff.; Judgment of 20 December 2017, C-434/16, *Nowak*, Rn. 27 ff.; Judgment of 22 June 2023, C 579/21, *J. M.*, Rn. 41 ff.; Judgment of 9 November 2023, C-319/22, *Gesamtverband Autoteile-Handel e. V.*, Rn. 44 ff. Cf. also the overly broad approach of the Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, 01248/07/EN WP 136.

established via several activities involving a variety of parties, it can be quite difficult to decide under which conditions the person in question can be regarded as "identifiable" in relation to which party.[143] This already results in a very broad spectrum of data that can be linked to a person and then provide information about them.

Moreover, the identifiability of a person in a given situation or the much-discussed problem of re-identification are not the only issues. In light of its aims of protection and governance, data protection law does not only cover situations or activities in which a connection between data and particular persons actually exist or might be created by identifying steps. It also aims at preventing in advance legally undesirable connections between particular data and persons, the resulting knowledge about a person and its potential disadvantageous use. Hence, it has to be more or less future-oriented and applicable prior to risks that have become manifest. The specification of personal data and the question of whether a person is identifiable therefore involve not only a substantive dimension, which may eventually be relational with respect to different parties, but also a temporal dimension. The possibility of referring data to persons over time and in contexts not yet foreseeable – data generated anew as personal data at a later point in time – must be taken into account to a certain extent. Under the conditions of a data-driven society and economy, data is constantly linked to persons in new and unpredictable ways. However, it cannot be sufficient for activating protection that somebody might link data to a person somehow at some point in time. Otherwise, all data would have to be classified as personal data. Data protection law would end up being a "law of everything"[144].

From these difficulties associated with the description and delimitation of personal data, we can draw several conclusions. Beyond pure identification data, the answer to the question of which data relates to a person requires a description of the quality that the relationship between the data and the person concerned must have, as well as a description of the contexts in which the handling of data and information takes place. In both respects, evaluative judgments and assumptions of probability come into play. To a considerable extent, prognoses and typifications may enter the

143 See the above mentioned judgment of the Canadian Supreme Court, *R. v. Bykovets*, 2024 SCC 6, which is controversial concerning how to determine the information content of IP addresses.

144 See n 137.

picture. The personal-relatedness of data is regularly not to be determined by looking at a single piece of data separately, but rather with a view to the information and the knowledge that can be produced, to the overarching context, under certain circumstances to different relationships and participants, and through evaluative decisions.

The answers to the question of when data is personal are just as legally constructed as the concept of data. The understanding and delimitation of "personal data" must be conceptualized against the background of the protected interests which are the reason for data protection. Thus, it is not a seemingly easily detectable personal-relatedness of data as such that justifies the protection of data subjects. It is the other way around: the reasons for protection make it possible to determine the personal-relatedness of data. Such an approach is not only normatively convincing. It enables us, for example, to find solutions for scenarios that occur more frequently with the Internet of Things: Data refers to several people in different ways, so that legal positions must be justified in more detail.

3. Understanding "personal data" within a network of basic elements

At this point, it has already become clear, that from a constitutional and legal perspective, data protection deals with a highly complex subject matter. It is not about data as such. We must expand this isolated view by including further elements: at a basic level the element of information, in the structural dimension knowledge, in the temporal dimension the flow of data and information, and in the broader context decisions and consequences of decisions. Data protection aims at regulating data processing, but also at regulating the production of information and knowledge, at influencing the decisions based on such knowledge, and at preventing adverse consequences for the individuals affected.

It is of utmost importance for the understanding of data protection law that data and information must not be seen as if they were synonymous.[145] This is true even though legal definitions and some scholarly contributions might not reflect this in the required manner. Our analysis has shown that several court decisions illustrate this necessity very well. In the first step, data and information must be strictly differentiated, and in the second step, their relationship to each other must be worked out on the level of abstrac-

145 More closely *Albers* (n 106), 87 ff.

tion or concretion that is necessary. Otherwise, neither the characteristics of data protection law nor the challenges it faces can be worked out.

Data protection law addresses data, on the one hand, as an objectified entity. Data might be described as characters or symbols that are stored in a certain format on a data carrier, including written documents or videos as well as data digitally stored on hard drives or mobile data storage devices. Data, forms of storage, and processing operations are shaped by the various media, technologies, and infrastructures. Against the backdrop of complex digitized processing, "virtual data" can also be covered. On the other hand, data protection law addresses data because it can acquire informational significance in social contexts. Data is relevant as "potential information". This is to be understood more or less abstractly; it does not mean that there are fixed intrinsic meanings associated with the data. Furthermore, data can be decoupled from its potential informational significance to a certain extent; it can be identified as a distinct entity and become the subject of law even if it contributes to information and knowledge only in conjunction with other data or processing procedures. Data is often less important as a single piece of data, but rather as part of data processing or data architectures. Without any potential informational significance, however, the legal relevance required in the context of data protection law is lacking.

Conceptualized within the framework tailored to social contexts and legal perspectives, information involves meaning. Pieces of information are elements of meaning that may base on data (or on observations or communications) and are then created by interpretations which take place in a particular social context.[146] Information is context-dependent in an elementary way. Although this insight may be well-established today, people hardly face up to the difficulties this entails for legal regulation and for a description of the object to be regulated. In the structural dimension of such context, knowledge – founded upon texts, files, archives, registers, databases, expert systems, but also upon institutional, organizational or procedural arrangements – makes interpretation possible, and limits the possibilities of interpretation.[147] In the temporal dimension, data as well

146 Data and information are above all not synonyms because, although data as a basis for information may provide information, it presupposes far more than just data. Information cannot be described without observing knowledge structures, processes and the broader social context in which it arises.

147 In more detail and with further references *Marion Albers*, Umgang mit personenbezogenen Informationen und Daten, in: Voßkuhle, Eifert and Möllers (eds.), Grundlagen des Verwaltungsrechts, Vol. I, 3rd ed. 2022, § 22, Rn. 8 ff.

as information is constantly generated anew and altered during processing operations. Information and knowledge are also crucial factors in decision-making; they serve as bases for certain decisions and actions. Such decisions have consequences and may have an adverse effect on the person to whom the data and information refer. If disadvantages are normatively undesirable and unjustified, protection against such disadvantages – or even against the mere risk of such disadvantages arising – is one of the reasons for data protection. There are other reasons that can be elaborated in the determination of protected interests. At this point, it should only be made clear that understanding data protection requires thinking in social relations, in overarching contexts and in processes. The scope and form of considering social contexts depend on how relatively loose or condensed the relationship between data and knowledge, actions and decisions is in the focused context.

As a result, data must be conceived of within a network of several fundamental elements: information, communication, knowledge, decisions and actions. It is one, but not the only reference point. Data protection law aims at regulating data processing, but precisely also at regulating the generation of information and knowledge, at influencing the decisions based on such generation, and at preventing adverse consequences for the individuals affected. At the same time, these analyses show at what fundamental level we are working when regulating data and information. It is as fundamental as regulating decisions or actions.

II. Essentials of appropriate legal approaches

With this subject matter in mind, we can already reach some insights: It would be naïve to think that protection of personal data and information could be described in terms of a uniform protected good. The requirement of multi-layered, multi-dimensional and multifaceted guarantees and rights is obvious. The characteristics of the subject matter also point to the necessity of partly novel doctrinal approaches and of elaborating complex relationships between constitutional provisions and statutory law. Data protection interests are to a certain extent in need of being concretized and shaped by law.

1. Multi-layered, multi-dimensional and multifaceted guarantees and rights

Firstly, constitutional guarantees and rights must be developed within a multilayered framework. At first sight, the factual fundamentals suggest an extension of the concept of freedom anchored in each fundamental right to the handling of data and information. In other words: to embed the protected interests in the context of the entire constitutional law and to search for them at the level of each individual fundamental right. At times, particular guarantees have already been drawn upon. The European Court of Justice mentions the freedom of expression quite regularly. The freedom of assembly has been acknowledged as being relevant in case of surveillance by intelligence services. The right to mental integrity could be interpreted with regard to the use of certain neurotechniques. However, if all the possible specific scenarios of the handling of personal data and information in particular contexts are considered, the application of specific guarantees turns out to be full of prerequisites. We are not confronted with a single act of intervention, but with processes. The contents of the information and the consequences of their use depend on the respective purpose. As data protection is primarily future-oriented, and aims at avoiding harms beforehand in a way that "we cannot afford to wait to vindicate it only after it has been violated"[148], we must be able to describe, which data are collected and how they are altered and linked with one another, which information could be derived from certain data, for which purposes it is used and which disadvantageous consequences the individual might have to expect. It is therefore necessary to work out the relevant context and to break down the processes of handling information and data to the necessary extent by means of descriptions and prognoses. These prerequisites are not given without further ado. But the problem can be solved by distinguishing two or more levels on which the constitutional requirements are to be developed. Meeting the requirements at the basic level can create the conditions that enable us to apply particular guarantees at the second level. From a doctrinal perspective, this can be described as a cooperation of coordinated fundamental rights within a multilayered conception of guarantees and rights. Within such a multilayered conception, certain interests of the data subject to be protected must or can be addressed at a basic level and resolved there, in particular: through appropriate regulation, while

148 Judgment of the Canadian Supreme Court, *R. v. Dyment*, [1988] 2 S.C.R. 417, at 23: "This is inherent in the notion of being *secure* against unreasonable searches and seizures."

more concrete protection interests that emerge in particular contexts may be covered by the guarantees of the specific fundamental rights.

Secondly, guarantees and rights must be multidimensional. They have to be more diverse than the traditional concept of protection against encroachments because the data subject is to be protected with regard to personal information and data which are generated and processed by others in particular contexts. As has just been explained, appropriate regulation at a basic level is necessary; at this level the state is anything but kept out. Beyond that, protection directed solely at defending against and refraining from processing personal data is insufficient because the data subject may also be interested in personal data being made available so that agencies or private persons have the information at their disposal which they need for a correct decision. And it is just as important that the data subject is informed about processing of personal data and information, and can influence it. Hence, individuals need not only "negative" or defensive rights, but also "positive" or enabling rights to regulation, to know, to obtain information, to participate, or to exert influence.

Thirdly, guarantees and rights must be multi-faceted in the sense that their appropriately extended concept of freedom includes a variety of protected interests, each of which has its own characteristics. Protection of fundamental rights in terms of the way in which government agencies or other private parties handle personal data and information is different from the legally protected interests with which we are familiar in the traditional understanding of fundamental rights. The subject matter of protection is not a person's freedom of behavior or decision and protection of personal data is also not primarily about protecting a private sphere or what is already existing from informational access by others. People are to be protected with regard to the data and information concerning them as well as to the knowledge developed by others about them and against the repercussions or adverse effects this information and knowledge has or may have. But already due to the mere fact that data and information are handled and interpreted, government agencies or other private persons are structurally involved in processing of personal data and information. From a general perspective, i.e. leaving aside the special cases, personal data cannot be assigned to the person in question like an object belonging to him or her. Individualistic patterns of assignment fall short. Reasoning why and to what extent the person to whom data, information and knowledge refer is to be protected must rather be made from a supraindividual perspective. The protected interests of data subjects have to be conceptualized with regard

to the sociality of the individual and to structurally involved counterparts. Hence, they require their own separate patterns of description.

2. Sophisticated doctrinal constructions and methodologies

The understanding of fundamental rights as multi-layered, multi-dimensional and multifaceted guarantees and rights is not conceivable without sophisticated doctrinal constructions and methodologies. Classical notions based on a bourgeois-liberal approach and the complementary doctrine that fundamental rights are merely rights of defense against encroachments have dysfunctional prerequisites and limitations.[149] If we fall back on them, we will fail to work out data protection interests and the required regulation appropriately. As has been explained, this is why the right to privacy often falls short of what is needed. Protection of personal data has to base upon the further development of the functions and the contents of fundamental rights.

Extensions of the functions of the fundamental rights and of the scope of their protection which go beyond the traditional understanding of fundamental rights are recognized in many countries by now. Modern codifications reflect the diversity of dimensions of protection in their catalogs of fundamental rights. Additionally, guarantees of fundamental rights are open to interpretation. By means of sufficiently sound and sophisticated methodologies, they permit an elaboration of diverse dimensions of protection, including positive obligations of the state to provide a regulatory framework and to protect individuals through legal rules and actions. Legal norms do not only limit freedoms. They can also create freedoms in the first place, make them concrete, and influence their social conditions and prerequisites.

3. Interplay between fundamental rights and statutory regulation

One of the core questions of all interpretations of fundamental rights that go beyond the "classical" defense against encroachment is the problem of the extent to which it is possible to develop provisions that are sufficiently clear to be effective as constitutionally binding from the textually relatively

149 More closely *Marion Albers*, Realizing the Complexity of Data Protection, in: Gutwirth/Leenes/de Hert (eds.), Reloading Data Protection. Multidisciplinary Insights and Conteporary Challenges, 2014, 213 (216 f.).

vague fundamental rights. If guarantees and rights have to be understood as multi-layered and multidimensional, legislation is addressed in different roles. It must not only create positive rights of the data subject to know about or to exert influence on the processing of personal data and information, but also an appropriate legal framework at a basic level. Under these circumstances, the pertinent fundamental rights must be interpreted as provisions that are directed at requiring legislation to achieve certain goals and fulfill certain functions. On the one hand, they do not lay down a definite program that simply has to be carried out. Rather, the legislator has a margin of appreciation in the choice of the legal measures and instruments, as long as the goals and functions set forth in the constitution are achieved with the regulation created. On the other hand, precisely because the fundamental rights demand such a result, they would fall short if they were limited to merely vague statements.

The challenges can be handled if we understand the pertinent fundamental rights in such a way that they take into account the regulatory choices of the legislation and are constantly reapplied at more specific stages with more concrete requirements. Thus, as long as there is no legislative framework, fundamental rights requirements initially start with relatively vague provisions. Then, at a second stage, they are conditioned in the sense that they are based on the legislator's regulatory choices of a specific framework and set more specific, concrete provisions for its rules and regulations. In the case law of the German Federal Constitutional Court, there are illustrative examples of such an approach in the areas of the guarantee of property, of the freedom of press, and, above all, of the freedom of broadcasting.[150] As a result of such a process of interpreting, the relation between the pertinent fundamental rights and statutory legislation can be described as being shaped in a way that secondary legislation impacts "the content of the fundamental right, which is therefore destined to be constantly in flux

150 See, for example, the landmark judgment *FRAG* of 1981, Decisions of the FCC, Vol. 57, 295, 319 ff. Initially, the fundamental right that safeguards broadcasting freedom provides merely general requirements, but no particular model of how to regulate and organize broadcasting. However, if the legislator chooses, for example, a dual model of public and private broadcasting, the guarantee of the freedom of broadcasting sets out more detailed guidelines based on the model chosen by the legislator.

and evolution"[151]. However, the relation is neither reverse nor is it a circle. It is important to note that the relative hierarchy between fundamental rights requirements and legal regulations always continues to exist. The underlying image may be that of a spiral with relative hierarchies, i.e. hierarchies that are constantly being re-constituted at each of the different stages. Altogether, the interplay between fundamental rights and statutory regulations in the field of data protection becomes extremely challenging.

III. Concretizing protected interests within a multi-layered conception

All in all, data protection responds to threats to freedom and needs for protection that require their own separate patterns of description, must be located at different levels and are manifold and diverse. An approach to fundamental rights that is in line with our insights calls for developing a complex bundle of provisions and rights within the framework of a multi-layered conception. This bundle must be open to ongoing revision and constantly adapted to novel threats.

1. Basic level: Rights to appropriate regulation

At a basic level, data protection responds to risks and harms that have been addressed since the emergence of new technologies in the 1960s and have increased even further with the internet. In a rough summary, the crucial problems center around a potentially all-encompassing, unlimited and non-transparent processing of personal data and information by the state or other private parties. Orwell's "Big Brother", Bentham's "Panopticon", and Kafka's "The Trial" might be illustrative as widely known, culturally anchored metaphors that – despite these narratives being rooted in quite different contexts – take up different facets of the dangers just mentioned above. In addition to these state-centered works, more recent novels, such as Dave Eggers' "The Circle", might be added with a view to social networks. Daniel Solove has shown that the well-known Big Brother metaphor effectively captures certain data protection problems, but that it is the Kafka metaphor that illustrates those elements of threats to privacy

151 *Yordanka Ivanova*, The Role of the EU Fundamental Right to Data Protection in an Algorithmic and Big Data World, in: Hallinan, Leenes, Gutwirth and De Hert, Data Protection and Artificial Intelligence, 2021, 145 (151).

which deal with certain data collection and circulation by others "without having any say in the process, without knowing who has what information, what purposes or motives those entities have or what will be done with that information in the future."[152] The very beginning of the work gives a sense of how threatening this can be: "Someone must have slandered Josef K., for one morning, without him having done anything wrong, he was arrested. Why so, he asks the guards, and receives the terse reply: We are not appointed to tell you that."

These considerations point to the fact that, at the basic level, there are already multifarious problems that data protection shall countervail. Data protection provisions and rights aim at ensuring that the handling of personal information and data is not largely unbound, unlimited, intransparent, or beyond any possibilities of influencing procedures or results. In the first place, they center on requiring the establishment and implementation of a legal framework suitable for countering the fundamental threats. This already requires a very sophisticated legal framework and a wide range of legal instruments. Additionally, as we have seen, the legal framework at the basic level also has the function of ensuring that contextually definable risks which the data subjects may face are recognizable and describable, and of creating the conditions for the applicability of specific fundamental rights. Thus, substantially, the regulations directed by certain constitutional guidelines must ensure that contexts of data processing are limited and shaped, that data subjects have certain rights of knowledge and of influence, or that there are appropriate institutional provisions. Functionally, the regulations must create the conditions that make it possible to apply specific guarantees and ensure, for example, that risks to specific protected interests can be identified and countered in due time.

In the legal approaches to the content of the relevant fundamental rights requirements for regulating the handling of personal data and information, a level precedent to cases that can be contextually delineated is recognized and addressed to a certain extent. This is reflected, for example, in the numerous considerations on the relationship between data protection and a democratic order. Data protection is seen as a factor in, or even a prerequisite for, enabling a democratic order to exist.[153] This presupposes, of course, that it is understood not as individual control over personal data, but

152 *Daniel Solove*, Privacy and Power: Computer Databases and Metaphors for Information Privacy, 53 Stanford Law Review 1393, 1426 (2001).

153 See for references to the democratic order Decisions of the FCC, Vol. 65, 1, 43.

as multilayered, multidimensional, and multifaceted.[154] But even without these references to democracy, some courts have pointed out that privacy or the right to respect for privacy, which has been extensively elaborated in some jurisdictions, is at the heart of liberty in a modern state and a condition for the enjoyment of other rights or non-discrimination.[155] However, as the right to privacy covers many facets from pre-conditions to various protected interests in contextually delimited cases and as the content of the protection is more or less blurred, this cannot be addressed with the necessary accuracy. Greater clarity and effectiveness can be achieved if these interests of the data subject at this basic level are assigned to a specific fundamental right and its protective content is developed accordingly.

With regard to German law, this is possible in view of Art. 2(1) in conjunction with Art. 1(1), if we leave behind the version of the right to informational self-determination that was established by the census ruling, and which is now in flux anyway, and develop a more complex fundamental rights conceptualization.[156] Even better suited to such an approach is a right of individuals "to" the "protection" of personal data concerning them. Such a right can be interpreted in such a way that it provides regulatory and protective requirements that primarily apply at a basic level prior to constellations that can be contextually delineated and addresses certain protection needs of the data subjects at a first-layer level. Regarding Art. 8(1) CFR, these considerations are consistent with the fact that Art. 8(2) and (3) CFR lays down a number of requirements, although these are a rather unsystematic compilation of several factors of different provenance, which do not exhaustively describe the core of the right to the protection of personal data. Art. 8 CFR primarily addresses the legislator with a complex set of provisions and, to a certain extent, corresponding individual rights aimed at ensuring that the substantive and functional requirements, as explained

154 Cf. also, from an overarching point of view, *Paul de Hert* and *Cristina Cocito*, The Added Value of Data Protection within the Framework of Digital Constitutionalism in Europe, in: De Gregorio (ed.), The Oxford Handbook of Digital Constitutionalism, 2024.

155 See as examples from our analysis of the case law Supreme Court of Canada, *R. v. Dyment*, [1988] 2 S.C.R. 417, at 17; Supreme Court of India, *Puttaswamy-I*, Part R (p. 243, 244); Constitutional Court of South Africa, *Amabhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others; Minister of Police v Amabhungane Centre for Investigative Journalism NPC and Others* (CCT 278, 279/19) [2021] ZACC 3, at 112 ff.

156 *Albers* (n 106), 454 ff.

above, are met through appropriate regulation. This is not done with *any* regulation. In particular, legislation must safeguard that the handling of personal information and data is not unrestricted, unlimited and opaque. It must also provide that risks to specific protected interests of data subjects can be identified and countered in a timely manner. Data subjects must have the opportunity to obtain sufficient knowledge of and influence over the processing of data and information relating to them. Given the inherent limitations of rights-based approaches alone, a number of obligations must be imposed on persons or entities that handle personal information and data. Institutional safeguards and control mechanisms must be added.[157] As explained above, in the interplay of fundamental rights and statutory regulations, the provisions of the right to the protection of personal data need to be continuously reapplied at more specific levels with more concrete requirements.

Since the fundamental right to the protection of personal data understood in this way requires, from a functional point of view, that the regulations at the basic level create the conditions that make it possible to apply specific guarantees, it points beyond itself to the spectrum of other fundamental rights. It sets the stage for them to enter the scene.

2. Second level: Data protection rights from specific fundamental rights

At a second level, specific fundamental rights can enter the picture. This applies to all possibly relevant guarantees: rights to mental integrity, to freedom of thought, conscience and religion, to freedom of expression, to freedom of assembly, or to freedom to choose an occupation. In the concept outlined here, if the right to privacy is established alongside a right to the protection of personal data, it can also be given specific content. The factual fundamentals already suggest the recourse to a broad normative basis to concretize fundamental rights requirements. The jurisprudence of the courts, as shown, has in principle recognized the relevance of the specific fundamental rights.[158] However, specific freedoms are often mentioned

157 Cf. *Albers* (n 149), 229 ff. Cf. also with partly different considerations, *Nikolaus Marsch*, Das europäische Datenschutzgrundrecht, 2018, 127 ff.; *Lorenzo Dalla Corte*, A right to a rule: On the substance and essence of the fundamental right to personal data protection, in: Hallinan, Leenes, Gutwirth and De Hert (eds.), Data protection and privacy: Data protection and democracy, 2020, 27 (38 ff.).

158 See n 74, 75, 80, 95.

only in passing. It is not worked out exactly under which conditions they actually apply and how.

Whether, when and how they are to be applied can be more clearly and precisely defined by considering that the ability to describe all relevant risks to data subjects that may or are likely to arise, and the specific interests to be protected, requires basic regulations at the first level. If such regulations exist and if we then can describe in more detail the contexts in which the handling of personal information and data takes place, the purposes, the players involved, and the procedures, potential contextually specific harms and particular interests of the data subject to be protected show up. Under these circumstances, specific fundamental rights tailored to particular contexts and risks can be referred to. We can interpret them in a problem-oriented way from a supraindividual perspective, keeping in mind the characteristics of data, information, and knowledge. Provisions and individual rights can be applied exactly where and insofar a need for protection can be identified. This results in a broad, dynamic and procedural concept of data protection rights derived from specific fundamental rights.

3. Cooperation of fundamental rights at different levels

In summary, data protection rights can be developed from an interplay of fundamental rights within the framework of a multi-layered concept. Such an interplay should not be conceived as an additive juxtaposition. Rather, it must be understood as a *functional cooperation* of fundamental rights at *different* levels. This results in a bundle of multi-layered, multidimensional and multi-faceted provisions and rights to which all fundamental rights with their substantive particularities can contribute. At the same time, it becomes clear, that it is necessary, but also possible, to embed data protection rights in overarching contexts and to coordinate them appropriately with other legal regimes.

E. Conclusion and Outlook: Data Protection as an Integral Part of the EU Data and Digital Strategy

Protection of personal data does not encompass a uniform legally protected good. In particular, the idea of control over one's own data fails because it does not fit the subject matter to be protected. Instead, protection of

personal data points to a variety of protected interests and to a bundle of provisions and rights that has to be developed in the framework of a multi-level approach as a functional cooperation of coordinated fundamental rights.

Data protection places high demands on law. This is all the truer as regulations are shaped not only by fundamental rights and the requirements they impose, but also by legal policy. Even if individual rights are developed in a way that reflects the characteristics of data and information and is problem-oriented, they are and should be only a small component of a much larger architecture.[159] The statutory rules and the legal positions of data subjects must be founded on the diverse functions and diverse forms of law. Regulation concepts must include a wide range of constituent elements which utilize the entire spectrum of legal forms and instruments. As an innovative and highly dynamic field, data protection law needs to be, in terms of legal theory, "reflexive law" and, from a doctrinal point of view, a mixture of stability and dynamics. This is reflected, for instance, in the delegation of legislation competences, in the use of legal terms which are vague and need to be concretized, in normative references to dynamically adapted technical standards, in rules allowing for experimentation, in evaluation procedures or in other tools to ensure the capacity to learn and develop. Regulatory concepts are therefore complex on its own terms and in addition, they have to be interwoven. The emerging variety of regulatory concepts is also compatible with a less legislation-centered understanding of law and regulation. From a political-science point of view, it has been analyzed, how the substance of data protection law is made concrete by the interactions among different actors—the legislative, executive and judicial branches, data protection agencies, data users, data subjects. An appropriate normative conception has to be responsive to the interplay of actors generating and concretizing law whilst, at the same time, keeping the normative perspective. Last but not least, it is essential to embed data protection rules and rights in overarching contexts and to coordinate them appropriately with other legal regimes.

How (personal) information and data may be processed has always been regulated, to some extent and from certain perspectives, by various legal regimes, such as media law or tort law. The resulting need for coordination

159 *Daniel Solove*, The Limitations of Privacy Rights, 98 Notre Dame Law Review 975, 977 ff. (2023).

between the rules of these regimes and data protection law is increasingly evident, and this is a very challenging task.[160] The same applies to the series of regulations within the EU data and digital strategy. Data protection is, and must be, an integral part of this overall strategy. However, as the GDPR to some extent sticks to traditional patterns of data protection that are not compatible with some of the other regulatory concepts, it cannot remain untouched. As a prerequisite, the fundamental rights and protected interests of data subjects must also be rethought and reconceptualized.

160 See *Anna Schimke*, Forgetting as a Social Concept. Contextualizing the Right to Be Forgotten, in: Albers and Sarlet (n 2), 179 (190 ff.).

The (In)Effectiveness of EU Data Protection: A Rejoinder

Giulia Gentile

Abstract: The emergence of a highly privatised digital environment driven by data has triggered a regulatory response in the EU built on public law tools, such as fundamental rights. The EU fundamental right to data protection has had a central role in scrutinising the conduct of tech companies within the EU and beyond. The application of this fundamental right has followed an expansive trajectory, aimed at offering effective and complete protection, to use the words of the European Court of Justice. Yet the fundamental right-driven enforcement of EU data protection rules has been heavily criticised, and not without reason. Among the several critiques, it has been observed that the breadth of data protection entails enforcement challenges, while the proceduralisation of this right *de facto* disguises the preservation of a business model in favour of digital actors. This chapter offers a rejoinder to these critiques by reflecting on and contextualising the criticisms of data protection's effectiveness against the background of the human rights' crisis. As the chapter demonstrates, several challengers against EU data protection rules mirror a broader critical movement against human rights. Hence, while many stances against data protection are worthy of consideration, scholars and regulators should not lose sight of the gains and protections afforded by data protection as a fundamental right. As a matter of fact, human rights remain one of the most effective tools to counteract imbalances of powers due to their iterative engagement governance, especially in the digital society.

A. Introduction

Data structures and underpins digital society. We can trace data in almost every daily activity carried out by individuals and public bodies: statistical

All the links have been accessed on 9 September 2024.

evidence and data are likely to underlie an increasing number of policies;[1] the study of patients' health and lifestyle is conducted through data analysis;[2] administrative decisions increasingly rely on data,[3] and so on. The emergence of a pervasive data-driven society was favoured by a private tech power, which exploited the structures of the digital environment in its favour. EU institutions[4] and States[5] have counteracted those imbalances of digital power though law, and especially the recognition of fundamental rights such as that to data protection. The application of fundamental entitlements in the digital environment was innovative, to a certain extent, as it affected private parties such as online platforms. It further signalled the advancement of public value considerations in the highly privatised digital environment, built on the exploitation of data. The advancement of constitutional guarantees to the digital environment has been captured under the concept of 'digital constitutionalism'.[6]

1 Md Altab Hossin et al 'Big Data-Driven Public Policy Decisions: Transformation Toward Smart Governance' (2023) 13(4) Sage Open, https://doi.org/10.1177/21582440231215123; Michela Arnaboldi and Giovanni Azzone, 'Data science in the design of public policies: dispelling the obscurity in matching policy demand and data offer' (2020) 6 Heliyon https://www.cell.com/action/showPdf?pii=S2405-8440%2820%2931144-0.

2 Richard Brown et al, 'Collecting and sharing self-generated health and lifestyle data: Understanding barriers for people living with long-term health conditions - a survey study' (2022) 8 Digit Health 1; see also the UK National Health System approach to data collection and data sets, available at https://digital.nhs.uk/data-and-information/data-collections-and-data-sets#:~:text=Our%20data%20collections%20cover%20many,authorities%20and%20independent%2Dsector%20organisations.&text=Our%20national%20data%20sets%20collect,areas%20of%20health%20and%20care.

3 See in the UK context the UK Department for Science, Innovation and Technology, 'Ethics, Transparency and Accountability Framework for Automated Decision-Making' 29 November 2023, available at https://www.gov.uk/government/publications/ethics-transparency-and-accountability-framework-for-automated-decision-making/ethics-transparency-and-accountability-framework-for-automated-decision-making; Ulrik B.U. Roehl, 'Automated decision-making and good administration: Views from inside the government machinery' (2023) 40(4) Government Information Quarterly 101864.

4 See 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 [1995] OJ L 281 (Directive 95/46).

5 See DLA Piper 'Data Protection Laws of the World' https://www.dlapiperdataprotection.com/index.html?t=law&c=FR&c2=DE.

6 Edoardo Celeste, 'Digital constitutionalism: a new systematic theorisation' (2019) 33(1) International Review of Law, Computers & Technology 76; Giovanni De Gregorio, 'The rise of digital constitutionalism in the European Union' (2021) 19(1) International Journal of Constitutional Law 41; Nicolas Suzor, 'Digital constitutionalism: Using the

Enshrined in Article 8 of the EU Charter and Article 16 TFEU, the fundamental right to data protection played a significant role in the EU digital constitutionalism. Data protection rules, introduced in the EU with Directive 95/46, were designed to address several challenges stemming from the emergence of data power, such as the regulation of personal data processing and the need to ensure harmonised rules on personal data transfers in the internal market.[7] Data protection cases like *Google Spain*[8] or the *Schrems* saga[9] demonstrated the power of fundamental rights, and especially data protection, in constraining digital power.[10] The latest iteration of data protection rules, the General Data Protection Regulation (GDPR), is a globally leading framework that has acted as a blueprint for other data protection laws across the world.[11] The GDPR has introduced several innovations, including detailed rules on remedies and enforcement[12] for the transnational enforcement of data protection rights.[13]

As an emanation of a fundamental right, by nature open-ended and amenable to judicial interpretation, data protection rules have been interpreted under a constitutional approach. Examples of the expansive fundamental-right interpretation of EU data protection rules concern the concept of personal data[14] and data processing,[15] the narrow reading of the house-

rule of law to evaluate the legitimacy of governance by platforms' (2018) 4(3) Social Media + Society 1.

7 See e.g. recitals 2 and 3 of Directive 95/46.

8 Case C-131/12 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* EU:C:2014:317.

9 See Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* (*Schrems I*) EU:C:2015:650; Case C-311/18 *Facebook Ireland and Schrems (Schrems II)* EU:C:2020:559.

10 Also across the Atlantic the application of fundamental rights guarantees regarded digital matters such as freedom of speech and indecent or obscene material (Reno v American Civil Liberties Union 521 US 844 (1997) and privacy (ACLU v Clapper 785 F3d 787 (2n Cir 2015).

11 Annegret Bendiek and Isabella Stuerzer 'The Brussels Effect, European Regulatory Power and Political Capital: Evidence for Mutually Reinforcing Internal and External Dimensions of the Brussels Effect from the European Digital Policy Debate' (2023) 20(5) Digital Society.

12 See Chapter 8 GDPR.

13 See Chapter 7 GDPR.

14 See Case C-434/16 *Nowak* EU:C:2017:582.

15 See Case C-101/01 *Bodil Lindqvist* EU:C:2003:596.

hold exemption,[16] and the joint liability regime for controllers.[17] Through the door of the GDPR, Big Tech's data power has been subject to scrutiny.

Yet the EU data protection rules have also been heavily criticised. The very features that have supported the broad application of the data protection framework, and, namely, its expansive scope (driven by the fundamental right approach), have been the target of several critiques. For example, authors have remarked that data protection rules apply to everything[18] and everyone,[19] and that they replicate market dynamics hidden behind a fundamental right narrative.[20] Laws that are excessively broad encounter enforcement problems and may not be effective. Lynskey has argued that the GDPR rules aspire to completeness, but cannot be effective.[21] In turn, it has been observed, a cumbersome framework may limit innovation and market freedoms.[22] Hence a paradox has materialised: while the fundamental right nature of data protection, and the consequent broad application of rules, were deemed as necessary by regulators to address the imbalances of power in the digital environment, they were also identified as its very weaknesses that undermine the effectiveness of data protection rules.

The effectiveness challenge for EU data protection rules is a critique that underlies the adoption of the Data Protection and Digital Information Bill (DPDIB) in the UK[23] – now defunct – in the aftermath of the withdrawal from the EU and the loss of the EU Charter from the UK legal order. Striking but perhaps unsurprising features of this framework were the very

16 See Case C-212/13 *Ryneš* EU:C:2014:2428.

17 See Case C-210/16 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH* EU:C:2018:388.

18 Nadezhda Purtova, 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law' (2018) 10(1) Law, Innovation and Technology 40.

19 Orla Lynskey, 'Complete and Effective Data Protection' (2023) 76 Current Legal Problems 297.

20 See the discussion on consent and legitimate interest as a ground for lawful processing, Midas Nouwens et al 'Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence' CHI '20: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems April 2020 1 https://doi.org/10.1145/3313831.3376321.

21 Lynskey (n 19).

22 Ryan Preston, 'Stifling Innovation: How Global Data Protection Regulation Trends Inhibit the Growth of Healthcare Research and Start-Ups' (2022) 37 Emory Int'L L Rev 135.

23 See UK Government, 'Data Protection and Digital Information Bill', available at https://bills.parliament.uk/bills/3430.

scarce references to fundamental rights' protection,[24] and the de-valuation of data protection to a set of procedural rules rather than a fundamental entitlement in its own right. Hence, while it favoured market interests and innovation, the Bill sought to abandon the ability to protect personal data as a matter of fundamental rights protection.[25]

These criticisms and policy developments test the conceptual boundaries of data protection and question its effectiveness as a source of fundamental protection. Has the fundamental right to data protection failed to demonstrate its value?[26] This paper argues that those critiques need to be contextualised in the broader crises of human rights.[27] As will be demonstrated, the contestation raised against data protection as a framework – and especially as a fundamental right – essentially reflect a critical movement against human rights.[28] In recent years, whether human rights are an effective mechanism to protect individuals and public values in our society has been questioned.[29] Accordingly, critiques to the effectiveness of data protection should be filtered to avoid falling prey to narratives that are essentially anti-human rights. While human rights have been criticised for

24 One of the consequences of Brexit has been the loss of the EU Charter of Fundamental Rights and the fundamental right to data protection granted thereunder. Accordingly, the UK Government has sought to seize the opportunity for innovation and increased competitiveness by revising data protection rules, and introducing the DPDIB. If adopted, this new framework could significantly transform the ability of individuals to protect their personal data.

25 This approach was evidently in stark contrast with the European Union context which instead recognises acknowledges the value of data protection as a fundamental right.

26 Orla Lynskey 'Deconstructing Data Protection: The 'Added-Value' of a Right to Data Protection in the EU Legal Order' (2014) 63(3) ICLQ 569; Maria Tzanou 'Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right' (2013) 3(2) International Data Privacy Law 88.

27 While the terminology 'human right' is typically used in the context of international law, 'fundamental rights' is generally employed in a European context.

28 Andrew Fagan, 'The Subject of Human Rights: from the Unencumbered Self to the Relational Self' (2024) The Nordic Journal of Human Rights 215; Kiyoteru Tsutsui 'Justice Lost! The Failure of International Human Rights Law To Matter Where Needed Most' (2007) 44 Journal of Peace Research 407; Oren Gross '"Once More Unto Breach": the Systemic Failure of Applying the European Convention on Human Rights to Entrenched Emergencies' (1998) 23 Yale Journal of International Law 436; Eric Posner, 'The Case Against Human Rights' 4 December 2014, The Guardian https://www.theguardian.com/news/2014/dec/04/-sp-case-against-human-rights; David Kennedy, 'The International Human Rights Movement: Part of the Problem?' (2002) 15 Harvard Human Rights Journal 101.

29 See also Eric Posner, *The Twilight of Human Rights* (OUP, 2013).

reinforcing neo-liberal dynamics and power structures, they nonetheless remain a legal tool that allows accountability and the imposition of positive and negative obligations on duty-bearers. In so doing, they have an equalising and protective function, insofar as they support the scrutiny of behaviours of parties in positions of power. According to de Búrca, the value of human rights stems from the 'iterative engagement'[30] governance they engender.

Similarly, personal data protection as a fundamental right has three features that make it particularly apt to respond to the complexities of the digital society. These are protectiveness, dialogue and a high degree of universality. Combined, these give rise to a governance structure that enhances scrutiny over the use of data by private and public bodies. Such scrutiny, although imperfect and certainly requiring improvement, allows the exercise of control over the behaviour of data entities enjoying a position of power over data subjects. The ability to scrutinise the conduct of data processors and controllers fosters an iterative approach to the regulation of the digital environment, which in turn stimulates reflections on the power dynamics of specific fields of law. By highlighting the value of data protection as a fundamental right, the chapter does not intend to entirely dismiss the criticisms raised against data protection. Many critiques are valuable and seek to foster better regulation of personal data. Yet, when rethinking data protection, sight should not be lost of the positive side of the story of the fundamental right to data protection: the data feudalism that permeates the digital environment can be successfully rebalanced through legal tools such as fundamental rights.

The paper proceeds as follows. First, it introduces the challenges of digital constitutionalism; then it explains the foundations of data protection rules in the EU legal order. Subsequently, the chapter critically analyses the fitness of data protection in the context of digital constitutionalism in light of the various critiques advanced in the literature. It does so by highlighting how the effectiveness crisis of data protection mirrors the deeper contestation experienced by human rights in recent decades. Conclusions will follow.

30 Grainne de Búrca, *Reframing Human Rights in a Turbulent Era*, (OUP, 2021) at 10.

B. The challenges of digital society and digital constitutionalism

Digital constitutionalism is a label used for an emerging regulatory phenomenon in the digital environment. Namely, digital constitutionalism seeks to capture the use of the law, and especially public law, to restrain the power of private digital entities that have permeated society in an increasing fashion. While there is a plurality of understandings of digital constitutionalism, they tend to converge on two tenets. First, the proliferation and strengthening of private digital actors has created power imbalances in the digital word. Second, due to their implications in the real world, these 'digital-power-imbalances' demanded regulatory tools, the law appearing as central to restrain power and tackle abuses perpetrated by private actors in the digital field. Both these dynamics speak to the introduction of public law guarantees in the online space. The prominent role of fundamental rights' protection in the EU digital regulation articulates one of the aspects of 'EU digital constitutionalism'. Digital constitutionalism can therefore be conceptualised as a legal response to the establishment of a 'digital society' governed by power dynamics and relationships with novel features linked to the structures of the internet and technology.[31] The use of public law in the context of digital constitutionalism essentially addresses three challenges stemming from the digital society.

First, with the emergence of the digital society and the rise of online platforms, digital private entities have benefitted from a prominent position and power vis-à-vis individuals.[32] Thanks to their ability to govern the structures, including access and enjoyment of digital services, the architects of the digital world were able to claim 'regulatory' authority in their space.[33] In so doing, these bodies have shaped the online digital world, as well as the freedoms and legal entitlements of users and players engaging with these technologies. For instance, social media platforms became, willingly or not,

31 See Tomi Dufva and Mikko Dufva, 'Grasping the Future of the digital society' (2019) 107 Futures 17; Vitaly V. Martynov, 'Information Technology as the Basis for Transformation into a Digital Society and Industry 5.0' available at https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8928305&casa_token=lb2s_fNfG-MAAAAA:MfzCoQEL8Eo9ElPgfz935n97JNYk3CvrLqUGs1WlbvdxTl4OhueA_EnUYYd7wdyuUelTOPfOXQHc&tag=1.

32 For a general discussion see Martin Moore and Damian Tambini (eds) *Digital Dominance: The Power of Google, Amazon, Facebook and Apple* (OUP, 2018).

33 See the discussion on 'Code is Law' initiated by Lawrence Lessig, *Code and Other Laws of Cyberspace* (Basic Books, 1999).

responsible of the freedom of speech of their users, as well as their ability to access information services or education.[34]

In turn, the dominant position of the architects of the digital society was amplified by a twofold externality. First, the merging of market power with digital power. Companies, such as Amazon, Facebook and Google, have de facto monopolies in the digital market.[35] And because of their dominant position in the markets, they can also more easily gather big data through their users. Such incredible amount of data also allows these entities to know more and more about their users, and ultimately, affect their free choice and fundamental rights.[36] Second, the informational gap and a-symmetries in favour of tech companies. Both regulators and individuals have for long been in a position of relative ignorance and seldom disregard concerning the digital world and its implications on society: the ignorance of others was power for digital actors. As described De Gregorio and Radu,[37] the *laissez-faire* attitude of the regulators has strengthened private digital power. Digital constitutionalism seeks to rebalance this imbalance on the online space.

A second challenge that digital constitutionalism grapples with is that of reconciling fundamental rights protection with other public interests, and, especially, the economic structures and rules of the (digital) market. As a matter of fact, it is complex to align market interests with fundamental rights protection: one of the two should at least partially give in. Because of the public interests identified in economic and market policies, as well as the limitations that are intrinsic to fundamental rights vis-à-vis public interests, fundamental rights have often been treated as secunda ratio to

34 Kate Klonick, 'The new governors: The people, rules, and processes governing online speech' (2017) 131 Harv. L. Rev. 131, 1598; see the liberal dimension of digital constitutionalism described by Francisco de Abreu Duarte et al, 'Perspectives on Digital Constitutionalism' in Bartosz Brozek et al (eds.), *Handbook on Law and Technology* (Edward Elgar, forthcoming) https://ssrn.com/abstract=4508600.

35 Emilio Calvano and Michele Polo 'Market power, competition and innovation in digital markets: A survey' (2021) 54 *Information Economics and Policy* 100853.

36 Nathalie de Marcellis-Warin et al., 'Artificial intelligence and consumer manipulations: from consumer's counter algorithms to firm's self-regulation tools' (2022) 2 AI Ethics 259.

37 Giovanni De Gregorio and Roxana Radu, 'Digital constitutionalism in the new era of Internet governance' (2022) 30(1) International Journal of Law and Information Technology 68.

the achievement of market goals and objectives.[38] At the same time, the opposite result involving the prevalence of fundamental rights over market objectives has been criticised both by companies and regulators as a possible constraint over innovation and the competitiveness.[39]

Seen from another perspective, the tension between individual and collective rights and values underpins the developments of digital constitutionalism. Focusing on data protection, the dichotomy between individual and collective interests emerges powerfully. Indeed, the protection of personal data might, in certain circumstances, hinder the protection of other fundamental rights, such as that to freedom of expression.[40] In addition, the perception of data protection breaches might change depending on whether we look at individual or collective implications. For instance, it has been argued that individual violations do not resonate as much as collective, systematic abuses of data protection rules, due to the scale of societal impacts and harms.[41] In this context, because of the broad applicability of data protection rules and the need to adjudicate these tensions, courts have been at the forefront of the digital constitutionalist transformation. The image that results from the jurisprudence of the cyberspace is one of polycentricity, with several complex dynamics and interests coming to the fore.

A third challenge explored by digital constitutionalism is the transnational enforcement of the law and especially of constitutional rules in the digital society.[42] Because of the transnational nature of several databases, social media and AI technologies, questions arise on the legal frameworks that apply to the digital environment and data.[43] From the perspective of digital constitutionalism, what is of interest is how to solve normative conflicts and the clashes of different conceptions of public law and fundamental

38 Síofra O'Leary, 'Balancing Rights in a Digital Age' (2018) 59 Irish Jurist 59 https://www.jstor.org/stable/26431267.

39 See Cat Zakrewsky 'Tech companies spent almost $70 million lobbying Washington in 2021 as Congress sought to rein in their power' (2022) The Washington Post https://www.washingtonpost.com/technology/2022/01/21/tech-lobbying-in-washington/.

40 David Erdos, 'Special, Personal and Broad Expression: Exploring Freedom of Expression Norms under the General Data Protection Regulation' (2021) 40 Yearbook of European Law 398–430, https://doi.org/10.1093/yel/yeab004.

41 Omri Ben-Shahar, 'Data Pollution' (2019) 11 Journal of Legal Analysis 104.

42 Oreste Pollicino, *Judicial Protection of Fundamental Rights on the Internet* (Hart, 2021).

43 Ibid.

entitlement. And this becomes particularly evident when considering the protection of privacy broadly understood and the freedom of expression in the US and in the EU.[44] Hence, digital constitutionalism also reflects on the migration of values and principles that influence digital regulation and enforcement.

All in all, the three challenges of power asymmetries and imbalances, balancing of rights and interests and migration and development of fundamental rights and values are not extraordinary to the digital constitutionalism *per se*. Yet the legal issues emerging from the digital environment stretch the common understandings of rights' entitlements and protections, and push the boundaries of the law to tackle novel questions, actors and tools. It is in light of this background that we should consider the effectiveness of data protection as a fundamental rights framework in tackling the challenges of digital constitutionalism.

C. European Data Protection Rules: objectives and tools

Data protection rules have been established at the EU level since 1995 with the adoption of Directive 95/46 that set out the blueprint for personal data protection across the Member States.[45] The introduction of EU data protection rules was premised on two practical issues. First, the increasing overproduction of and overreliance on data, which can be used to identify, profile, exclude and manipulate individuals.[46] The need to protect individuals from abuses deriving from the exploitation of their personal information accordingly emerged. In this context, the fundamental right to privacy was put under strain and exposed to novel tests, due to the invisibility of privacy breaches through data (ab)use and the technologies used for the processing of personal data. A secondary challenge was of internal market's matrix, being the need to ensure harmonised protection for personal data in the context of cross-border transfers of information and data across the European Union.[47] In this sense, EU data protection rules were borne out at the intersection between fundamental rights and internal market objectives.

44 Ibid.
45 Orla Lynskey, *The Foundations of Data Protection* (OUP, 2015).
46 See Recital 4 Directive 95/46.
47 See Recital 3 Directive 95/46.

The fundamental right dimension of data protection emerged before the entry into force of the EU Charter.[48]

Since 2018, the Directive has been replaced by the GDPR, which has strengthened some of the tenets of data protection rules in Europe. The GDPR has essentially bolstered the fundamental right dimension of data protection while detailing procedural rules for the processing of personal data and cooperation among data protection authorities.[49] Indeed, the EU Charter of fundamental rights has officially introduced a fundamental right to data protection under EU law.[50] It has been already discussed that data protection has a specific role that cannot be fully replicated under the right to privacy.[51] Data protection and privacy are two connected rights, but the former adds value to the latter.[52] Namely, data protection allows individuals to control the use and security of their data. Other theories on the role of data protection as a fundamental right have focused on its separate and instrumental nature in relation to privacy.[53] Another aspect that data protection rules expand compared to privacy protection is the ability to offer enhanced protection to sensitive data.[54] The fundamental right to data protection, supported by its procedural framework, empowers data subjects to monitor the information relating to them. In parallel, data controllers and processors have a series of obligations to ensure personal data lawfully. Hence, data protection is the EU fundamental digital right *par excellence*. The data protection as a fundamental right presents several features shared with other EU fundamental rights, such as labour rights[55] or consumer protection.[56]

48 See *Lindqvist* (n 15) in which the Court of Justice linked data protection to the fundamental right to privacy, para 79.
49 Giulia Gentile and Orla Lynskey, 'Deficient by Design? The Transnational Enforcement of the GDPR' (2022) 71 ICLQ 799.
50 However, see Convention 108.
51 Lynskey, 'The added value of data protection', (2014) 63(3) ICLQ 569.
52 Lynskey (n 26).
53 Tzanou (n 26).
54 Ibid.
55 See among others Article 31 of the EU Charter of Fundamental Rights, as interpreted in the *Bauer* case, C-569/16 EU:C:2018:871.
56 See Article 38 of the EU Charter of Fundamental Rights.

Regulated and proceduralised

The fundamental right to data protection in the EU is highly regulated through secondary measures, coupled with several opinions issued by the European Data Protection Board (EDPB) and, previously, Article 29.[57] Hence, courts in the Member States and at EU level can rely on a plethora of guidance documents. Moreover, in addition to the EU rules and procedures, national procedural rules also play a role in the enforcement of data protection rules. In so doing, the protection of personal data is harmonised but leaves space for the peculiarities of national systems. For instance, the variance of procedural rules involved in the enforcement of data protection can hinder the effective and equal enforcement of data protection rights across the EU.[58]

Breadth

Data protection is a broad fundamental right *ratione personae*, *materiae*, and *loci*. Anyone whose personal data[59] is affected can invoke the protection of personal data protection under Article 8 of the EU Charter. But in addition to a broad personal scope, the fundamental right to personal data protection also has a broad material scope. Data protection rules cover all areas of human activities that involve personal data processing.[60] The consequence of this framework is that only in few instances – carefully crafted under the GDPR – is it possible for Member States to exclude the reach of data protection rules, an example being national security.[61] The broad scope *ratione materiae* and *loci* is further expanded by the horizontality of data protection. Through the more detailed rules of the GDPR, the fundamental right to data protection imposes very specific procedural obligations and duties to entities (be they private or public) processing personal data.

But beyond the broad personal and material scope of application of the GDPR, it is also well-settled that data protection rules apply also beyond

57 See Lynskey (n 19).
58 Gentile and Lynskey (n 49).
59 See Articles 2 and 3 GDPR.
60 The concept of data processing is very broad, too. See Lynskey (2023) and Opinion of AG Bobek in Case C-245/20 *X and Z v Autoriteit Persoonsgegevens* EU:C:2021:822.
61 See Article 2 GDPR. However, cfr with Article 23 GDPR.

the borders of the European Union, as demonstrated by the *Schrems* saga and as clearly established in the GDPR.[62] Data protection rules also bind third countries and their operators so long as they have been recognised as providing an equivalent protection to the EU in the field of data protection or so long as in any event individuals are sending are consenting for their personal data to be processed in the territory of that third country. The broad scope of application of data protection may be deemed as unique. However, several judicial decisions from the EU Courts and scholars have indicated that the EU Charter can also apply extra-territorially, so long as EU law is applicable.[63] Therefore, data protection rules are a byproduct of EU law and its international reach.

Weight

Another feature of data protection is that it is a very 'heavy' fundamental right in the context of balancing carried by the CJEU. The scale has often tilted in favour of data protection against the freedom of expression[64] or the ability of individuals to carry out journalistic activities.[65] Personal data as a fundamental right is subject to the rules of the EU Charter which require, for instance, that the essence of personal data protection is always respected, while instead its periphery can be derogated.[66] The violation of the essence of data protection remarkably led to the annulment of the Safe Harbour decision in the *Schrems I* case.[67] In that case, the CJEU granted comprehensive protection to data protection, and connected fundamental rights, over other interests, such as trade and data flow to third countries. The importance of data protection in balancing exercises is shared with

62 See Article 3 GDPR.
63 Eva Kassoti and Ramses A. Wessel, 'The EU's Duty to Respect Human Rights Abroad; The Extraterritorial Applicability of the EU Charter and Due Diligence Considerations' (2020) available at https://www.asser.nl/media/680298/cleer_020-02_web_final.pdf.
64 See *Google Spain* (n 8).
65 See Case C–345/17 *Buidvids*. EU:C:2019:122.
66 See Takis Tridimas and Giulia Gentile 'The Essence of Rights: An Unreliable Boundary?' (2019) GLJ 794.
67 See *Schrems I* (n 9).

other EU fundamental rights, such as the right to an effective remedy protected under Article 47 of the EU Charter.[68]

Enforcement framework

In addition to the enforcement that individuals can claim through individual remedies, public-oriented enforcement structure also underpins the framework of data protection rules in the EU, relying on the role of Data Protection Authorities (or DPAs). These bodies are the watchdogs of GDPR-application across Europe and are granted a crucial guarantee of being independent.[69] The independence of the DPAs is of the essence according to the relevant provisions that construe the meaning of data protection rules.[70] The independent nature of DPAs is instrumental both to ensure the freedom of those bodies from public powers, but also to effectively carry out activities that may require quasi-adjudicatory powers, such as the management of complaints under the GDPR.

Moreover, data protection is a peculiar fundamental right because of the tension that exists between transnational and national enforcement. While data can be produced and stored locally, data tends to travel beyond borders. Let us consider the possibility to access websites in any territory of the European Union, or the ability of data subjects to process their personal data beyond national borders. To regulate those instances, the GDPR provides rules on the transnational enforcement of data protection through the Cooperation and Consistency mechanisms.[71] The ability to enforce the GDPR in a transnational context is crucial to ensure data subjects' control over their personal data, even though the personal data moves across borders. At the same time, the tension between national and transnational enforcement of data protection rules has brought to the fore several questions and doubts on the reach of those rules, as well as the com-

68 See Case C-64/16 *Associação Sindical dos Juízes Portugueses v Tribunal de Contas* EU:C:2018:117, and the Polish judges saga, including cases such as C-*619/18 European Commission v Republic of Poland* EU:C:2019:531.

69 See Article 16 TFEU and Article 8 EU Charter of Fundamental Rights.

70 Case C-518/07 *Commission v Germany* EU:C:2010:125 para 23; Case C-614/10 *Commission v Austria* EU:C:2012:631 para 37; Case C-288/12 *European Commission v Hungary* EU:C:2014:237 para 51.

71 See Gentile and Lynskey (n 50).

petence of different bodies involved in the enforcement of this framework, such as the various DPAs of the member states or the EU institutions.[72]

Procedural legitimacy

Finally, data protection is a highly proceduralised fundamental right. The EU data protection framework lays down procedural duties imposed on data processors and controllers.[73] The existence of these procedures between the data subject, the data processor and the data controller influences the ways in which data protection as a fundamental right can be exercised. Examples are provided by the procedural rights that individuals enjoy vis-à-vis data processors and controllers, such as the right to access their data, the right to object to personal data processing, or the right to receive an explanation of the processing by the personal data processor. The presence of procedural elements in the GDPR framework points to a high level of input legitimacy, whereby data subjects, controllers and processors can engage in participatory procedures.[74]

Having set out the content and the peculiar features of data protection, the next section introduces the critiques to the effectiveness of data protection as a fundamental right and a framework more generally.

D. Critiquing EU data protection rules

There are essentially three arguments that underlie the contestation against EU data protection rules.

The first criticism is that data protection rules are the law of everything and everyone,[75] and for this reason their effective enforcement cannot be achieved. The argument suggests that the broad scope of data protection undermines its effectiveness. This is because the aspirations of the EU data protection framework cannot reasonably be met in light of the various constraints on enforcement bodies, time, and more generally resources

72 Ibid.

73 See Chapter 4 GDPR.

74 Alexander I Ruder, Neal D Woods, 'Procedural Fairness and the Legitimacy of Agency Rulemaking' (2020) 30(3), Journal of Public Administration Research and Theory 400, https://doi.org/10.1093/jopart/muz017.

75 See above.

for individuals.[76] A broad scope of application entails that individuals can invoke data protection rules in virtually all circumstances in which a form of personal information and data processing is involved. The GDPR's focus on individual remedies, while providing only limited collective, public remedies,[77] only exacerbates the inability to effectively enforce data protection. As a result, the burden of the data protection rules' enforcement lies on the shoulders of individuals who might not have the time or ability to consistently monitor how their personal data has been processed and whether this has been done lawfully.[78] In parallel to the focus on individual remedies, mention should be made of the complexity for GDPR public enforcement. The GDPR's broad scope also affects the ability of administrators to enforce data protection rules. Constraints such as budget, and a lack of staff limit the power of DPAs to proceed with all data protection complaints – and sometimes even to deal with them in an effective manner. Seen from the companies' perspective, the GDPR is also too cumbersome for companies that are overwhelmed with procedural requirements, and those mechanisms may not lead to meaningful protection. As discussed by Lynskey, data protection cannot be both effective and complete.[79]

There is also a second, powerful argument. The weight that Luxembourg courts have afforded the right to data protection in context of balancing has seldom obscured other fundamental rights and interests.[80] The oversized nature of data protection has established a form of constitutionalism that situates data protection at the peak of the hierarchy of values.[81] Hence, those who support freedom of expression as a higher value for democratic society compared to privacy and personal data processing will see an enemy in data protection.[82] This line of argument also underpins a feminist critique to EU data protection rules. Legal scholars have observed that the GDPR system is Eurocentric and tends to colonise the approach to fundamental

76 Lynskey (n 19).
77 See Article 80 GDPR.
78 See Gentile and Lynskey (n 50).
79 Lynskey (n 19).
80 David Erdos 'European Union Data Protection and Media Expression: Fundamentally Off Balance' (2016) 65(1) International and Comparative Law Quarterly 139.
81 Pollicino (n 42) at 137 and ff.
82 Erdos (n 80).

rights balancing in third countries[83] favoured by the extra-territorial reach of the GDPR.[84] The reach of personal data protection rules as developed in Europe leads to a form of balkanization of the fundamental rights landscape that compresses other perspectives on fundamental rights balancing across the globe.[85]

A third critique against data protection rules is the so-called business model critique,[86] which contradicts, to a certain extent, the previous critique. Several scholars have observed that the data protection framework reproduces innovation and market considerations linked to the digital markets' structures and actors, without providing meaningful protection to data subjects. Accordingly, while the framework provides an appearance of protective aspiration, in reality, it supports tech companies by subjecting the protection of personal data to the existing business structures.[87] An example on point is the impact assessment requirement developed under the GDPR.[88] As observed in literature, this procedure leads to limited, if not minimal, protection of personal data because of its formulaic dimension not necessarily conducive of enhanced protection for individuals.[89] The business model critique has also emerged as a result of judicial ex-post rationalisation of rules in light of Big Tech's business models. The *GC* case decided by the European Court of Justice is an instance of such ex-post rationalisation of data protection rules in light of the Big Tech's approach to data processing.[90]

Ultimately, these criticisms question the protection that individuals can derive from the current EU data protection framework, which is excessively broad in scope, tends to take over other fundamental rights when in conflict and is Eurocentric, and fosters a business model that may not be conducive of effective protection. Such critiques become even more press-

83 Jens T. Theilen, et al 'Feminist data protection: an introduction' (2021) 10(4) Internet Policy Review DOI: 10.14763/2021.4.1609. https://policyreview.info/articles/analysis/feminist-data-protection-introduction.

84 Ibid.

85 Pollicino, (n 42) at 137 and ff.

86 https://www.sciencedirect.com/science/article/pii/S0007681322001288.

87 Lynskey (n 19) at 324.

88 See Article 35 GDPR.

89 Eyup Kun, 'Questioning The Effectiveness of The Data Protectıon Impact Assessment under the GDPR In Time of COVID-19 Crisis' (June 30, 2020). Koronavirüs Döneminde Güncel Hukuki Meseleler Sempozyumu Bildiri Tam Metin Kitabı (İbn Haldun Üniversitesi Yayınları) 743, available at https://ssrn.com/abstract=4002566.

90 Lynskey (n 19) at 336.

ing when considering the legal systemic challenges of the digital society, including the rebalancing of individual protections vis-à-vis Big Tech companies, the reconciliation of fundamental rights and other interests, and the transnational enforcement of laws in the digital environment. Are EU data protection rules and the data protection fundamental-right-dimension developed in the EU an effective, resilient mechanism for the systemic challenges of the digital society?

As the following section will illustrate, the identified criticisms certainly have value and should not be taken lightly. Yet the controversy around data protection appears to have hijacked by several narratives that concern the field of fundamental rights more in general. Such lines of arguments have been subject to scrutiny and scholars have offered reflections to nuance them, thus shedding light on the value of human rights.[91] Hence, when considering those lines of arguments in the field of data protection, we should equally filter those claims, or else risk of falling prey of anti-human rights narratives. Only more nuanced critiques of data protection, as for any other fundamental right, can permit us to identify what to reform, what to maintain, and what to eliminate, especially in light of the advancement of the digital society and its systemic challenges.

E. The crisis of data protection as a human rights crisis: a rejoinder

The critiques of data protection both as a framework and as a fundamental right should be contextualised in the broader debate which has emerged in recent years *against* human rights. As a matter of fact, the criticisms raised against data protection mirror a broader crisis experienced by human rights.

Human rights (also called as 'fundamental rights' in a European context) are not an entirely recent idea or project. Woodiwiss[92] observed that Locke was among the first thinkers to argue that a series of entitlements belong to humans as such, regardless of the presence of a social contract under a natural law approach. These entitlements are grounded in freedom, equali-

91 de Búrca (n 30), Gráinne de Burca, 'Human Rights Experimentalism' (2015) Max Weber Lecture https://cadmus.eui.eu/bitstream/handle/1814/38110/MWP_LS_DeBurca_2015_02.pdf?sequence=1&isAllowed=y.

92 Anthony Woodiwiss *Human Rights*, (Routledge 2005) at 36.

ty and independence.[93] But since Locke, human rights have undergone a series of transformations and evolutions in conjunction with revolutions and wars. As a result of the World War II, human rights have entered the common language and the political agenda of various jurisdictions and international organisations. Authors have spoken of a new form of constitutionalism that draws from the expansive, protective power of human rights.[94] After a period of expansion in the 20th century, the criticisms have started arising. Prominent scholars such as Posner,[95] Moyn[96] and Hopgood[97] have advanced powerful arguments against the effectiveness of human rights. We can identify at least six criticisms that are currently questioning the value and effectiveness of fundamental rights, which, to a certain extent, also permeate the critiques of data protection explored above.

The first critique directed to human rights is a form of general contestation. Several authors also argued that human rights are too broad and ubiquitous, and for this reason, they are highly contested.[98] Human rights are abstract, aspirational, and searching a soul, using the language of Baxi.[99] This is akin to the 'law of everything' critique for data protection.

A second critique advanced against human rights is encapsulated by the expression 'money over values'.[100] The repeated financial crises that have affected Europe but also the rest of the world have put strain on the protection of fundamental rights. As a result, governments are pressured to deliver fundamental rights protections in a context of limited public resources. Under the current financial constraints, fundamental rights have become secondary to public budget considerations, thus fostering the idea

93 Ibid.
94 Richard Bellamy, 'Political constitutionalism and the Human Rights Act', (2011) 9(1) International Journal of Constitutional Law 86.
95 Eric Posner, *The Twilight of Human Rights* (OUP, 2013).
96 Samuel Moyn, *Not Enough: Human Rights in an Unequal World* (Harvard, 2019).
97 Stephen Hopgood, *The Endtimes of Human Rights* (Cornell University Press, 2015).
98 See literature cited at n 28.
99 Upendra Baxi 'Critiquing Rights: The Politics of Identity and Difference' in Aakash Singh Rathore and Alex Cistelecan Wronging Rights? Philosophical Challenges for Human Rights (Routledge, 2011), 61.
100 Rana S. Gautam, *Human Rights Practices During Financial Crises* (Springer, 2019), Emma Luce Scali, *Sovereign Debt and Socio-Economic Rights Beyond Crisis: The Neoliberalisation of International Law* (CUP, 2022).

that human rights ultimately entrench neo-liberalism in society.[101] As a matter of fact, the enforcement of fundamental rights can become particularly expensive when it comes to data protection rules. For instance, the enforcement requires several actions before courts or before administrations with a very complex technical dimension: initiating and advancing these actions is costly and demands financial resources. This criticism is linked to the 'law of everything' critiques discussed above insofar as it acknowledges that effective enforcement of data protection rules, whose scope of application is ever-expanding, depends on sufficient public resources, and as such cannot be fully achieved.

A third root of the crisis of human rights is legal complexity and polycentricity.[102] Fundamental rights are increasingly operating in a polycentric environment, where they may conflict not only with other general interests, but also with other fundamental rights. As a result, creating a hierarchy of values and of fundamental rights within legal orders has become highly contested and complex. This critique echoes the argument according to which during balancing exercises data protection is likely to overtake other values and objectives worthy of protection.

A fourth critique that has affected fundamental rights and that also shapes the crisis of EU data protection results from generalisation of failures. Specific failures of human rights have been generalised and weaponised against human rights. Because of these failings, the effectiveness of human rights as tools to protect the vulnerable has been questioned.[103] The same line of argument has emerged in the field of EU data protection. The limits to the enforcement of data protection rights emerged in cases like *GC*,[104] in which the CJEU has de facto allowed the processing of sensitive data against the wording of the GDPR, or the partial effectiveness of impact assessment under the GDPR[105] should not entail completely dismissing the value of data protection.

101 Samuel Moyn, 'A Powerless Companion: Human Rights In The Age Of Neoliberalism' (2014) 77(4) Law and Contemporary Problems, 147–169. http://www.jstor.org/stable/24244651; Susan Marks, 'Human Rights and Root Causes' (2011) 74(1) The Modern Law Review 57.

102 Jeff King 'Polycentricity' in Jeff King, *Judging Social Rights* (CUP, 2021) 189-210.

103 Fagan (n 28), Posner (n 28).

104 Case C-136/17 *GC* EU:C:2019:773.

105 Nóra Ni Loideain and Rachel Adams, 'From Alexa to Siri and the GDPR: The gendering of Virtual Personal Assistants and the role of Data Protection Impact Assessments' (2020) 36 Computer Law & Security Review 105366.

Last but not, human rights have been contested as a legal domain that has been progressively colonised by private powers. In other words, the public nature of those entitlements has been challenged by subjecting their realisation to private entities choices. For instance, the application of human rights such as the right to freedom of expression or due process by private bodies could lead to a form of responsive regulation that undermines the public nature of data protection rules.[106] Similarly, the application of data protection by private bodies bears the same risk of infusing private, tech-driven values in an area governed by public values, such as data protection. This criticism correlates to the business model critique explored above.

Clearly, human rights, including data protection, are under the spotlight. Yet this paper submits that human rights, and especially data protection, remain one of the most appropriate tools to face digital society's challenges. Human rights are essential for the protection of fundamental entitlements and new vulnerabilities precisely thanks to their expansive scope and their adaptability. Hence, fundamental rights can offer protections that may be crucial in the context of the digital society and could ultimately rebalance the imbalances of the digital society. Fundamental rights also offer a dialectic tool for legal reasoning in reconciling conflicting rights and interests, by providing special protection to certain values deemed essential in societies governed by the rule of law.[107] They also have universal aspirations that make them prone to transnational enforcement, although various constitutional systems may resist their advancement.[108]

Similarly, the EU fundamental right to data protection has *protective*, *dialogic* and *universal* aspirations that make it particularly suited to deal with the challenges of the digital society. The following sections illustrates the effectiveness of the fundamental rights' governance, before critically discussing the features of data protection as a fundamental right and their effectiveness.

106 See Kate Klonick 'The Facebook Oversight Board: Creating an Independent Institution to Adjudicate Online Free Expression' (2020) 129(8) Yale Law Journal 2418.

107 See Robert Alexy 'Constitutional Rights, Balancing and Rationality' (2003) Ratio Juris 16(2) 131; Takis Tridimas 'Wreaking the wrongs: Balancing Rights and the Public Interest in the EU Way' (2023) 29(2) Columbia Journal of European Law 185.

108 See the approach of the US to privacy and data protection, for a discussion see Pollicino (n 43) at 137 and ff.

F. The fundamental right governance of EU Data Protection

Protective

The EU fundamental right to data protection seeks to protect data subjects. It does so by empowering individuals to control their data and imposing obligations on data processors and controllers. The independence of DPAs is an essential feature highlighting the protective nature of EU data protection rules.[109] Fundamentally, the enforcement structure of the GDPR is in alignment with its protective intentions. That protecting role for the EU data protection framework should be preserved: in light of the advancement of the digital society, it would be short-sighted to limit the reach of data protection rules, insofar as they ensure the ability to scrutinise the conducts of tech companies relying on personal data. The varying perceptions of the harms caused by data protection violations should not be used to undermine its importance. A useful parallel is the right to vote or the right to paid leave: while not everyone may decide to exercise those fundamental entitlements, it does not mean that their centrality for democracy is lost.

The above observations do not aim to underestimate the challenges surrounding data protection rules. For instance, it has been extensively discussed how the consent model enshrined in the GDPR could lead to paradoxical situations where individuals cannot effectively control their data processing and become victims of dark patterns.[110] The very protective rationale for EU data protection rules would seem defeated. Another challenge to the protectiveness of data protection rules is the entanglement of those rules with economic considerations. Personal data is used by several entities as part of their business models. To empower data subjects, Malgieri and Custers advocated for the right to know the economic value of personal data, with the hope of increased awareness and empowerment concerning the fundamental right to data protection.[111] At the same time, it has been observed that subjecting the exercise of a fundamental right such

109 See Article 16 TFEU and Article 8 EU Charter.

110 Midas Nouwens et al, 'Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence' (2020) CHI Conference on Human Factors in Computing Systems available at https://arxiv.org/pdf/2001.02479; Cristine Utz et al, '(Un)informed Consent: Studying GDPR Consent Notices in the Field' (2019) CCS proceedings, available at https://dl.acm.org/doi/pdf/10.1145/3319535.3354212.

111 Gianclaudio Malgieri and Bart Custers 'Pricing privacy–the right to know the value of your personal data' (2018) 34(2) Computer Law & Security Review 289.

as that to data protection to the payment of a fee commodifies that entitlement and diminish its protectiveness. The EDPB observed that the 'Pay or Okay' model recently proposed by Meta, according to which that platform could charge users a fee to avoid the processing of their data, hinders the protective aspirations of data protection as a fundamental right.[112]

Regulators and enforcers have a crucial role in determining the content and application of data protection rules, and should be cautious not to water down its protective ambitions. The importance of data protection as a protective framework is also a matter of education and sensibility towards the increasing risks and threats posed by the digital society. The more the public becomes aware of the exploitation engendered by the digital environment, the more it can, and likely will action the protections afforded by the fundamental right to data protection in the EU.

Dialogue

The presence of procedural duties and rights under the GDPR enhances the input legitimacy of the framework. Through procedures, the parties involved in the enforcement of data protection rules can exchange their views and opinions in a dialogue aimed at identifying the correct interpretation of EU data protection rules, while also ensuring the achievement of data protection as a public value. Examples of iterative governance fostered by the GDPR are the Consistency and the Cooperation mechanisms that govern the transnational enforcement of data protection rules.[113] Through these procedures, DPAs, the EDPB, data processors and controllers and (although to a more limited extent) data subjects can participate in shaping the governance of personal data protection.

While the scrutiny entailed by the GDPR procedures may not be fully complete or effective,[114] it nonetheless opens a gate in the curtain of the tech companies' world and potential abuses of personal information for their own purposes. Such iterative dynamics, which involve national and European bodies as a form of experimental governance which, according

112 EDPB 'Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms' 17 April 2024 https://www.edpb.europa.eu/system/files/2024-04/edpb_opinion_202408_consentorpay_en.pdf.

113 See Chapter 7 GDPR, for instance.

114 Gentile and Lynskey (n 50).

to de Búrca,[115] is of the essence for the success of fundamental rights. The presence of various actors and channels of enforcement for data protection entitlements may not be a guarantee for effectiveness in the short term, but certainly stimulates critical considerations and ultimately long-term reflections on the enforcement strategies to adopt in the field. This becomes evident when considering the recent reforms and proposals[116] adopted by the EU Commission and the EDPB, which have both participated in a complex institutional negotiation for improving the future of GDPR, and supported by the public and academic discourses. Seen from another perspective, such a dialogue preserves the ability of individuals and public bodies to ensure the scrutiny of the behaviour of tech companies processing personal data. Such dialogic structures also allow market operators and companies acting as processors and controllers to input their views in the enforcement of EU data protection rules.

But frameworks imbued with procedural legitimacy considerations are not entirely free of risks. A crucial limitation is the potential undermining of *substantive* justice: the existence of procedures that seek to foster dialogue and input from all the parties involved in a dispute may not necessarily reach the *fairest* outcomes.[117] This is all the more likely in situations of imbalance of power that emerge in the digital environment, whereby individuals may not enjoy the same access to legal resources and advice as powerful tech corporations. These observations do not wish to dismiss the value of procedural legitimacy. On the contrary, it should be recalled that procedural justice is also interested in equality of arms, and thus has an equalising power.[118] In other words, the achievement of procedural justice and ultimately legitimacy lies in the ability of regulators and legal frameworks to address the disadvantages experienced by parties involved in a dispute to make their views heard. The procedures governing the enforce-

115 de Búrca, (n 30) at 10.

116 European Commission 'Data protection: Commission adopts new rules to ensure stronger enforcement of the GDPR in cross-border cases' 4 July 2023 available at https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3609. This proposal has received the green light from the Council, see Council of the EU 'Data protection: Council agrees position on GDPR enforcement rules' 13 June 2024 available at https://www.consilium.europa.eu/en/press/press-releases/2024/06/13/data-protection-council-agrees-position-on-gdpr-enforcement-rules/.

117 See David Thacher 'The Limits of Procedural Justice' in David Weisburd and Anthony Braga (eds.) *Police Innovation: Contrasting Perspectives* (CUP, 2019).

118 Cathérine Van de Graaf 'Procedural fairness: Between human rights law and social psychology' (2021) 39(1) Netherlands Quarterly of Human Rights 11.

ment of the EU fundamental right to data protection have the ambition and the ability to attain the demands of procedural justice, including equality of arms, so long as the regulators and enforcers of data protection address the imbalances of resources that may emerge from the digital environment.[119] Other fundamental rights, such as that to effective remedies and a fair trial included in the EU Charter, have already demonstrated their potential for strengthening the data protection as a fundamental entitlement.[120]

Universality

The EU fundamental right to data protection has a broad scope of application, even beyond the boundaries of the EU.[121] It also relies on several procedures and rules on international transfers, as well as the Cooperation and Consistency mechanisms that apply in the context of the transnational enforcement of the GDPR. Mention should be also made of the Council of Europe's Conventions 108 and 108+, both enhancing the broad application of data protection also beyond EU borders.[122] While these documents do not affect the application of EU rules on data protection, they strengthen the case of the universal aspiration of EU data protection as a fundamental right. Such universality facilitates transnational enforcement strategies that are necessary in the borderless digital environment. While contested as a form of colonialism and balkanisation,[123] the fundamental nature of EU data protection provides nonetheless protection beyond the EU borders to EU citizens invoking that right. In the increasingly inter-connected and globalised digital society, the universal ambition of data protection provides data subjects with entitlements and defences vis-à-vis instances of abuses of their personal data.

In light of the above discussion, the EU fundamental right to data protection offers a solid battleground for the risks and challenges of the digital society that digital constitutionalism seeks to address. Hence, its importance as an EU fundamental right should not be underestimated or undermined in future reform attempts. It would be short-sighted to lower

119 Gentile and Lynskey (n 50) at 808 and ff.
120 *Schrems I* and *II* (n 9).
121 See the *Schrems* cases (n 9) and Articles 2 and 3 GDPR.
122 See Council of Europe, 'Convention 108 +, Convention for the protection of individuals with regard to the processing of personal data' (2018).
123 Pollicino (n 42) at 130 and ff.

the protection offered by this fundamental right, especially in light of the advancement of the digital society and its intrinsic threats, including the rapid developments of artificial intelligence. Rather, such a fundamental right has already played and will continue to play a fundamental role in ensuring that technological developments maintain a human centric perspective aimed at protecting individual values such as autonomy and dignity. A fundamental right approach to the digital environment, such as that offered by data protection in the EU appears a first promising step in regulating the digital environment and its risks. Data protection, like all other fundamental rights, should not simply dismissed due to selected failures or inefficiencies. There is a value in fundamental rights that cannot be easily replicated by other legal instruments. All in all, the current fundamental right approach to EU data protection seems appropriate to face the challenges of the digital society and digital constitutionalism.

G. Conclusion

The digital society, with its challenges, is here to stay. The EU´s fundamental right to data protection has been applied by EU and national institutions in several crucial cases that have shaped the regulation of the digital environment in the EU and beyond. At the same time, data protection is one of the most contested legal frameworks and fundamental rights in the EU. It has been challenged by private parties, academics and institutions alike. Many of these criticisms contain elements of truth and valid observations that should be considered by regulators in future reforms of EU data protection rules. Yet this chapter has attempted to demonstrate that many of the criticisms affecting EU data of mirror more a more general contestation towards human right. Hence, the critiques towards data protection as a fundamental right and a framework more in general should be filtered. Only nuanced criticisms of data protection as a fundamental right, also taking into account its advantages to address the challenges of the digital society, can lead to a more strategic and better rethinking of that fundamental entitlement. The chapter has illustrated that the EU fundamental right to data protection has three features that make it particularly suitable to address the systemic challenges of the digital society and further the objectives of digital constitutionalism. These are its protective nature, its dialogic procedural structure and its universality. Data protection, like all other fundamental rights, should not simply be dismissed due to selected

failures or inefficiencies. There is a value in fundamental rights that cannot be easily replicated by other legal instruments.

The right to personal data protection in Brazil: The formation of a new fundamental right

Rodrigo Brandão

Abstract: This article describes the path taken to recognize personal data protection as an autonomous fundamental right in Brazil. It begins by analyzing how the Brazilian Constitution of 1988, in response to the indiscriminate processing of personal data by information agencies during the military regime, particularly safeguarded privacy. This protection was manifested through creating a legal remedy (habeas data), which was later replicated in other Latin American countries. However, the initial optimism was frustrated by the limited effectiveness of habeas data and a restrictive jurisprudence that confined privacy to protecting intimate and communication-flow data. The scenario begins to change in the second decade of the 21st century, with Brazilian jurists recognizing the fundamental right to data protection. Subsequently, the Supreme Federal Court's jurisprudence and a constitutional amendment formally incorporated it into the catalog of fundamental rights, reinforcing its effectiveness: safeguarding its core in the face of not only ordinary laws but also constitutional amendments, immediate applicability irrespective of legislative regulation, and prima facie priority when conflicting with other constitutional principles. Despite these advancements, Brazilian law still has a long way to go to define the essential aspects of the fundamental right to personal data protection, particularly delineating its scope, subjective and objective dimensions, and parameters for conflict resolution with other fundamental rights.

A. Privacy protection in the 1988 Constitution: frustrated optimism

The 1988 Brazilian Federal Constitution contains several provisions to safeguard different aspects of private life. The central provision is Article 5, Section X: "The intimacy, private life, honor, and image of individuals are inviolable, ensuring the right to compensation for material or moral damage resulting from their violation." Additionally, the Brazilian constitu-

tional tradition, initiated in the imperial Constitution of 1824[1] to protect the inviolability of the home[2] and the confidentiality of communications,[3] has been maintained.

A highly relevant innovation was the creation of habeas data, a procedural instrument designed for issues related to public databases containing personal information.[4] Some authors have derived a corresponding substantive right to access and rectify personal data from this new legal action.[5]

This was a clear response from the 1988 Brazilian Constitution to the use of personal information by the Brazilian military regime's security agencies, revealing its concern with the risks posed by public entities' broad processing of personal data.[6] This innovation had a notable influence in Latin America, given the typical scenario of overcoming military dictatorships where similar abuses were committed by "information communities."[7][8]

Despite the 1988 Constitution's favorable stance on privacy, a restrictive position regarding its scope initially prevailed, particularly concerning protecting personal data. Notably, the previous constitutional order's restrictive

1 Article 179.
2 Article 5º, XI, Brazilian Federal Constitution, 1988.
3 Article 5º, XII, Brazilian Federal Constitution, 1988.
4 Article 5º, LXXII, Brazilian Federal Constitution, 1988.
5 PERTENCE, Sepúlveda. Dois instrumentos de garantia de direitos: habeas corpus, ação popular, direito de petição, mandado de segurança individual e coletivo, mandato de injunção e habeas data. Seminário sobre Direito Constitucional. Série Cadernos do CEJ. Brasília: Conselho da Justiça Federal, 1992, p. 54.
6 Luís Roberto Barroso argues that these entities have become involved in ordinary politics, delving "into a murky terrain of persecutions against adversaries, often operating on the fringes of marginality." He asserts that "the community of information has become a parallel and aggressive power, which, at times, surpasses institutional political power, resorting to illicit means for condemnable ends." BARROSO, Luís Roberto. A viagem redonda: habeas data, direitos constitucionais e provas ilícitas. In: WAMBIER, Teresa Arruda Alvim (coord.). Habeas Data. São Paulo: Ed. RT, 1998.
7 It is the case, for example, in Colombia, Paraguay, Peru, Argentina, Ecuador, Venezuela, and Chile.
8 Before the 1988 Constitution, the states of Rio de Janeiro and São Paulo had advanced laws on the subject, as they provided for the right to access and rectify personal data, the linking to specific purposes, and the requirement of informed consent. Clémerson Merlin Cléve attributes to José Afonso da Silva the proposal for creating habeas data, which was already part of the draft Constitution prepared by the Afonso Arinos Commission. In this, the proposal was innovative, as it provided for a material right to the protection of personal data not only with the prerogatives of access and rectification but also with the prohibition of storing information about "political activities and private life." CLÈVE, Clèmerson Merlin. Habeas data: some reading notes. Habeas Data. WAMBIER, Teresa Arruda Alvim (ed.). Habeas Data. São Paulo: RT, 1998, p. 75.

orientation was maintained, indicating that obtaining personal information would be guided by the secrecy/access dichotomy, and the guarantee of secrecy would depend essentially on the connection of personal data to intimate issues.[9] Data related to specific individuals but not linked to their private lives would not be covered by constitutional protection.[10]

Also, only data in the flow of communication, not stored data, would be subject to protection. This position prevailed in the Brazilian Supreme Federal Court (STF) in the judgment of RE n. 418416-8/SC[11] when its rapporteur, Justice Sepúlveda Pertence, stated that Article 5, Section XII, of the 1988 Constitution, by explicitly referring to the "secrecy of telegraphic communications data" linked the terms "communications" and "data" in a way that protected only the secrecy of data in transit, not the data itself.[12][13]

---

9 DONEDA, Danilo. Da privacidade à proteção de dados pessoais: fundamentos da lei geral de proteção de dados. 3. ed. São Paulo: Thomson Reuters Brasil, 2021, p. 269.

10 STF (Supreme Federal Court), Full Bench, Case No. 418416-8/SC, Rapporteur Justice Sepúlveda Pertence, judgment on May 10, 2006. Indeed, the explicit codification of the fundamental rights to privacy and private life led to the interpretation that intimate information would be subject to legal protection, but not other information related to specific individuals. Thus, the possibility of third-party use of such information depended on its content, that is, its connection to privacy. Furthermore, the protection of privacy was essentially achieved through secrecy, i.e., the prohibition of third parties capturing and using such information rather than regulating the terms under which its processing would be permissible.

11 It was an extraordinary appeal filed against the judgment of the Santa Catarina Court of Justice that upheld the criminal conviction under Article 203 of the Penal Code: "to frustrate, through fraud or violence, a right secured by labor legislation.".

12 The theoretical foundation relied upon the influential article by Tércio Sampaio Ferraz Jr., who, in summary, considered that the term "data" referred to in Article 5, XIII, should be interpreted as "computer data," in line with the proposal of Manoel Gonçalves Ferreira Filho based on the premise that it was an innovation of the 1988 Constitution prompted by the evolution of information technology. Thus, confidentiality would be linked "to communication, in the interest of privacy," as confirmed by the literal wording of the provision, establishing a connection between the terms "data" and "communications." Therefore, "what violates the freedom to withhold thought is entering into someone else's communication, causing what should stay between private subjects to pass into the domain of a third party legitimately. FERRAZ JR., Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. Cadernos de Direito Constitucional e Ciência Política. Rt 1/77, 82. The article was also published in the Revista da Faculdade de Direito da Universidade de São Paulo, vol. 88, pp. 447, 1993.".

13 This guidance was reiterated, among others, in the case HC 91867/PA, where the legality of the conduct of police officers who, during the defendant's arrest on the spot, seized mobile phones and analyzed call records was being examined. It was found that the data on phone calls did not connect with "any constitutionally protect-

There is no doubt that the secrecy of intimate information and communication of personal data is an element that composes the scope of protection of the rights to privacy and confidentiality of communications. However, due to individuals being recognized in various spheres through profiles created from the collection and automated processing of their data, it seems clear that denying constitutional protection to personal data in general (including those stored or not directly related to intimate matters) poses severe risks to the free development of personality and, consequently, to the principle of human dignity in its autonomy aspect.

Another frustration occurred with the limited practical effectiveness of habeas data, contrasting with its symbolic impact beyond national borders. Several factors led to this result: first, the emphasis on the procedural aspect (creating a new constitutional action) and silence on the material dimension (subjective right to access and rectify personal data) must meet contemporary needs in addressing the issue. Second, the need for prior administrative requests and the cautious acceptance of the new institute by the courts, among other factors, significantly limited its effectiveness even for its typical purposes (access and rectification of personal information in public databases), let alone addressing contemporary challenges in the information society.

B. The beginning of the recognition in legal doctrine of the fundamental right to personal data protection

In international treaties and national constitutions, the express recognition of an autonomous fundamental right to personal data protection is still in its early stages. In this regard, Ingo Sarlet points out that "there is no express provision for a corresponding human right in the UN international system, as well as in the European and Inter-American Conventions, so that, for now, it is only possible to deduce such a right as implicitly enshrined through the work of the judicial bodies that oversee the interpretation/ap-

ed value," being a "mere numerical combination (that) in itself means nothing, just a phone number." Furthermore, following the cited precedent, it was stated that "the clause in Article 5, XII, of the Constitution cannot be interpreted to protect data as a record, registry deposit. Constitutional protection is for the communication 'of data' and not the 'data'." Supreme Federal Court (STF), 2nd Panel, HC 91867/PA, Rapporteur Justice Gilmar Mendes, judgment on April 24, 2012, rapporteur's vote p. 9.

plication of treaties, which, by the way, still occurs to a large extent in the case of constitutions."[14]

In Brazilian law, even before Constitutional Amendment (EC) No. 115/2022 and paradigmatic judgments of the Supreme Federal Court (STF), some authors had already spoken in favor of the autonomy of the right to personal data protection about privacy. For example, Ingo Sarlet emphasizes that the scope of protection of the former is broader than that of the latter, as it would encompass all data that allows the identification of a specific person. Furthermore, he recognizes it as a materially fundamental right because "it does not pose a greater difficulty in demonstrating its relevance to the individual sphere of each person and to the collective interest (of organized society and the State), of the values, principles, and fundamental rights associated with the protection of personal data and protected by it. In this sense, he highlights, among others, the principle of human dignity, the right to free development of personality, and the right to privacy."[15]

In the same vein, Laura Schertel Mendes notes that, given the extensive protection of personality and private life, it makes no sense to exclude the protection of personal data from its scope, as nowadays privacy is much more at risk due to the massive and automated collection of personal data than by "traditional methods," such as paparazzi and sensationalist newspapers.[16]

As early as 2011, Regina Linden Ruaro, Daniel Piñeiro Rodriguez, and Brunize Finger advocated for the autonomy of the right to data protection, arguing that privacy had emphasized "exclusively individual protection

14 SARLET, Ingo. Fundamentos constitucionais: o direito fundamental à proteção de dados. In: MENDES, LAURA Shertel; DONEDA, Danilo; SARLET, Ingo; RODRIGUES JR., Otávio Luiz (org), Coordenador Executivo BIONI, Bruno. Tratado de Proteção de dados pessoais. Rio de Janeiro: Forense, 2021, p. 26.

15 SARLET, Ingo. Fundamentos constitucionais: o direito fundamental à proteção de dados. In: MENDES, LAURA Shertel; DONEDA, Danilo; SARLET, Ingo; RODRIGUES JR., Otávio Luiz (org), Coordenador Executivo BIONI, Bruno. Tratado de Proteção de dados pessoais. Rio de Janeiro: Forense, 2021, p. 28/9.

16 MENDES, Laura Shertel: Habeas Data e autodeterminação informativa: os dois lados de uma mesma moeda. In: MENDES, Laura Shertel; ALVES, Sérgio Garcia; DONEDA, Danilo. Internet e Regulação. São Paulo: Saraiva, 2021, p. 309.

instruments," while advances in data processing make it imperative to enhance the State's duties to protect the individual.[17]

These doctrinal contributions were crucial for the Supreme Federal Court to begin recognizing that, even before being formally enshrined in the 1988 Constitution, protecting personal data already constituted an implicit fundamental right autonomous about privacy.

C. New perspectives in the jurisprudence of the Supreme Federal Court

The beginning of a new phase in the jurisprudence of the Supreme Federal Court (STF), more attuned to contemporary needs in personal data protection, can be considered with the judgment of RE No. 673,707. It originated as a habeas data filed to ensure access to information from the Corporate Checking Account System of the Federal Revenue Service (SINCOR).[18] On this occasion, the Brazilian Supreme Court overturned the decision of the 1st Region Federal Court of Appeals, which had denied the existence of a duty for the Federal Revenue to provide "complex, burdensome, and general information from a non-public registry. "Instead, the STF considered that taxpayers have the right to access information stored in a database managed by the Federal Revenue to preserve "the status of their name, business planning, investment strategy, and especially the recovery of wrongly paid taxes."

Beyond the result itself, it is noteworthy that the rapporteur defined the habeas data's object broadly, based on an equally comprehensive concept of databases, "understood in its broadest sense, encompassing everything related to the interested party, whether directly or indirectly." Thus, it aligned with the concept of personal data as any information referring to a specific individual. Moreover, Justice Gilmar Mendes envisioned the possibility of the case becoming "the starting point for a revitalization of habeas data

17 RUARO, Regina Linden, RODRIGUEZ, Daniel Piñeiro, FINGER, Brunize. O Direito à Proteção de Dados e a Privacidade. Revista da Faculdade de Direito - UFPR, Curitiba, n. 53, p. 45/67, 2011, p. 10.

18 Supreme Federal Court (STF), Full Bench, Appeal Number: RE 673,707, Rapporteur: Justice Luiz Fux, Date of Judgment: June 17, 2015. Publication: DJe (Electronic Justice Diary) on September 30, 2015.

in a broader perception, beyond procedural issues, turning towards the recognition of a fundamental right to informational self-determination."[19]

This new phase was consolidated with the paradigmatic judgment of ADIs 6387, 6388, 6390, and 6393,[20] in which the interim decision of the rapporteur, Justice Rosa Weber, was endorsed by the majority of STF members to suspend the effectiveness of Provisional Measure No. 954/2020.

According to Article 2: "telecommunications companies providing Fixed Switched Telephone Service (STFC) and Personal Mobile Service (SMP) must make available to IBGE, electronically, the list of names, telephone numbers, and addresses of their consumers, individuals or legal entities." This provision mandated telecommunications companies to provide a pervasive set of data about their service users to the Brazilian Institute of Geography and Statistics (IBGE), "for the official statistical production, to conduct non-face-to-face interviews within the scope of household surveys" (Article 2, § 2).

Despite the formal limitations of the provisional measure,[21] Justice Rosa Weber considered that "such information, related to the identification – actual or potential – of a natural person, constitutes personal data and, in this measure, falls within the scope of protection of constitutional clauses ensuring individual freedom (Article 5, caput), privacy, and the free development of personality (Article 5, X and XII). Its manipulation and treatment, therefore, must observe, at the risk of harm to these rights, the limits outlined by constitutional protection. Derivatives of the rights of personality, respect

19 In this context, as Laura Schertel Mendes aptly pointed out, "if the Constitution provides habeas data as a procedural guarantee available to the individual to access or correct data concerning them, it is logical to assume that there is a substantive right supporting this procedural guarantee: the fundamental right to data protection or the right to informational self-determination, to use the terminology of German law." MENDES, Laura Shertel: Habeas Data e autodeterminação informativa: os dois lados de uma mesma moeda. In: MENDES, Laura Shertel; ALVES, Sérgio Garcia; DONEDA, Danilo. Internet e Regulação. São Paulo: Saraiva, 2021, p. 305.

20 "Supreme Federal Court (STF), Full Court, Rapporteur Justice Rosa Weber, Judgment on May 7, 2020."

21 Article 3 aimed to establish limitations on the use of such data, safeguarding its confidential nature (i), its connection to the purpose above (ii), the prohibition of its use as evidence in administrative, fiscal, or judicial proceedings (iii), its availability to other public entities (§ 1), and, after its use, the obligation to disclose the situations in which the data were used and a report on the impact on the protection of personal data (§ 2). On the other hand, Article 4 provided that once the emergency situation resulting from the coronavirus pandemic was overcome, the information would be eliminated.

for privacy, and informational self-determination were stated in Articles 2, I, and II of Law No. 13,709/2018 (General Data Protection Law) as specific foundations of personal data protection regulation."

Justice Luís Roberto Barroso stated that the case involved a typical case of balancing constitutional principles: on one side, statistics as a tool aimed at providing reliable data for the conception and implementation of public policies; on the other side, privacy, "which is the right that every person has to have an area of their life that is not accessible, either to the State or to other people, except, possibly, by their own will."

He emphasized initially that objective and reliable data are essential for the development of public policies by the state and for economic growth (given that valuable contemporary companies mainly have data processing as their primary asset). Although the "internet industrial revolution" with the notable expansion of capturing and processing personal data, has provided "great advantages," especially in communication, it has also brought "serious risks and threats," such as disinformation campaigns, defamation, hate speech, deepfakes, robotized digital militias, hacking, misuse of data for political purposes, etc.

Despite assigning enormous importance to data, he considered that, since the provisional measure did not provide security elements regarding the precautions for its sharing and there was no prior debate about what those measures would be, there was a significant risk of misappropriation of this data, leading to privacy damage.

In his significant vote, Justice Gilmar Mendes also advocated for the autonomy of the fundamental right to protect personal data. In his words: "The affirmation of the autonomy of the fundamental right to the protection of personal data - it must be said - is not contingent on mere theoretical enchantment but rather on the inescapable need to assert fundamental rights in contemporary democratic societies. It also recognizes the dual dimension of this right because it involves, from a subjective perspective, the protection of the individual against the risks that threaten their personality in the face of the collection, processing, use, and circulation of personal data, and, from an objective perspective, the attribution to the individual of the guarantee to control the flow of their data."

Similarly, Justice Luiz Fux acknowledged that "the protection of personal data and informational self-determination are autonomous fundamental rights, which involve specific legal protection and scope of application. These rights are derived from the integrated interpretation of the guarantee of the inviolability of intimacy and private life (Article 5, X), the principle

of human dignity (Article 1, III), and the procedural guarantee of habeas data (Article 5, LXXII), all provided for in the 1988 Federal Constitution."

The decision is relevant for several reasons, notably the recognition of the right to informational self-determination due to individual freedom, privacy, and the free development of personality. Additionally, the Court stated that the Head of the Executive Branch needed to demonstrate that the measure would be necessary to protect a legitimate public interest, not even providing minimal clarification on how and for what purpose this massive amount of data would be used.

Despite formally establishing its "secrecy" and prohibiting sharing with other public agencies, it "does not present technical or administrative mechanisms capable of protecting personal data from unauthorized access, accidental leaks, or misuse," failing to adequately protect the mentioned fundamental rights, which were aggravated by the non-enforcement of the General Data Protection Law (LGPD) at the time.

Finally, note that the inherent exceptionality of the pandemic raised debates about the relativization of privacy standards.[22] The Supreme Court's decision, by rejecting the generic argument of the "state of sanitary exception" and by requiring concrete measures to safeguard the right to personal data protection, demonstrated faithful compliance with its role as the guardian of fundamental rights, which is especially important and challenging in crisis contexts such as the COVID-19 pandemic.

D. The Material and Formal Foundations of the Fundamental Right to Data Protection

On February 10, 2022, the National Congress approved Constitutional Amendment Project (PEC) No. 17/2019, which became Constitutional Amendment (EC) No. 115/2022, as follows:

> "Art. 1 The twelfth item of article 5 of the Federal Constitution shall be amended to read as follows:
> 'Article 5 (...)
> XII – the confidentiality of correspondence and telegraphic, data, and telephone communications is inviolable, except, in the latter case, by judicial order, in the situations and the manner established by law for

22 VÉLIZ, Carissa. Privacidade é poder: por que e como você deveria retomar o controle de seus dados. 1. ed. São Paulo: Editora Contracorrente, 2021, p. 74/5.

criminal investigation or criminal procedural instruction, as well as the right to the protection of personal data, including in digital media.'
Art. 2 The heading of article 22 of the Federal Constitution shall be amended to include the following item XXX:
'Article 22 (...) XXX – **protection and processing of personal data**.' (Emphasis added) [23] "

The constitutional amendment, besides granting exclusive competence to the Federal Union to legislate on 'the protection and processing of personal data,' included the right to the protection of personal data in the list of Article 5 of the Brazilian Constitution, which contains the list of fundamental rights. There is no doubt that it is formally a fundamental right in Brazil. This innovation is essential to bring certainty to the application of the constitutional effectiveness inherent in the legal regime of fundamental rights to the protection of personal data, even though the doctrinal and jurisprudential orientation presented in the previous topics, which considered it a material fundamental right, seems correct.

Indeed, Article 5, paragraph 2 of the Brazilian Constitution contains an opening clause in the constitutional catalog of fundamental rights, as it recognizes the material fundamentality of other rights 'arising from the regime and principles adopted by it or from international treaties in which the Federative Republic of Brazil is a party.' Despite doctrinal controversies about the substantive requirement for identifying these 'other rights,' the right to personal data protection fulfills the main criteria, especially the constitutional relevance of its content to the community. It cannot be entirely left to regulation by the ordinary legislator,[24] and its indispensability for protecting the dignity of the human person is evident.[25] This is crucial in the face of the relevance of protecting personal data for individual autonomy against oppressive measures by public and private entities.

Therefore, its material fundamentality seems clear. This conclusion is reinforced when analyzing the concern of the 1988 constituent in safeguarding privacy (Article 5, X), particularly personal data in public databases, with the provision of habeas data in Article 5, LXXII. Furthermore, recog-

23 SARLET, Ingo Wolfgang. A Eficácia dos Direitos Fundamentais. 9. ed. Porto Alegre: Livraria do Advogado, 2009, p. 90/156.
24 ALEXY, Robert. Teoría de los derechos fundamentales. Madrid: Centro de Estudios Constitucionales. 1997.
25 ANDRADE, José Carlos Vieira. Os direitos fundamentais na constituição portuguesa de 1976. 2. ed. Coimbra: Almedina, 2001.

nizing the autonomy of this right concerning privacy is significant in the current context of the information society.[26] There is no doubt about the proximity between these rights and overlapping areas in their scopes, which is common when dealing with fundamental rights.

This is evident not only in cases of access and processing of sensitive personal data (e.g., philosophical and religious beliefs, health, sexual orientation etc.), but also in cases of personal data that, although not initially exposing the private life of the holder (civil identification document, profession, marital status etc.), when processed extensively by artificial intelligence tools to create 'profiles' of their holders,[27] captured by internet usage surveillance tools, and used for purposes other than those that led to their capture, may raise excessive exposure of the individual's private life.

The image of continuous monitoring of the individual - at home by voice assistants, computers, and 'smart' appliances, and on the street by cameras, sensors, and Wi-Fi networks - highlights the privacy risks. The formation of these digital profiles or 'digital dossiers' and the circumstance of the natural person being somewhat hostage or stigmatized by a kind of 'digital biography' indicates that the right to know and rectify personal data in these databases is more directly connected to the general clause of personality protection and the dignity of the human person as autonomy than to privacy. It aims to safeguard the person's ability to make free decisions. It does not seek to protect the secrecy of intimate information but only the accuracy of personal data processed in an automated manner.

On this point, Stefano Rodotà clarifies that privacy traditionally has been attributed a negative and static dimension, guided by the possibility of the holder denying third parties' access to intimate information. The right to personal data protection does not follow this logic of secrecy, as it recognizes the possibility of third-party collection and processing of personal data, providing, however, powers to the data subject to ensure control measures over these activities.[28]

---

26 Manuel Castells argues that contemporary society is characterized by "a new informational mode of development, in which the source of productivity lies in knowledge generation technology, and information and knowledge are the central actors in economic production." CASTELLS, Manuel. A sociedade em rede. 3. ed. São Paulo: Paz e Terra, 2000.

27 SOLOVE, Daniel. The Digital Person: technology and privacy in the informational age. New York: New York University Press, 2004, p. 3.

28 RODOTÁ, Stefano. A vida na sociedade de vigilância: a privacidade hoje. (org. Maria Celina Bodin de Moraes). Rio de Janeiro: Renovar, 2008.

Thus, although it has close connections with privacy, the right to protect personal data plays autonomous and relevant roles in the current information society. The perception of how the formation of digital profiles implies the 'categorization of people' that radically conditions their economic and existential opportunities indicates that the massive collection of personal data can lead to a 'data dictatorship,'[29] diminishing individual freedom. Damages can also be caused by equality, as algorithms may reproduce biases of those who conceived them, further reduce opportunities for disadvantaged groups, and promote arbitrary distinctions between people.

The Chinese social credit system is an example of how indiscriminate data collection can be oppressive to citizens. It involves using big data for the massive collection of personal data, and its application to all areas of life, guided by moral standards of credibility. As Carissa Vèlez explains, 'Good actions earn you points, and bad actions make you lose points. Buying diapers earns you points. Playing video games, buying alcohol, or spreading fake news makes you lose points.'[30] The significant repercussions in the lives of citizens - advantages or disadvantages in waiting lists, prices of public and private services, access to work and credit, have even led to the prohibition of millions of Chinese citizens buying air and high-speed train tickets and the installation of cameras at home doors for the government to check if people complied with quarantine during the pandemic - make evident the risk to individual freedom.

The protection of freedoms presupposes a certain degree of ignorance about human behaviour. This draconian scenario of authoritarian regimes helps make even more evident the risks generated by the massive collection of data for categorizing people based on digital profiles, even in democratic societies. This phenomenon can restrict access to relevant economic and existential opportunities and establish unreasonable discriminations between people based on mechanisms that are not transparent outside public and private entities that collect and process them (or their respective agents with powers of command over such activities).

The exponential development of these technological mechanisms for collecting and processing personal data and the multiple economic and political uses that technological evolution has allowed have made information,

29 MAYER, Jonathan; NARAYANAN, Arvind. Do not track universal web tracking opt-out. IAB Internet Privacy Workshop Position Paper, Nov. 2010.

30 VÉLIZ, Carissa. Privacidade é poder: por que e como você deveria retomar o controle de seus dados. 1. ed. São Paulo: Editora Contracorrente, 2021, p. 87.

which has always represented a source of power and wealth, the main asset of contemporary societies. In this context, the affirmation of a fundamental right to the protection of data, autonomous concerning privacy, freedom, and other fundamental rights, fulfills the notable function of making any activity of collecting and processing personal data a restriction to the respective fundamental right, raising the need for special justification in the light of its reinforced constitutional effectiveness.

As in other countries, particularly in the European context, the 'recognition' of this new fundamental right in Brazil was the result of a rich contribution between members of civil society, law professors, and judges who paved the way for its subsequent recognition by the legislator (in the Brazilian case, by a constitutional amendment, which positively distinguished our experience by formally linking the protection of this right to the constitutional sphere and the reinforced effectiveness of fundamental rights).

The power of public and private entities benefiting from the massive use of personal data, the lack of transparency in data collection and processing methods, and the high political and economic value of this data in today's information society reveal that recognizing the formal and material foundations of the right to data protection, while crucial, is only the first step on a challenging path.

It will be the task of Brazilian legal doctrine to develop the scope of protection, the subjective and objective dimensions, and the horizontal effectiveness of this fundamental right, among other elements inherent in the grammar of fundamental rights. Courts, particularly the Supreme Federal Court, will face complex issues regarding its practical application, revealing a tension between, on one side, public and private entities interested in the massive processing of personal data for various purposes (national security, efficiency in providing public services, creating new businesses, profit, etc.), and on the other, individuals (and public and private actors supporting their cause) interested in preserving some control over the management and use of their data.

Striking a balance between protecting human dignity, freedom, equality, and transparency in data management in the face of free enterprise, economic development, and preserving trade secrets will take a lot of work. This challenge is also felt by lawmakers, as evidenced by the approval of laws such as “Lei Geral De Proteção de Dados” (LGPD, Law No. 13.709/2018, our General Data Protection Law) and the intense debates in the National Congress on combating misinformation and hate speech on the internet

and regulating artificial intelligence. Although challenging, this is a doctrinal, jurisprudential, and legislative agenda and an essential political debate for preserving human dignity in the face of the challenges posed in Brazil by the overwhelming pace of digitization in the 21st century.

III.
AI, Consumer Protection, and Online Governance in a Digital World

The Regulation of Disinformation in the EU – Overview and Open Questions

Alexander Peukert[*]

Abstract: This article provides an overview of the current state of the regulation of disinformation in the EU. It shows that the concept of disinformation, the purpose of anti-disinformation measures and their content and enforcement can only be understood if a holistic view is taken of private, hybrid-co-regulatory and public law norms. The delicate field of disinformation is to a large extent dealt with outside of statutory law. The questions raised thereby are largely unresolved.

A. The Short History of Disinformation Regulation

"Disinformation" is a shimmering term. In the interim, it can be defined as a statement which is false or otherwise misleading and which has a negative impact on public interests, but which is not in itself unlawful.[1] State measures against such "harmful" content are delicate because they constitute an interference with communicative freedoms going beyond the general laws and the rights of third parties.[2] And indeed, Union law knows neither a legal definition nor an explicit legal prohibition of disinformation.[3]

---

* This is a translation of the article "Desinformationsregulierung in der EU: Überblick und offene Fragen", JuristenZeitung 2023, 278-286. Work on this article was completed in March 2023.

1 For more details see below, B.

2 High level group on fake news and online disinformation, A multi-dimensional approach to disinformation, 2018, 19 ('government or EU regulation of disinformation can be a blunt and risky instrument'); preamble lit. c Strengthened Code of Practice on Disinformation 2022, https://disinfocode.eu (in the following: Disinformation Code 2022) ('delicate balance').

3 Cf. European Commission, COM(2020) 825, 10; Pamment, The EU's Role in Fighting Disinformation: Crafting A Disinformation Framework, 2020, 2 et seq. One exception can be found in Lithuanian law, which prohibits the dissemination of disinformation in the media; cf. European Audiovisual Observatory, Mapping of national rules applicable to video-sharing platforms: Illegal and harmful content online, 2022, 290.

Nevertheless, the EU institutions have taken or promoted numerous measures against disinformation since 2015. According to the "European Declaration on Digital Rights and Principles for the Digital Decade" of 15 December 2022, there will be no change to this policy in the foreseeable future. This is because the Commission, Parliament and Council solemnly proclaim in this Declaration to continue their "fight" against disinformation in order to "create a digital environment in which people are protected from disinformation and information manipulation and other forms of harmful content, including harassment and gender-based violence".[4]

This policy goal enjoys broad support in social science and legal literature. According to this view, disinformation in the internet age poses a significant challenge to liberal Western-style democracies that requires regulation.[5] Firstly, due to the openness of political debate, these pluralistic societies are said to be in principle more susceptible to informational manipulation than autocratic systems.[6] Secondly, the functional logic of the Web 2.0 intensifies the dangers that have always emanated from false and misleading statements. Disinformation is easily created with digital tools such as image manipulation, spreads rapidly via social networks and other online services, and can be artificially amplified by manipulative measures such as bots.[7]

Three examples in particular are cited in academia and politics as evidence for these assumptions: disinformation campaigns by the Russian

4 Chapter IV no. 15 and lit. c European Declaration on Digital rights and Principles for the Digital Decade, 26.1.2022, https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles; OECD Declaration on a Trusted, Sustainable and Inclusive Digital Future, OECD/LEGAL/0488, 15.12.2022 (combatting disinformation online).

5 Literature overviews at Kapantai et al, New Media & Society 23(5) (2001), 1301 et seq.; de Place Bak/Walter/Bechmann, New Media & Society 2022, https://doi.org/10.1177/14614448221122146. Support can be found in legal academia, for instance in Hong, Rechtswissenschaft 2022, 126, 173; Kuhlmann/Trute, GSZ - Zeitschrift für das Gesamte Sicherheitsrecht, 2022, 115; with reservations Peukert, Kritische Vierteljahresschrift für Gesetzgebung und Rechtswissenschaft, 2022, 57, 75 et seq.

6 Cf. Schünemann, in: Cavelty/Wenger (eds.), Cyber Security: Socio-Technological Uncertainty and Political Fragmentation, 2022, 32, 33 with further references.

7 Recital 5 sentence 2 Regulation 2022/2065 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), OJ L 277/1 (in the following: DSA); European Commission, COM(2018) 236, 6 et seq.; Bennett/Livingston, European Journal of Communication 33(2) (2018), 122 et seq.; de Place Bak/Walter/Bechmann, New Media & Society 2022, https://doi.org/10.1177/14614448221122146.

government in the context of the Ukraine conflict (since 2014/2015),[8] "fake news" in the context of domestic events such as the Brexit referendum and the election of Donald Trump in 2016/2017,[9] and health-related disinformation on vaccines and other public health policies during the COVID-19 pandemic,[10] all of which served as catalysts for the regulation of disinformation.

In March 2015, the Council requested the then High Representative of the EU for Foreign Affairs and Security Policy to develop an action plan to counter Russia's disinformation campaigns.[11] As a result, the "East StratCom [Strategic Communication, A.P.] Task Force" was set up within the framework of the European External Action Service, which since September 2015 has been countering Russian disinformation in three fields of action by making EU communication more effective with regard to the countries of the Eastern Partnership, strengthening free and independent media in this region, and collecting examples of disinformation and presenting and correcting them on the website euvsdisinfo.eu as part of an awareness-raising campaign.[12] Germany reacted to the phenomenon of "fake news" in autumn 2017 with the Network Enforcement Act. At the end of that year, the Commission set up a high-level group of experts, which recommended numerous measures in March 2018, which in turn found their way into the ground-breaking Commission Communication

8 European Commission, JOIN(2018) 36, 5; European Commission, COM(2020) 790, 24.

9 de Place Bak/Walter/Bechmann, New Media & Society 2022, https://doi.org/10.1177/14614448221122146; Zimmermann/Kohring, M&K Medien & Kommunikationswissenschaft 66 (2018), 526 et seq.

10 On vaccination-related disinformation, see European Commission, JOIN(2018) 36, 4 et seq. and no. 9 lit. c Council Recommendation of 7.12.2018 on strengthened cooperation against vaccine-preventable diseases, OJ C 466/1. On the COVID-19 'infodemic' see WHO Coronavirus disease 2019 (COVID-19) Situation Report – 45, 5.3.2020; European Commission, JOIN(2020) 8; Kapantai/Christopoulou/Berberidis, New Media & Society 23(5) (2021), 1301, 1304.

11 http://www.consilium.europa.eu/de/press/press-releases/2015/03/20/conclusions-european-council/; Pamment, The EU's Role in Fighting Disinformation: Taking Back the Initiative, 2020, 7 ('In response to representations from a small group of concerned member states, the European Council ‚stressed the need to challenge Russia's ongoing disinformation campaigns' in March 2015.').

12 https://euvsdisinfo.eu/to-challenge-russias-ongoing-disinformation-campaigns-the-story-of-euvsdisinfo.

"Tackling online disinformation: a European Approach" of 26 April 2018.[13] The most important outcome of these activities was the EU Code of Conduct "tackling online disinformation", signed in October 2018, in which the major platform operators and advertising service providers (Facebook, Google, Twitter, and later also Microsoft and TikTok) committed to taking 15 measures against disinformation, including highlighting the accessibility of trustworthy content.[14] Finally, the COVID-19 pandemic proved to be a "test case" of the anti-disinformation measures previously taken, and a "stress test" for the Code of Conduct.[15] In response to a request from the Commission, the online platforms participating in the Code published monthly reports on their rules and measures against pandemic-related disinformation from August 2020 onwards.[16]

However, in the Commission's view, this additional transparency measure only revealed the structural weaknesses of the first Disinformation Code, which suffered from unclear definitions, unspecific obligations and, not least, a lack of sanctions.[17] For this reason, the Commission called on the signatories of the Code as well as other relevant actors (especially from the advertising industry) to participate in a revision and strengthening of the Disinformation Code 2018. The Commission provided itself with the leverage for this move in December 2020 by proposing the Digital Services Act (DSA).[18] From then on, the Commission emphasized that strengthening the Code "offers an early opportunity for stakeholders to de-

13 Cf. High level group (n 2); European Commission, COM(2018) 236, 3; European Commission, JOIN(2018) 36. On the origins of the German Network Enforcement Act (NetzDG) and its effects, see Peukert, in: Spiecker gen. Döhmann/Westland/Campos (eds.), Demokratie und Öffentlichkeit im 21. Jahrhundert – zur Macht des Digitalen, 2022, 229 et seq. Considerably more hesitant the Joint Declaration of the Special Rapporteur on Freedom of Opinion and Expression of the UN, the OECD, the Organization of American States and the African Commission on Human and Peoples' Rights, 3.3.2017, FOM.GAL/3/17, Freedom of Expression and 'Fake News', Disinformation and Propaganda.

14 No. (ix) Code of Practice on Disinformation https://digital-strategy.ec.europa.eu/en/library/2018-code-practice-disinformation (in the following: Disinformation Code 2018); cf. European Commission, SWD(2020) 180.

15 European Commission, JOIN(2020) 8, 19; European Commission, COM(2021) 262, 3 et seq.

16 European Commission, JOIN(2020) 8, 10; the reports are available at https://digital-strategy.ec.europa.eu/en/policies/covid-19-disinformation-monitoring.

17 European Commission, SWD(2020) 180, 18.

18 European Commission, COM(2020) 825.

sign appropriate measures in view of the adoption of the proposed DSA".[19] The "Strengthened Code of Practice on Disinformation 2022" (Disinformation Code 2022) was negotiated in the shadow of the DSA legislation and more recently also of the Ukraine war. It was signed by the major tech companies in June 2022 and explicitly refers to the DSA, which had not yet been enacted at that time.[20] The last building block of the regulation of disinformation in the EU followed on 19 October 2022 with the adoption of the DSA, whose liability rules and due diligence obligations for providers of intermediary services and search engines will enter into force on 17 February 2024.[21] Its recitals use the term "disinformation" no less than 13 times, including in the teleologically central Recital 9, according to which the DSA is to ensure a "safe, predictable and trusted online environment" and to address "the dissemination of illegal content online and the societal risks that the dissemination of disinformation or other content may generate".[22]

The following article provides an overview of the current state of the regulation of disinformation in the EU. It will become apparent that the concept of disinformation (see B), the purpose of anti-disinformation measures (see C) and their content and enforcement (see D) can only be understood if a holistic view is taken of private, hybrid-co-regulatory and public-law norms.[23] The delicate field of disinformation is to a large extent dealt with outside of statutory law. The questions raised thereby are largely unresolved (see E).

B. The Concept of Disinformation

The very definition of "disinformation" is derived from non-state norms. The DSA only defines the term "illegal" content, namely as "any informa-

19 European Commission, COM(2021) 262, 2 et seq. Cf. German Federal Government, Bundestags-Druckssache 20/2308, 5 et seq. ('Moreover, the DSA will raise the previously self-regulatory 'Code of Conduct for Disinformation' to a stronger co-regulatory EU instrument.'); Kuhlmann/Trute, GSZ - Zeitschrift für das Gesamte Sicherheitsrecht, 2022, 115, 119 et seq.

20 Cf. preamble lit. h, i and j as well as Commitment 44 Disinformation Code 2022 (n 2); on this Kuhlmann/Trute, GSZ - Zeitschrift für das Gesamte Sicherheitsrecht, 2022, 115, 122 (cooperative mechanism).

21 Art. 93 DSA.

22 Recitals 2, 9, 69, 83, 84, 88, 95, 104, 106, 108 DSA.

23 Cf. Peukert, Modi der Plattformregulierung, Arbeitspapier des Fachbereichs Rechtswissenschaft der Goethe-Universität Frankfurt am Main 4/2022.

tion that, in itself or in relation to an activity … is not in compliance with Union law or the law of any Member State … irrespective of the precise subject matter or nature of that law".[24] The DSA consistently distinguishes "illegal" from "otherwise harmful" information and activities, which may be incompatible with the terms and conditions of the service providers and therefore may be the subject of content moderation activities.[25] The example most frequently mentioned in the recitals for non-illegal but "otherwise harmful" content is "disinformation".[26] What is meant by this is not precisely defined in the recitals either, but only described by references to incorrect or misleading or deceptive content as well as frequently coordinated manipulations such as the inauthentic use of a service, use of bots or fake accounts.[27]

A fairly precise definition of this term, on the other hand, can be found in the Commission's 2020 Action Plan for Democracy[28] and verbatim in the Disinformation Code 2022. Recital 106 second sentence DSA explicitly refers to these documents and thus incorporates a broad concept of disinformation that encompasses four different phenomena:[29]

- Misinformation is false or misleading content shared without harmful intent though the effects can still be harmful, e.g., when people share false information with friends and family in good faith;
- Disinformation is false or misleading content that is spread with an intention to deceive or secure economic or political gain, and which may cause public harm;
- Information influence operation refers to coordinated efforts by either domestic or foreign actors to influence a target audience using a range of deceptive means, including suppressing independent information sources in combination with disinformation; and
- Foreign interference in the information space, often carried out as part of a broader hybrid operation, can be understood as coercive and deceptive

24 Art. 2 lit. h DSA; on illegal disinformation Kastor/Püschel, Kommunikation und Recht (K&R) 2023, 20, 21 with further references.
25 Cf. art. 2 lit. t and u, art. 34 Abs. 1 sentence 3, recital 5 sentence 2, recital 68 sentence 2, recital 84 in fine, recital 95 sentence 2, recital 104 DSA.
26 Cf. recitals 2 sentence 1, 9 sentence 1, 69 sentence 2, 83 sentence 2, 84, 88 in fine, 95 sentence 2, 104, 108 sentence 2 DSA.
27 Cf. recitals 69 sentence 2, 83 sentence 2, 84, 95 sentence 2, 104 sentence 3 DSA.
28 European Commission, COM(2020) 790.
29 European Commission, COM(2020) 790, 22; preamble lit. a with notes 5-10 Disinformation Code 2022 (n 2).

efforts to disrupt the free formation and expression of individuals' political will by a foreign state actor or its agents.

The extension of the conventional concept of disinformation in the sense of deliberate and malicious deception (alternative 2) to the three other groups of cases is historically related to the COVID-19 pandemic and the Ukraine conflict. In the pandemic, it had become clear that a relevant potential for harm is inherent not only in deliberate disinformation campaigns, but also in false or otherwise misleading information spread in good faith, even if it is only shared among friends or family – such as the advice to treat a COVID infection by drinking bleach.[30] Case groups three and four, on the other hand, come from military intelligence jargon and describe behaviors by a domestic or foreign enemy (adversary) in the context of a hybrid conflict that is also conducted with information.[31] They differ from misinformation and classical disinformation in that they are intended to manipulate the behavior of a target group in a coordinated manner by various means, including by way of disseminating per se true information, e.g., through a coordinated hack-and-leak action.[32]

According to the father of the four-part disinformation concept,[33] strategic communications expert James Pamment, who has, inter alia, worked for the NATO Strategic Communications Centre of Excellence, the case groups are in a graduated, escalating relationship to each other: The most serious form of disinformation in the broad sense is interference from abroad. This can comprise a number of influence operations, which in turn can involve various forms of disinformation in the narrower sense, which then can for their part trigger or be linked to bona fide misinformation.[34] Pamment considers sanctions against disinformation advisable only in the particularly

30 Cf. the definition of misinformation in the documents referenced in note 29 ('e.g. when people share false information with friends and family in good faith'); furthermore European Commission, JOIN(2020) 8, 4; European Commission, COM(2021) 262, 5 et seq.

31 Pamment (n 3), 3 et seq.; recitals 5-10 Regulation (EU) 2022/350 amending Regulation (EU) No. 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine, OJ L 65/1; General Court of the EU, judgment of 27.7.2022 – T 125/22, RT France, ECLI:EU:T:2022:483, paras 52 et seq., 209 et seq.

32 Cf. also art. 34(2) subparagraph 2 DSA as well as Pamment (n 3), 3 et seq.; Pamment (n 11), 16 et seq.

33 Cf. European Commission, COM(2020) 790, 22 with reference to Pamment. On Pamment see also https://www.isk.lu.se/james-pamment.

34 See Pamment (n 11), 16 et seq.

serious cases of coordinated influence operations and interference from abroad.[35] According to Pamment, the four types of disinformation in the broad sense each have different characteristics:[36]

	Misinformation	**Disinformation**	**Influence Operation**	**Foreign Interference**
Actor	Any, less likely a large organization or state actor	Any	Any, but likely a large organization or state actor	State actor and/or its proxies
Behaviour	No evidence of an intent to deceive	Evidence of deliberately deceptive behaviour	Coordination of various techniques aimed at a common goal	Coordination of various techniques aimed at a common goal
Content	Often legitimate expression of an opinion	verifiably deceptive or untrue elements[37]	Any, often multiple types of measures	Any, often multiple types of measures
Degree	Limited evidence of coordination	Any	Scale of the operation indicates coordination	Any
Effect	Any	Any	Any, but should further the objective(s) of the actor	Any, but should further the objective(s) of the actor

According to the Commission and the signatories of the Disinformation Code 2022, the term "disinformation" does not include "misleading advertising, reporting errors, satire and parody, or clearly identified partisan news and commentary".[38] This very list reveals the difficulty of distinguishing harmful disinformation from legitimate expressions of opinion. How many errors does a journalistic medium have to commit before it degenerates into an unreliable source of repeated disinformation? How are "fake parody accounts" to be distinguished from "real", legitimate parodies?[39] Does a single Twitter user suggesting a #hashtag launch a coordinated influence operation? What generally is to be understood under an influence

35 Pamment (n 3), 2-5.
36 Pamment (n 3), 11.
37 The Commission and the Disinformation Code 2022, in contrast, do include false (true) but otherwise misleading content under the concept of misinformation and disinformation; see supra n 29. Likewise the concept of 'misleading' in unfair competition law pursuant to art. 5(2) German Unfair Competition Act ('false statements or other information suited to deception').
38 European Commission, COM(2018) 236, 2; preamble lit. a Disinformation Code 2022 (n 2).
39 European Commission, SWD(2020) 180, 14.

operation if the actor in question is based in the Union and not controlled by a third country?

C. The Purpose of Anti-disinformation Measures

The clarification of these delicate issues is complicated by the fact that the four-element concept of disinformation differentiates between different actors and behaviors but does not explain what is meant by a relevant "harm". The Disinformation Code 2022 only states that the signatories agree with the Commission that disinformation is a major challenge for Europe.[40] What exactly this challenge is and what interests are to be protected from disinformation remains open.

However, the DSA provides information about these purposes, thus reversing the interplay between the Code of Conduct and statutory law. While the Disinformation Code 2022 defines the subject matter of regulation, the DSA specifies the interests protected by the relevant measures.

Informative for this teleology are the terms "systemic risk" (Art. 34(1) DSA) and "crisis" (Art. 36(2) DSA). These terms constitute substantive requirements for special due diligence obligations with regard to illegal and otherwise harmful content, including disinformation, of very large online platforms (hereinafter VLOPs) and very large online search engines (hereinafter VLOSEs) with an average monthly number of at least 45 million active users in the Union.[41] The references to "systemic" risks and "public" security and health in Art. 36(2) of the DSA make it clear that the disinformation regime does not serve to protect the individual legal interests of specific individuals, but rather, on a more abstract level, to protect public goods/interests. The risk management and crisis response measures laid down in the DSA address "societal concerns" with regard to very widespread online services and their effects on the formation of public opinion.[42] The classic, narrow concept of disinformation (now case group 2 of the broad concept of disinformation) already aimed at preventing such

40 Preamble lit. b Disinformation Code 2022 (n 2).

41 Cf. recitals 83 sentence 2, 84, 88 in fine, 95 sentence 2, 104, 108 sentence 2 DSA and infra IV 2 c.

42 Cf. recital 79 DSA; definition of disinformation in the narrow sense, supra n 29.

"public" damage.[43] This general purpose was not affected by the extension to bona fide misinformation.[44]

More details on the protective purposes of disinformation regulation are provided by the enumeration of the systemic risks in Art. 34(1) third sentence DSA that VLOPs and VLOSEs must constantly assess and, if necessary, mitigate. According to this provision, VLOPs and VLOSEs must not only contain the dissemination of illegal content (lit. a), but also any actual or foreseeable negative effects on

- "the exercise of fundamental rights" (lit. b),
- "on civic discourse and electoral processes, and public security" (lit. c) and
- "in relation to gender-based violence, the protection of public health and minors and serious negative consequences to the person's physical and mental well-being" (lit. d).

Three protected interests can be derived from this list. Firstly, risk management is intended to protect the democratic opinion- and consensus-forming processes (elections). This protected interest is considered from two perspectives in Art. 34(1) third sentence lit. b and c DSA. On the one hand, in the view of the Commission and probably also of the Union legislator, disinformation represents a systemic risk to individual freedom of expression.[45] Behind this view, which is by no means self-evident, is the idea that non-governmental disinformation can also go so viral or be artificially amplified that correct statements are pushed to the margins of the debate or are no longer voiced at all because they appear to the individual to be deviant. Secondly, item (c) protects the collective processes of deliberative democracy, namely electoral processes. This regulatory purpose is based on the assumption that disinformation often pushes radical or extremist views, undermines citizens' trust in democratic institutions and contributes to the polarization of debate.[46] This risk profile can be found not only in

43 European Commission, COM(2018) 236, 2; preamble Disinformation Code 2018 (n 14).

44 Cf. European Commission, COM(2021) 262, 5 et seq.

45 European Commission, COM(2018) 236, 1; art. 34(1) sentence 3 lit. a in connection with recital 81 sentence 2 DSA ('submission of abusive notices or other methods for silencing speech'); Pamment (n 11), 6.

46 European Commission, JOIN(2018) 36, 13 et seq.; European Commission, COM(2018) 236, 1 et seq.

coordinated disinformation campaigns but also in misinformation that is shared en masse.

The second protected interest, "public security", is present both in Art. 34(1) third sentence lit. c DSA and in the legal definition of a "crisis" according to Art. 36(2) DSA. While "actual or foreseeable negative effects" on public security are sufficient for a systemic risk, a crisis requires exceptional circumstances that lead to a serious threat to security. The security risks or crises can concern both the internal security of Union citizens (Art. 3(2) TEU) and the security of the Union as such and of its citizens in their relations with the wider world (Art. 3(5) TEU).[47] The focus of the relevant Union measures has for some time been on the second-mentioned public security of the Union in relation to the Russian Federation.[48] After initially strengthening the Union's strategic communication in this regard,[49] in response to the Russian invasion of Ukraine in February 2022, the Council suspended the broadcasting licenses of several Russian television channels and prohibited the transmission or distribution of these programs by any means, and the placing of advertising on them.[50] The immediate aim of these measures is to counter disinformation attributed to the Russian Federation, which is described as part of a comprehensive hybrid threat in the form of systematic war propaganda.[51] According to the four-part concept of disinformation in the broad sense, this is therefore to be qualified as interference from abroad, which, according to Pamment, indeed justifies the most far-reaching countermeasures.[52] The General Court of the

47 On the term 'security' cf. nos. 9 et seq. Action Plan of the Council and the Commission on how best to implement the provisions of the Treaty of Amsterdam on an area of freedom, security and justice, 3.12.1998, OJ C 19 of 23.1.1999, 1.

48 Cf. General Court of the EU, judgment of 27.7.2022 – T 125/22, RT France, ECLI:EU:T:2022:483, paras 52-55; European Commission, JOIN(2018) 36, 2-4; European Commission, JOIN(2018) 16, 4.

49 Supra I with n 12.

50 Art. 2 lit. f Regulation (EU) No. 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine, as amended by Regulation (EU) 2023/250, OJ L 32I/1; Keber, Computer und Recht 2022, 660, 662.

51 Recitals 5-10 Regulation 2022/350 (n 31); General Court of the EU, judgment of 27.7.2022 – T 125/22, RT France, ECLI:EU:T:2022:483, paras 56 et seq., 88, 162, 209 et seq. (war propaganda). On the concept of propaganda, see Joint Declaration (n 13), no. 2 lit. c (state statements which demonstrate a reckless disregard for verifiable information); Baade, Europarecht 2020, 653; Schünemann, in: Dunn Cavelty/Wenger (n 6), 32, 34; Bauer/Nadler, Harvard Kennedy School (HKS) Misinformation Review 2021, https://doi.org/10.37016/mr-2020-64.

52 Cf. Pamment (n 3).

EU sees these measures as pursuing two objectives that are in conformity with primary and fundamental rights, namely the protection of the public security of the Union itself and the protection of peace in Ukraine and thus of international security.[53]

The third protected interest of the anti-disinformation rules is, according to Art. 34(1) third sentence lit. d, Art. 36(2) second alternative DSA, public health, including the well-being of particularly vulnerable sections of the population, such as minors. The separate mention of public health can be attributed to the experience with the COVID-19 pandemic, which showed that, in addition to coordinated disinformation campaigns, other manipulations (= misinformation), possibly spread in good faith, may also harbor health risks.[54]

It is questionable whether measures against disinformation can also be justified with a view to other public goods such as the environment or international peace outside the Union. In my view, the DSA and the Disinformation Code 2022 cannot be used as a basis for such interferences with communicative freedoms. According to the wording of Art. 34(1) third sentence and recital 80 DSA, VLOPs and VLOSEs are only obliged to assess and, if necessary, reduce the four risks expressly listed.[55] From a teleological point of view, the DSA thus leads to a specification of the disinformation regime, which according to the earlier concept was supposed to protect "public goods" of any kind from harm.[56] From the perspective of the rule of law, this clarification appears indispensable, because an obligation backed up by state penalties to deal with unspecific communication risks for all legal goods listed in Art. 3 TEU and referred to in the Charter of Fundamental Rights would be practically impossible for VLOP and VLOSE providers to honor and would thus be disproportionate. The concept of a "crisis" according to Art. 36 and Art. 48 DSA, which requires a serious threat to public security or public health in the Union or in significant parts of it, is even more limited. Only such extraordinary circumstances justify

53 General Court of the EU, judgment of 27.7.2022 – T 125/22, RT France, ECLI:EU:T:2022:483, para 202. The idea to protect international peace goes beyond the concept of the (information) crisis pursuant to art. 36(2) DSA, which requires a serious threat to public security 'in the Union or in significant parts of it'.

54 Cf. recital 83 DSA.

55 Cf. also recital 80 sentence 1 DSA.

56 European Commission, COM(2018) 236, 2 and Preamble Disinformation Code 2018 (n 14) ('Public harm comprises threats to democratic political and policy-making processes as well as public goods such as the protection of EU citizens' health, the environment or security.').

the far-reaching powers of the Commission in a "crisis". Communicative threats to democracy or the environment are not sufficient.

The limited protective purpose of the DSA does not preclude anti-disinformation measures from being founded on other legal bases though, namely the law on common foreign and security policy.[57] Disinformation about the dangers of climate change could furthermore be qualified as a security risk and thus indirectly become subject to DSA and Disinformation Code obligations. However, such broad interpretations run the risk of undermining the horizontally comprehensive and at the same time teleologically limited approach of the DSA. Disinformation regulation is generally delicate. Extending it beyond the already far-reaching wording of the DSA is therefore, in the event of doubt, neither necessary nor justified.

D. Content and Enforcement of Measures Against Disinformation

The previous two sections have shown that the current regulation of disinformation in the EU results from an interplay between private self-regulation and formal statutory law. The Disinformation Code 2022 provides the definition of the subject matter of regulation, while the DSA states the regulatory objectives. Private norms and statutory due diligence obligations also intertwine with regard to the content and enforcement of anti-disinformation measures.

I. Risk-based Approach, Proportionality and Precautionary Principle

The hybrid disinformation regime follows a risk-based approach committed to the principle of proportionality. Accordingly, duties to reduce disinformation must be appropriate, necessary and not unduly burdensome in order to effectively reduce the potential harm of a statement or campaign in view of the severity of the potential impact and the probability of its occurrence.[58] Risk assessment and mitigation duties must, in other words,

57 General Court of the EU, judgment of 27.7.2022 – T 125/22, RT France, ECLI:EU:T:2022:483, paras 52 et seq.

58 Cf. art. 5(4) TEU in connection with art. 34(1) sentence 3 and recital 79 sentence 5 DSA; on the risk-based approach cf. eg Art. 3 no. 18 Regulation (EU) 2019/1020 on market surveillance and compliance of products, OJ L 169/1; art. 2 no. 6 Directive

be proportionate in view of the nature of the danger and the probability of its realization.[59] On the one hand, online services are not required to reduce the risk of disinformation to zero.[60] On the other hand, the (self-)obligations to take measures against disinformation take effect at a very early stage in order to prevent public harm from the outset:

The preventive nature of disinformation regulation already follows from the concept of disinformation, which extends to all content that *can* be harmful.[61] Thus, it is generally sufficient that there is an informational potential for harm, the realization of which does not have to be demonstrated and proven. A systemic risk for a relevant public good pursuant to Art. 34(1) DSA is accordingly present if certain content is likely or "foreseeable" to have adverse effects. Moreover, according to the fiction of Art. 36(2) DSA, an informational "crisis" is already considered to have arisen when extraordinary circumstances such as "armed conflicts or acts of terrorism, including emerging conflicts or acts of terrorism, natural disasters such as earthquakes and hurricanes, as well as from pandemics and other serious cross-border threats to public health" occur.[62] In contrast to the concept of risk, the concept of crisis is therefore not linked to the dissemination of disinformation, which has the potential to cause harm (disinformation → harm), but even earlier to events that are so exceptional that they trigger a public debate in which disinformation can occur, which in turn threatens public safety or health (circumstance → disinformation → harm). Art. 36(2) DSA logically does not presuppose a threat to public security or health, but a situation (= extraordinary circumstances) that can lead to a serious threat.[63] If the concept of crisis is interpreted broadly, the Commission could make use of its powers under Art. 36 even if it cannot be determined with certainty whether there is a disinformation risk at all and

(EU) 2022/2557 on the resilience of critical entities, OJ L 333/164; European Commission, COM(2021) 206, 3 et seq.

59 Cf. also Pamment (n 3), 5 et seq. (ABCDE framework covering disinformation actors, their behaviour, the content of the information, the degree of harm and the effects of disinformation).

60 Cf. art. 19(2) Regulation (EU) 2019/1020 (n 58); on over-blocking through filter systems in copyright law see the opinion of AG Saugmandsgaard Øe of 15.7.2021 – C 401/19, Poland / Parliament and Council, ECLI:EU:C:2021:613, para 184.

61 Supra II.

62 Cf. recital 91 sentence 3 DSA, see also Art. 48(1) sentence 2 DSA.

63 Although 'can' is missing in the English and French versions of art. 36(2) DSA, it is found in all the language versions of the explanatory recital 91 sentence 2 ('can lead to a serious threat', 'peuvent entraîner une menace grave').

how serious it is.[64] According to this interpretation, the DSA would extend the precautionary principle known from environmental and health law to the regulation of the public debate.

This is achieved, as already mentioned, through the new substantive legal terms of "disinformation", "systemic risk" and "crisis", which trigger special duties of care on the part of VLOPs and VLOSEs as well as powers of intervention on the part of the Commission. The DSA thus by no means establishes a purely procedural compliance regime that merely serves to effectively combat content that has otherwise been declared illegal. On the contrary, the DSA establishes new substantive requirements and sanctions precisely in the particularly sensitive area of non-illegal but otherwise harmful content. These measures are only limited to the extent that they are not directly aimed at the individual speaker, but rather at Big Tech companies, which have to incorporate the prohibitions of disinformation into their private regulations and enforce them against their users.

II. The Three Levels of Disinformation Regulation

In line with this approach, the regulation of disinformation is always based on private norms, namely the platform terms and conditions and other internal service rules, such as the rules governing the ranking of search results. This micro level of regulation is subject to collective self-commitments (meso level) for signatories of the Disinformation Code, and to the legal due diligence obligations of the DSA on a societal macro level for VLOPs and VLOSEs.

1. Micro Level: Private Rules of Online Services

Information society services are in principle free to prohibit all forms of disinformation in their terms and conditions and to enforce this contractual prohibition through automated content moderation measures, if neces-

64 Cf. on the precautionary principle see CJEU, judgment of 5 May 1998 – C-157/96, The Queen / Ministry of Agriculture, Fisheries and Food and Commissioners of Customs & Excise, ex parte National Farmers' Union and others, ECLI:EU:C:1998:191, para 63; CJEU, judgment of 1 October 2019 – C-616/17, Blaise and others, ECLI:EU:C:2019:800, para 43.

sary.[65] The large US Big Tech companies have been doing this for years, sometimes at short notice under informal pressure from politicians and the public, but especially in the COVID-19 pandemic even acting before the event.[66] As correctly observed by the German Federal Court of Justice, the willingness to fight all kinds of "harmful" expression follows from the fact that Facebook and the like have a vital business interest in "creating an attractive communication and advertising environment for both their users and their advertisers".[67] This interest is incompatible not only with hate speech, but also with false or otherwise misleading information that undermines users' trust in the reliability and security of the content provided via the service and thus ultimately trust in the service as such.[68]

However, the freedom of online services to establish and enforce contractual prohibitions on disinformation is not unlimited. According to the German Federal Constitutional Court and the Federal Court of Justice, very large services such as Facebook are under the spell of an indirect third-party effect of both the fundamental rights of freedom and the principle of equality.[69] They may therefore not arbitrarily delete or otherwise downgrade content without an objective, comprehensible reason, for example to suppress a particular political opinion.[70] Art. 14(4) DSA further obliges all providers of intermediary services, regardless of their size, to proceed "in a diligent, objective and proportionate manner" when applying and

65 Cf. the definitions in Art. 2 lit. a, t and u DSA and German Federal Constitutional Court, order of 11 April 2018 – 1 BvR 3080/09, Stadionverbot, ECLI:DE:BVerfG:2018:rs20180411.1bvr308009, para 40 (English translation available at http://www.bverfg.de/e/rs20180411_1bvr308009en.html); German Federal Court of Justice, judgment of 29 July 2021 – III ZR 179/20, Hassrede-AGB, ECLI:DE:BGH:2021:290721UIIIZR179.20.0, para 78; Pamment, The EU's Role in Fighting Disinformation: Developing Policy Interventions for the 2020s, 9 et seq.

66 Cf. Peukert, in: Spiecker gen. Döhmann/Westland/Campos (n 13), 229, 240 et seq. with further references; High level group (n 2), 15 et seq.; European Commission, JOIN(2020) 8, 9.

67 On the regulation of private hate speech see German Federal Court of Justice, judgment of 29 July 2021 – III ZR 179/20, Hassrede-AGB, ECLI:DE:BGH:2021:290721UIIIZR179.20.0, para 92.

68 Schmid/Braam/Mischke, MultiMedia und Recht 2020, 19, 23 with further references.

69 German Federal Constitutional Court, order of 20.9.2021 – 1 BvQ 100/21, Der III. Weg, ECLI:DE:BVerfG:2021:qk20210920.1bvq010021, para 15; German Federal Court of Justice, judgment of 29 July 2021 – III ZR 179/20, Hassrede-AGB, ECLI:DE:BGH:2021:290721UIIIZR179.20.0, para 64.

70 German Federal Court of Justice, judgment of 29 July 2021 – III ZR 179/20, Hassrede-AGB, ECLI:DE:BGH:2021:290721UIIIZR179.20.0, paras 80-82.

enforcing contractual moderation rules, and to take into account "the rights and legitimate interests of all parties involved, including the fundamental rights of the recipients of the service", including freedom of expression. Consequently, they too must not moderate user content arbitrarily or on the basis of purely hypothetical assumptions about the potential for harm.[71] Online platforms must even reverse unfounded measures according to Art. 20(4) DSA without undue delay.

2. Meso Level: Self-commitments per Disinformation Code

The micro level of the fight against disinformation is thus characterized by private autonomous decisions of the service providers. Those who have not been designated by the European Commission as a VLOP or VLOSE can but are not obliged to take action against disinformation.[72]

The meso level of disinformation regulation in the EU is the Disinformation Code 2022. Although the Code is aimed at VLOPs and VLOSEs through its link to Art. 34 et seq. DSA, smaller service providers are free to submit to the Code's voluntary obligations, and some indeed do.[73] On 40 tightly printed pages, the Code sets out no less than 44 commitments to 128 concrete measures, the structure, and objectives of which can only be outlined in this article.

A crucial aspect for understanding the functioning of the Code is the insight that it is by no means only directed at online platforms and search engines, but at all "relevant" actors who can influence the dissemination of disinformation.[74] These include, firstly, organizations that assess whether content qualifies as disinformation and whether websites repeatedly make disinformation accessible. This category comprises fact checkers, actors who assess the trustworthiness of news sites (e.g., the US company "NewsGuard" and the British "Global Disinformation Index") as well as

71 Fundamental rights thereby require a showing of causality between disinformation and public harm based on objective facts; cf. German Federal Court of Justice, judgment of 29 July 2021 – III ZR 179/20, Hassrede-AGB, ECLI:DE:BGH:2021:290721UIIIZR179.20.0, para 82.

72 Cf. art. 16, 19 DSA.

73 Cf. preamble lit. a, k and l Disinformation Code 2022 (n 2) and e.g. https://disinfocode.eu/signatory-report/vimeo-inc/?chapter=integrity.

74 Cf. commitment 41 Disinformation Code 2022 (n 2) and European Commission, COM(2021) 262, 7 et seq.; art. 45(2) DSA ('civil society organisations and other relevant stakeholders').

academics. The Code obliges the platforms and search engines to cooperate with this diverse disinformation monitoring community, to fund the corresponding services or research activities and to integrate their findings into their own services.[75]

Secondly, the Code has been signed by organizations that can be classified as belonging to the military-intelligence cybersecurity sector and have expertise in countering coordinated disinformation campaigns from within and outside a country.[76] The online platforms and search engines bound by the Code have undertaken to design their services in cooperation with these intelligence actors in such a way that as far as possible all forms of disinformation in the broad sense are not disseminated and in any event are not recommended or otherwise amplified.[77]

Thirdly, numerous advertising companies and advertising industry associations have joined the Code. Their participation aims to reduce the financial incentives for the dissemination of often scandalous disinformation that promises high engagement.[78] For this purpose, the automated online advertising systems are fed with the ratings of fact checkers and other content monitoring actors. Sources flagged as distributing disinformation are to be cut off from the advertising market.

The ongoing cooperation and decision-making in this disparate, not a-priori limited circle of "relevant actors" is institutionalized in a permanent task force. This task force is chaired by the European Commission, although it is not formally involved in the Code.[79]

3. Macro level: DSA Obligations for VLOPs and VLOSEs

However far-reaching and sophisticated the voluntary obligations of the Disinformation Code may be, its weak point is and remains the enforcement of its measures. Failure to participate in the Code, failure to comply with voluntary commitments and withdrawal from the Code without giv-

75 Commitments 26-33 Disinformation Code 2022 (n 2).
76 E.g. https://www.crispthinking.com/, https://www.globsec.org/.
77 Commitments 14-16 ('integrity of services') and 17-25 ('empowering users') Disinformation Code 2022 (n 2).
78 Commitments 1-3 Disinformation Code 2022 (n 2); European Commission, COM(2021)262, 9.
79 Commitment 37 Disinformation Code 2022 (n 2) (decisions are reached by consensus).

ing reasons does not trigger any legal consequences.[80] This enforcement deficit is remedied at the societal macro-level by the DSA.

First, the DSA establishes a legal framework for the elaboration and further development of codes of conduct. According to Art. 45(1) of the DSA, the Commission and the European Board for Digital Services, which comprises the Member State Digital Services Coordinators, shall encourage and facilitate the drawing up of voluntary codes of conduct at Union level to contribute to the proper application of the DSA, taking into account in particular the specific challenges of tackling different types of illegal content and systemic risks. According to paragraph 4 of this Article, "the Commission and the Board shall assess whether the codes of conduct meet the aims ... and shall regularly monitor and evaluate the achievement of their objectives ... In the case of systematic failure to comply with the codes of conduct, the Commission and the Board may invite the signatories to the codes of conduct to take the necessary action". According to its wording and its position in the section on "Other provisions concerning due diligence obligations", this power also applies to small and medium-sized intermediary services. However, it only empowers the Commission and the Board to "invite" the Code signatories to comply with their voluntary commitments, and the provision does not stipulate a mandatory obligation to comply with the Disinformation Code. Accordingly, the recitals state that the provisions on the conclusion of codes of conduct should not impair "the voluntary nature of such codes and the freedom of interested parties to decide whether to participate".[81] Finally, this restrictive interpretation is supported by the fact that a more far-reaching proposal of the European Parliament to empower the Commission and the Board, "in case of systematic failure to comply with the codes of conduct", to "decide as a last resort to temporarily suspend or definitively exclude platforms that do not meet their commitments as signatories to the codes of conduct", has not become law.[82]

The legal situation is different for VLOPs and VLOSEs. Due to their size and social importance – one could also speak of systemic relevance – they are generally subject to the most intensive due diligence obligations under the graduated system of the DSA. This also includes the obligation to

80 Regarding the Disinformation Code 2018 see European Commission, SWD(2020) 180, 18; preamble lit. u and v Disinformation Code 2022 (n 2).

81 Recital 103 sentence 4 DSA.

82 See European Parliament, 9_TA(2022)0014, amendment no. 371 to art. 35(5).

"put in place reasonable, proportionate and effective mitigation measures" against systemic risks, including disinformation, as stipulated in Art. 35(1) sentence 1 DSA. Compliance with this due diligence obligation can be enforced in two ways.

On the one hand, the Commission can oblige VLOP or VLOSE providers to initiate or adjust cooperation with other providers through codes of conduct or "voluntary" crisis protocols (Art. 48 DSA). If a service provider refuses to enter into this commitment "without proper explanations", this can, according to the recitals, be taken into account when determining whether such a recalcitrant provider violates its DSA obligations.[83] On the other hand, the Commission can directly order a VLOP or VLOSE provider to adopt the risk mitigation measures listed in Art. 35(1) second sentence DSA. This could include an order to cooperate with trusted flaggers and/or to adapt the terms and conditions, content moderation processes, advertising systems and features or functioning of their services.[84] As a result, the DSA empowers the Commission to force uncooperative VLOPs and VLOSEs to take measures that the signatories of the Disinformation Code take voluntarily.

The same is true in a "crisis", which, as explained, is even further upstream. Art. 36(1) and (7) DSA grant the Commission, upon recommendation of the Board, the power to "require" VLOP and VLOSE providers to take temporary special measures, including highlighting reliable information. The Board may also recommend that the Commission initiate the drawing up of voluntary crisis protocols for addressing crisis situations. Moreover, as soon as an "exceptional circumstance" in the sense of Art. 36(2) DSA has occurred, systemic disinformation risks can usually be identified, the management of which can be enforced via Art. 34 et seq. DSA. Finally, experience teaches that Big Tech will not refuse to follow certain communication protocols in future crisis situations.[85]

83 Cf. recital 104 sentence 6 and arts. 66(1), 73(1) lit. a, 74(1) lit. a, 75(2) sentence 3 and (3) sentence 3 DSA (commitment to adhere to relevant codes of conduct).

84 The powers of the exclusively competent (cf. art. 56(2) DSA) commission result from arts. 70(1) (interim measures 'where there is an urgency due to the risk of serious damage for the recipients of the service … on the basis of a prima facie finding of an infringement'), 73(3) (non-compliance decision), 75(4) in connection with 76(1) lit. e (penalty payments) and 82(1), 51(3) sentence 1 lit. b (temporary restriction of access of recipients to the service).

85 Pamment (n 65), 13 ('This collaboration already exists to a certain degree but could be developed particularly for crises like the coronavirus pandemic.').

E. Unresolved Issues

In the light of all the above, disinformation regulation in the EU is based on a complex web of private and public communication norms involving numerous actors. The subject matter of regulation – "disinformation" – is defined by the Disinformation Code 2022, the regulatory purposes are specified by the DSA, and the concrete measures against disinformation are to be found in the private platform rules (micro-level), the voluntary commitments of the Disinformation Code (meso-level) and, for the societal macro-level of VLOPs and VLOSEs, in the risk management rules of the DSA, which at the same time links all three regulatory levels together. The practical implementation and further development of the Code and DSA requirements also take place in a coordinated-cooperative manner, namely on the private side in the permanent working group of the signatories of the Disinformation Code (see above) and on the state side in the "European Board for Digital Services" (Arts. 61-63 DSA). The connection between these two central institutions of the fight against disinformation is established via the Commission, which chairs all the meetings.[86]

The reason for this complex structure is the fact that a conventional state order to suppress content that is "harmful", yet covered by freedom of expression and also otherwise legal, has so far been correctly considered unconstitutional for lack of a legal basis.[87] Whether the EU legislature has succeeded in finding a sustainable solution in terms of the rule of law appears extremely doubtful and requires detailed analysis. Questions in need of clarification include:

(1) What is the factual significance and effect of objectively false (untrue) and otherwise misleading content at the societal level? In this respect, the state of empirical research is much less clear-cut than the constantly repeated, consistently anecdotal references to "Trump", the "Infodemic" or "Russia" would have one believe.[88] On several occasions, subsequent investigations could not confirm suspected disinformation

86 Commitment 37 Disinformation Code 2022 (n 2); art. 62(2) DSA.

87 Cornils, Designing platform governance, 2020, 32; Ferreau, Archiv für Presserecht 2021, 204, 209. For a critical view of the crisis protocols see German Bundesrat, Bundesrats-Drucksache 96/21, 21.

88 Pamment (n 11), 3 ('evidence of harm caused by disinformation and influence operations is patchy'); Schünemann, in: Cavelty/Wenger (n 6), 32, 40 et seq. with further references.

campaigns.[89] Against this backdrop, there are increasing voices in communication studies research that see an empirically unsubstantiated alarmism at work in the fight against disinformation.[90]

(2) Does the TFEU, and in particular the internal market competence referenced in Art. 1(1) DSA, authorize the EU to regulate legal but otherwise harmful speech of a non-specific nature in the interests of democracy, public safety and health?[91]

(3) Are platform-based measures against disinformation attributable to the EU if the service providers thereby wish to comply with their DSA obligations?[92]

(4) Is the protection of "civic discourse" in a deliberative democracy a constitutionally permissible goal of repressive measures against per se legal expression?[93] Does freedom of expression imply a state duty to

89 European Commission, COM(2020) 790, 4 with n 8 ('isolated cyberattacks, data protection and other elections-related complaints had been received, but that a covert, coordinated large-scale effort to interfere in the elections had not been identified'); https://digital-strategy.ec.europa.eu/en/policies/covid-19-disinformation-monitoring (no coordinated disinformation campaigns related to Covid-19); Beyer/Almeida Saab, Verfassungsblog, DOI: 10.17176/20221223-121639-0 (no decisive influence of Russian disinformation campaigns on the elections in Italy); Benkler/Faris/Roberts, Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics, 2018, 235 et seq. (no decisive Russian influence on Trump's election); without examples Kommunikationsbericht der Bundesregierung 2021, Bundestags-Drucksache 19/31165, 2 et seq.; critically also Baade, Europarecht – EuR 2020, 653, 683.

90 See Schünemann, in: Cavelty/Wenger (n 6), 32, 43; Anderson, Communication Theory 31(1) (2021), 42 et seq.; Jungherr/Schroeder, Social Media and Society 7(1) (2021), https://doi.org/10.1177/2056305121988928 (Disinformation not a driver of social or political divisions); Altay/Berriche/Acerbi, Social Media and Society 9(1) (2023), https://doi.org/10.1177/20563051221150412 ('misinformation on misinformation'). Critically on the conceptual and theoretical vagueness of the sociological fake news literature e.g. Tandoc/Lim/Ling, Digital Journalism 6(2) (2018), 137 et seq.; Zimmermann/Kohring, M&K Medien & Kommunikationswissenschaft 66 (2018), 526 et seq.; Camargo/Simon, Harvard Kennedy School (HKS) Misinformation Review 2022, https://doi.org/10.37016/mr-2020-106.

91 Upheld for anti-war propaganda by the General Court of the EU, judgment of 27.7.2022 – T 125/22, RT France, ECLI:EU:T:2022:483, paras 52 et seq.

92 Upheld for the copyright liability of platforms by the CJEU, Judgment of 26 April 2022 – C-401/19, Poland / Parliament and Council, ECLI:EU:C:2022:297, para 56 (overblocking is the 'direct' consequence of a copyright liability norm); generally Eifert, in: Voßkuhle/Eifert/Möllers (eds.), Grundlagen des Verwaltungsrechts, vol. 1, 3rd ed. 2022, § 19 para 163 (question of attributability with complex control mechanisms is highly disputed).

93 German Bundesrat, Bundesrats-Drucksache 96/21, 3.

protect citizens from disinformation?[94] What image of man is this assumption based on?[95] Do statements that are spread in good faith and are true per se, which, as explained, may well fall under the concept of disinformation in the broad sense, also trigger a corresponding duty to protect?

(5) Is it proportionate to preventively suppress legal but otherwise potentially harmful content using a risk-based approach or should the self-regulatory forces of open debate be trusted, especially in unclear crisis situations?[96] How much communicative deviance does the current disinformation regime still allow?[97]

(6) Does the repeatedly mediated disinformation regulation, with its coercive instruments directly aimed only at a small number of VLOPs and VLOSEs, undermine legal recourse of the alleged disseminators of disinformation, including possibly professional journalists and entire media companies, in a way that is inadmissible under the rule of law? Against this background, can it be assumed that Art. 20(4) second sentence DSA establishes a subjective right to the restoration of content that is neither illegal nor in breach of contract, which can be enforced before the civil courts of the Member States?

94 Cf. also General Court of the EU, judgment of 27.7.2022 – T 125/22, RT France, ECLI:EU:T:2022:483, para 197 (obligation to display a banner or a warning insufficient).

95 On the concept of the 'informational citizen' Anderson, Harvard Kennedy School (HKS) Misinformation Review 2021, https://doi.org/10.37016/mr-2020-64.

96 Generally Grimm, Die Zukunft der Verfassung, 1991, 216 (preventive measures require sufficient suspicion of serious threats to a high-ranking legal interest); critically Cornils, Zeitschrift für Urheber- und Medienrecht 2019, 89, 103; Ingold, MultiMedia und Recht 2020, 82, 85; Joint Declaration (n 13), no. 3 lit. a; undecided Holznagel, Computer und Recht 2021, 733 para. 19 (weakness or strength). See also CJEU, judgment of 10 June 2021 – C-65/20, KRONE – Verlag, ECLI:EU:C:2021:471, para 40 (strict liability for inaccurate health advice 'would be detrimental to the objective of ensuring that risk is fairly apportioned between the injured person and the producer'). There is, as a matter of principle, contrary to the Commission (JOIN(2018) 36, 9), no 'manipulation-free' discourse, not even, and particularly not, if disinformation is regulated.

97 Regarding the broadcasting and distribution ban on Russian TV channels cf. General Court of the EU, judgment of 27.7.2022 – T 125/22, RT France, ECLI:EU:T:2022:483, paras 97, 187 (the applicant's media coverage of the aggression did not maintain 'a balance in so far as concerns the choice of participants, content, images and views communicated in those sequences').

(7) Should the sensitive area of legal but otherwise harmful content not be regulated at a greater distance from the state or with greater involvement of the European Parliament?[98]

Given the shaky empirical and normative foundation of the regulation of disinformation at EU level, it is irritating that in its relevant papers the Commission itself reports violations of media freedom under the pretext of combating disinformation, even in Member States.[99] With all the trust that the Commission can claim for itself, it seems downright naïve to consider such abuse at EU level impossible in principle, especially since the daily fight against disinformation is controlled and executed by private organizations, often not based in the EU.[100] Accordingly, the open-ended scholarly accompaniment of the further development of the EU disinformation regulation is all the more important. The observers of the social debate need critical observation.

98 On the creation of so-called platform boards cf. Koalitionsvertrag zwischen SPD, Bündnis 90/Die Grünen und FDP 2021, 17.

99 European Commission, JOIN(2020) 8, 12 et seq.; European Commission, COM(2020) 790, 14; Pamment (n 11), 4 ('Experts also express increasing concerns that EU member states themselves are becoming a source of misinformation and disinformation.').

100 In addition to the US and Chinese Big Tech companies, this also includes evaluation and rating organizations based in the USA (e.g. https://www.newsguardtech.com) or the United Kingdom (e.g. https://www.disinformationindex.org). Both of these organizations have received payments from the US federal government budget, NewsGuard even directly from the US Department of Defense; cf. Shellenberger, The Censorship-Industrial Complex, 2023, 51 et seq.

Consumer Protection and Digitalization: Challenges to Overcome New Consumer Vulnerabilities in the Digital Age

Claudia Lima Marques

Abstract: This paper analyses how consumer laws are facing the challenges proposed by digitalization. The first part will focus on the exam of the new sources of consumer vulnerabilities on the digital scenario and the second part will analyse the new instruments developed by the praxis to overcome those vulnerabilities, and rethinking consumer protection in the digital economy. The second part analyses the legislative and regulatory challenges of the data and platform economy to protect consumers, calling for the revival of its constitutional bases and the need for a source dialogue between consumer law and data protection. To participate in this discussion about digital constitutionalism, the main hypothesis is that consumers are made more vulnerable by the very structure and architecture of choice of digital markets. The objective of this paper is to reflect how to overcome these new consumer vulnerabilities with new compensatory legal consumer law and data protection instruments. And call the attention to ILA´s Consumer Global Compact in the Digital Economy.

A. Introduction

It is a pleasure to participate in this discussion about digital constitutionalism and the existence of fundamental rights for the internet users.[1] I will focus on the consumer protection on the digital scenario. Today, markets are becoming more globalized, and the consumption is highly digitalized

1 Short version of the paper present at the Frankfurt University in March 2023. We thank Prof. Dr. Indra Spiecker (Frankfurt) and Prof. Dr. Laura Schertel Mendes (UnB and Frankfurt) for the kind invitation and Lorenzo Nicoletti, LL.M UFRGS-CDEA for the Englisch correction of the first version.

and at distance.[2] But in this digital environment traditional consumer rights mechanisms no longer seem as effective as in the analogical world. At the 2015 Revision of the UN Guidelines on Consumer Protection (UNGCP)[3] a new chapter on E-commerce (GL 63 to 65) was introduced, aiming to accommodate existing consumer policies to the 'special features of electronic commerce' to enhance 'consumer confidence' in the new digital marketplaces, also the collaboration between States in this matter. Specially, at the 2015 Revision of the UNGCP a new right to 'equal protection online and offline' was created for digital consumers. The UNGCP, Guideline 5, 'j' expresses this new 'principle of equal protection' as follow: "*A level of protection for consumers using electronic commerce that is not less than that afforded in other forms of commerce*"), but its efficacy remains a great challenge.

To achieve this equal level of protection we need to be aware of the special forms of consumer vulnerabilities at the digital and data-driven transactions. In my opinion the protection of digital consumers depends more and more on the respect of their fundamental rights in digital consumption. The 2015 Revision of the UNGCP also mention the need to protect consumer privacy[4] and in this point consumer law meet the new digital constitutionalism.[5]

Digital Constitutionalism give light of the use of constitutional tools by big tech compagnies,[6] but also for the need of an effective bill of rights

2 MICKLITZ, Hans-W.; SAUMIER, Geneviève. *Enforcement and effectiveness of consumer Law*. Springer: Cham, 2018. p.3.

3 The UNGCP were first adopted by the General Assembly in Resolution 39/248 of 16 April 1985, expanded in 1999 and now revised by the General Assembly in Resolution 70186 of 22 December 2015. Available in: General Assembly Resolution 70/186 on Consumer protection, Adopted on 22 December 2015 (unctad.org).

4 So UNGCP GL 5, 'k' ("The protection of consumer privacy and the global free flow of information") and GL 11, 'e' ("Protection of privacy. Businesses should protect consumers' privacy through a combination of appropriate control, security, transparency and consent mechanisms relating to the collection and use of their personal data".

5 So MENDES, Gilmar Ferreira; FERNANDES, Victor Oliveira. Eficácia dos direitos fundamentais nas relações privadas da internet: o dilema da moderação de conteúdo em redes sociais na perspectiva comparada Brasil-Alemanha. *Revista de Direito Civil Contemporâneo,* vol. 31. ano 9. p. 33-68. São Paulo: Ed. RT, apr./jun. 2022.

6 CELESTE, Edoardo. Digital Constitutionalism: Mapping the Constitutional Response to Digital Technology's Challenges (July 25, 2018). *HIIG Discussion Paper Series* No. 2018-02, Available at: Digital Constitutionalism: Mapping the Constitutional Response to Digital Technology's Challenges by Edoardo Celeste :: SSRN.

on the internet.[7] Mendes and Fernandes call for a methodological chance to achieve efficient protection of human rights at the internet.[8] Indeed, new global governance tools should be looked for,[9] because the todays new forms of digital consumption, its scale and the constant use of platforms by consumers presents methodological and practical challenges for consumer protection, consumer enforcement and consumer law.

As starting point I want to use the theory of a digital vulnerability ('architectural, relational, and data driven vulnerability') of Helberger, Sax, Strycharz and Hans Micklitz.[10] The authors argue that the old concept of a 'well-informed, observant' or reasonably rational consumer has no use to face the new online targeted marketing and dark patterns strategies of the digital markets. The vulnerability concept is used to identify individuals, users, or group of persons, that require particular policy and legal attention "because of their lack of bargaining power, structural inequalities, and other market or social conditions that make them more susceptible to harm (e.g. in the form of discrimination or unequal treatment)."[11] Consumers are the weaker party vis-a-vis providers and traders.

My work hypothesis is that consumers are made more vulnerable by the very structure and architecture of choice of digital markets.[12] The objective

7 CELESTE, Edoardo. Internet Bill of Rights: Generalization and Re-Specification Towards a Digital Constitution, in *Indiana Journal of Global Legal Studies*, vol. 30#2 (summer 2023), p. 25-54.

8 MENDES, Gilmar Ferreira; FERNANDES, Victor Oliveira. Eficácia dos direitos fundamentais nas relações privadas da internet: o dilema da moderação de conteúdo em redes sociais na perspectiva comparada Brasil-Alemanha. *Revista de Direito Civil Contemporâneo*. vol. 31. ano 9. p. 33-68. São Paulo: Ed. RT, apr./jun. 2022, specially part III about the horizontal effects of fundamental rights in private internet.

9 MARQUES, Claudia Lima; BAQUERO, Pablo M. Global Governance Strategies for Transnational Consumer Protection: New Perspectives to Empower Societal Actors, in *Revista de Direito do Consumidor*, vol. 143/2022, p. 167-188, sep./oct. 2022, p. 168ff.

10 HELBERGER, N.; SAX, M.; STRYCHARZ, J.; MICKLITZ, · H.-W. Choice Architectures in the Digital Economy: Towards a New Understanding of Digital Vulnerability, in *Journal of Consumer Policy* (2022) 45:175–200, p. 175ff, accessible at: Choice Architectures in the Digital Economy: Towards a New Understanding of Digital Vulnerability (springer.com).

11 HELBERGER, N.; SAX, M.; STRYCHARZ, J.; MICKLITZ, · H.-W. Choice Architectures in the Digital Economy: Towards a New Understanding of Digital Vulnerability, in *Journal of Consumer Policy* (2022) 45:175–200, p. 175.

12 RIEFA, Christine. Transforming consumer law enforcement with technology: from-reactive to proactive? In *Journal of European Consumer and Market Law, EuCML* 3/2023, volume 12, p. 97.

of this paper is to reflect how to overcome these new consumer vulnerabilities.

B. The new consumer vulnerabilities on the Digital Economy: architectural, relational and data-driven vulnerability

Vulnerability (from Latin *vulnus*) is the status (e.g. because y their age, physical or mental disability) or situation (e.g. consumers) where a person can be harm.[13] A key element and particularity of Brazilian Law is the legal recognition that all consumers are vulnerable.[14] Under Brazilian Consumer Defense Code – CDC (Law n. 8.078/1990), the recognition of a general 'consumer vulnerability' is a principle of the National Policy for Consumer Relations (Article 4, I). Brazilian scholars[15] and also Helberger and Micklitz argue that in digital marketplaces "all consumers are potentially vulnerable."[16] In Europe, the very architecture of the internet and the choices given to the consumers are being considered sources of structural asymmetries and new vulnerabilities.[17]

13 MARQUES, Claudia Lima; MIRAGEM, Bruno. *O novo direito privado e a proteção dos vulneráveis*. 2. ed. rev., atual. e amp. São Paulo: Revista dos Tribunais, 2014, p. 102.

14 See MARQUES, Claudia Lima. Algumas observações sobre a pessoa no mercado e a proteção dos vulneráveis no Direito Privado *In*: GRUNDMAN, Stefan, MENDES, Gilmar, MARQUES, Claudia Lima, BALDUS, Christian e MALHEIROS, Manuel. *Direito Privado, Constituição e Fronteiras*. Encontros da Associação Luso-Alemã de Juristas no Brasil. 2. Ed. São Paulo: RT, 2014. p. 287ss.

15 See for all the book, CANTO, Rodrigo Eidelwein do. *A vulnerabilidade dos consumidores no comércio eletrônico e a reconstrução da confiança na atualização do Código de Defesa do Consumidor*. São Paulo: Revista dos Tribunais, 2015.

16 HELBERGER, N.; SAX, M.; STRYCHARZ, J.; MICKLITZ, · H.-W. Choice Architectures in the Digital Economy: Towards a New Understanding of Digital Vulnerability, in *Journal of Consumer Policy* (2022) 45:175–200, p. 177.

17 See BEUC. *EU consumer protection 2.0: structural asymmetries in digital consumer markets*. Bruxelas, 2021. Available at: https://www.beuc.eu/publications/eu-consumer-protection-20-structural-asymmetries-digital-consumer-markets-0. Accessed on August 20, 2021.

I. Choice architecture on online consumption and Dark Patterns: impacts on consumer vulnerability

Helberger and Micklitz argue, that in the digital and platform economy, consumer vulnerability is not a 'simply weakness', an individual 'lack of ability' or a 'vantage point' for providers, but describes, "a universal state of defencelessness and susceptibility to (the exploitation of) power imbalances that are the result of the increasing automation of commerce, datafied consumer-seller relations, and the very architecture of digital marketplaces."[18]

Indeed, in the data driven economy, the increasingly use of AI, of algorithmic profiling, of automated decision-making, of data driven commercial strategies, of predictive analytics, and of new digital marketing strategies that intensify and personalize the relationship between trader and consumer, can have a result 'new forms of unfair commercial practices'[19] and 'new power imbalances'[20] against consumers.

About Dark Patterns, I have stated, there is not a unanimous definition on *dark commercial patterns.* The OECD roundtable on dark commercial patters online was based of the definition given by Mathur et al.[21] as "user interfaces used by some online businesses to lead consumers into making decisions they would not have otherwise made if fully informed and capable of selecting alternatives."[22] Also known as *deceptive design practices*, this practice is also described as "tricks used in websites and apps that make you do things that you didn't mean to, like buying or signing up

18 HELBERGER, N.; SAX, M.; STRYCHARZ, J.; MICKLITZ, · H.-W. Choice Architectures in the Digital Economy: Towards a New Understanding of Digital Vulnerability, in *Journal of Consumer Policy* (2022) 45:175–200, p. 186ff.

19 MARQUES, Claudia Lima; MENDES, Laura Schertel; BERGSTEIN, Laís. Dark Patterns e padrões comerciais escusos, in *Revista de Direito do Consumidor,* vol. 145/2023, p. 295-316, jan./feb. 2023.

20 HELBERGER, N; MICKLITZ, H-W. et al. Choice Architectures in the Digital Economy: Towards a New Understanding of Digital Vulnerability, in Journal of Consumer Policy, vol. 45, p. 175-200, 2021, p. 175-176.

21 MATHUR, A., J. Mayer; KSHIRSAGAR, M. (2021), "What Makes a Dark Pattern... Dark? Design Attributes, Normative Considerations, and Measurement Methods". Available at: <https://dl.acm.org/doi/10.1145/3411764.3445610>. (http://dx.doi.org/10.1145/3411764.3445610.).

22 OECD. Roundtable on Dark Commercial Patterns Online. Summary of discussion. Available at: <https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/CP(2020)23/FINAL&docLanguage=En>. Accessed on March 18, 2022.

for something."[23] Several examples of this practice that lure consumers are listed by organizations concerned with the safety of online environments.[24] Researches worldwide indicates that dark patterns are present in more than 10% of global shopping websites[25] and more than 95% of the 200 most popular apps[26]. And "the combination of lack of awareness and lack of capability" makes dark patterns' effects particularly dangerous"[27] for consumers. The extensive use of personal data in marketing and consumer contracts is a fundamental aspect of the research on commercial dark patterns, because often web scraping or harvesting techniques are employed. In Brazil we need a dialogue between the Consumer Protection Code (in Portuguese *Código de Defesa do Consumidor*-CDC, Art. 1,4,6, 7 and 39) and the General Data Protection Act (in Portuguese *Lei Geral de Proteção de Dados Pessoais* - LGPD, Art. 7, § 4, 45 and 64), to reassure the legality and no leakage of the structured database. The Ministry of Justice from Brazil has enacted a Technical Note Safe online tourism environment personal data of the consumers and found a violation of articles 4, caput, clauses I and III; 6, clauses II, III and IV, and 39, clauses II, IX and X of the Consumer Defense Code. And punished a fly tickets and tourism platform with an administrative penalty of a fine "for using consumer location data to differentiate the price of accommodations and deny vacancies, when available."[28]

23 Deceptive Design: formerly darkpattersns.org. Available at: <https://www.deceptive.design/>. Accessed on March 20, 2022.

24 See The Hall of shame of *Deceptive Design.* Available at: <https://www.darkpatterns.org/hall-of-shame/all>. Or the research of UX Design available at: <https://darkpatterns.uxp2.com/>. Both accessed on March 20, 2022.

25 MATHUR, Arunesh; ACAR, Gunes; FRIEDMAN, Michael J; LUCHERINI, Elena; MAYER, Jonathan; CHETTY, Marshini; NARAYANAN, Arvind. 2019. Dark patterns at scale: Findings from a crawl of 11K shopping websites. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW(2019), 1-32.

26 DI GERONIMO, Linda; BRAZ, Larissa; FREGNAN, Enrico; PALOMBA, Fabio; BACCHELLI, Alberto. 2020. UI dark patterns and where to find them: a study on mobile applications and user perception. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. 1–14. Available at: UI Dark Patterns and Where to Find Them: A Study on Mobile Applications and User Perception (acm.org).

27 MARQUES, Claudia Lima; MENDES, Laura Schertel; BERGSTEIN, Laís. Dark Patterns e padrões comerciais escusos, in *Revista de Direito do Consumidor,* vol. 145/2023, p. 295 – 316, jan./feb. 2023.

28 BRASIL. Ministério da Justiça. Departamento de Proteção e Defesa do Consumidor – DPDC. Processo: 08012.002116/2016-21.

II. New Relational and Data driven consumer vulnerabilities

Helberger and Micklitz argue, that in the digital and platform economy, consumer vulnerability is more and more relational, not only to providers, but now also to the intermediaries and big tech companies that have the platforms.[29] The EU has called from a different liability and duties to these 'gatekeepers' of the consumption. One great challenge for consumer protection in the Digital and Service's Society is the raise of the powerful intermediaries, especially in the new form of digital business.[30] The former middleman is now in the global digital marketplaces as 'gatekeepers'[31] of most of the consumer transactions. About the liability of these new 'intermediaries gatekeepers' I have already wrote: "They do not provide, they create the consumption opportunity, but they have the consumer data, they survey everything and they control it. They control also all practices and contracts; clauses, codes of conducts and policies of the legal relation... Sometimes they control also the payment, but always they control the consumer's data, the real 'money' in the digital world. Sometimes they also provide counting on private schemes to solve the conflict. These powerful intermediaries are the keepers of the B2C transactions, their labels, Trademarks and names are known worldwide. The result is an overconfidence of the consumer...".[32]

The UNWTO International Code of the Protection of Tourists-ICPT has an entirely Part III of the chapter IV on e-tourism because the special vulnerability of consumers in these platforms.[33] The UNWTO ICPT recognize "*the important role of digital platforms and online services in the tourism industry, as well as the risks stemming from the use of digital tourism services by tourists, Part III comprises a set of Principles calling for a fairer,*

29 HELBERGER, N.; SAX, M.; STRYCHARZ, J.; MICKLITZ, · H.-W. Choice Architectures in the Digital Economy: Towards a New Understanding of Digital Vulnerability, in *Journal of Consumer Policy* (2022) 45:175-200, p. 188ff.

30 MELLER-HANNICH, Caroline, Share Economy and Consumer Protection. *In:* SCHULZE, Reiner; STAUDENMAYER, Dirk (Orgs.). *Digital Revolution: Challenges for Contract Law in Practice*. 1. ed. Baden-Baden: Nomos, 2016. p. 119ff.

31 Expression used by Prof. Dr. Hans Micklitz in the SECOLA Conference in Oxford. See MARQUES, Claudia Lima. A nova noção de fornecedor no consumo compartilhado: um estudo sobre as correlações do pluralismo contratual e o acesso ao consumo, *Revista de Direito do Consumidor*, v. 111, n. 26, p. 247-268, may/jun. 2017, p. 247.

32 MARQUES, Claudia Lima. Perspectives for Consumer Protection in the XXI Century, in *Macau Journal of Brazilian Studies*, Vol. 4, Issue 1, Apr. 2021, p. 73-86, p. 77-78.

33 UNWTO- INTERNATIONAL CODE FOR THE PROTECTION OF TOURISTS, available in: International Code for the Protection of Tourists (unwto.org).

safer, reliable, easily accessible, transparent and accountable online tourism environment which respects and protects the human rights, tourism ethics, fundamental freedoms and consumer rights of tourists and guarantees independent recourse to judicial redress." And present 5 principles on tourists' OR consumer' protection in digital services, that can be universalized and new principles or Internet rights: 1. Safe online environment; 2. Equality and non-discrimination; 3. Transparency and fairness; 4. Protection from abuse; 5. Liability; 6. Risk prevention and management; 7. Data Protection. Coordination and cooperation; Dispute Resolution and redress.

The rise of these big tech gatekeepers-providers is a reality and consumer law must develop new instruments to deal with.

About the so called new 'data-driven vulnerability' is needed to stress that the data protection legislation is recent in Brazil. The General Data Protection Act (in Portuguese LGPD, Law n. 13.709) was promulgated in August 2018, but with a two year long *vacation legis*. The rights of consumers[34], holders of personal data, are among others at the LGPD: *I)* to know for what purpose your personal data will be processed and to know the specific purpose for which it will be processed; *ii)* to have free and easy access to your personal data, free of charge; *iii)* to be able to make corrections to personal data if they are wrong or outdated and even to demand that they be deleted, if necessary; *iv)* not have your personal data used for discriminatory, illicit or abusive purposes; and v) have security in the treatment of your personal data, so that they are not accessed by those who are not authorized. However, despite of the efforts of the personal data protection authority, the 'Autoridade Nacional de Proteção de Dados-ANPD', and the Consumer Protection System, the illegal collection and wrongful use of personal data, are a widespread reality in Brazil.[35]

The challenges are so great that we can ask if consumer law is ready for the ongoing digital age. At this point I want to call the attention of the changes of expectation of the consumers vis-à-vis the products and services.

34 MENDES, Laura. Segurança da informação, proteção de dados pessoais e confiança. *Revista de Direito do Consumidor*, v. 90, p. 245-260, nov./dec. 2013.

35 See MARQUES, Claudia Lima; MENDES, Laura Schertel; BERGSTEIN, Laís. Dark Patterns e padrões comerciais escusos, in *Revista de Direito do Consumidor,* vol. 145/2023, p. 295-316, jan./feb. 2023, p. 295ff.

C. The task of overcoming legislative and regulatory challenges of the data and platform economy to protect consumers: the revival of the constitutional bases and the need for a source dialogue

The task of overcoming new consumer vulnerabilities in the digital era is not an easy one and should be guided by the constitutional values: the protection of consumers is anchored as fundamental right in Brazil. [36] Also the use of all laws or sources to achieve the constitutional value, the so called 'Source Dialogue' by Erik Jayme,[37] can be a value instrument to overcome these challenges proposed by the digital society.

I. The need to reinforce the constitutional roots of consumer protection at the digital society: a call for more digital fundamental rights and source dialogue

In my opinion there is a need to reinforce the constitutional roots of consumer protection. The 1988 Brazilian Federal Constitution assure fundamental rights to consumers,[38] in Art. 5, XXXII: *The State must provide consumer defense through the law*.[39] With this imperative, a fundamental protection duty[40] is imposed: the State shall provide, as set forth by law, for the protection of consumers in Brazil.[41] Consumer protection becomes

36 SILVA, José Afonso. *Curso de direito constitucional positivo*. 19ª ed. São Paulo: Malheiros, 2001, p. 44ss.

37 JAYME, Erik. *Identité Culturelle et Intégration: Le droit international privé postmoderne. Cours général de droit international privé*. p. 9-268. In: Recueil des Cours: collected courses of the Hague Academy of International Law. Tomo 251. Haia: Martinus Nijhoff Publishers, 1996. p. 259.

38 BENJAMIN, Antônio Herman, O transporte aéreo e o Código de Defesa do Consumidor, in *Revista de Direito do Consumidor*, vol. 26, Apr. 1998, p. 33.

39 Official translation of the MINISTRY OF JUSTICE, *Consumer Defense in Latin America- Geopolitical Atlas*, English version, Editor Ideal, Brasília, 2005, 16. The full text of the provision is: "Article 5 is the list of individual and collective fundamental rights. All persons are equal before the law, without any distinction whatsoever, Brazilians and foreigners residing in the country being ensured of inviolability of the right to life, to liberty, to equality, to security and to property, on the following terms: {…] XXXII - *The State must provide consumer defense through the law*".

40 MENDES, Gilmar Ferreira. BRANCO, Paulo Gustavo Gonet. Curso de Direito Constitucional. 15. Ed. São Paulo: Saraiva Educação. 2020, p. 178.

41 So the oficial trabslation by the Supremo Tribunal Federal: "XXXII – the State shall provide for consumer protection, as set forth by law", accessible in: brazil_federal_constitution.pdf (stf.jus.br).

in Brazil a new hierarchy.[42] The Constitutionalization of Private Law stems from the idea of a social function to private law[43] that goes above the interest of individuals,[44] and is thus guided by the constitutional public order.[45] As a consequence all consumer protection rules of the Brazilian Consumer Code (CDC) are 'ordre publique' (Art. 1).[46]

The 1988 Brazilian Constitution is a fruit of the process of democratization after more than 20 years long military regime.[47] The 1988 Brazilian Constitution is the "most comprehensive and detailed document on human rights ever adopted in Brazil"[48] and include social-economic fundamental rights, as it of Art.5, XXXII. [49] This inclusion of private rights at the list of individual and collective fundamental rights is not a mere narrative or programmatic rule, but it has concrete consequences: "at least, establishing them as preferential over other infra-constitutional matrix rights. At most, determining concrete measures for its achievement."[50] This is especially important on the Internet, [51] where digital transactions are linked with data

42 See commentaries in MARQUES, Claudia Lima; MIRAGEM, Bruno; LIXINSKI, Lucas. Desenvolvimento e Consumo- Bases para uma análise da proteção do consumidor como direito humano, in PIOVESAN, Flávia and SOARES, Inês V. P., *Direito ao Desenvolvimento*, Belo Horizonte: Editora Forum, 2010, p. 201ss.

43 GIERKE, Otto von. *Die soziale Aufgabe des Privatrechts* (1889), republ. by Erik Wolf, Frankfurt am Main: Vittorio Klostermann, 1940, p. 2.

44 See SARLET, Ingo W. Direitos Fundamentais e Direito Privado: algumas considerações em torno da vinculação dos particulares aos direitos fundamentais", in *Revista de Direito do Consumidor*, vol. 36 (2000), p. 54-102.

45 See MELI, Marisa. Social Justice, Constitutional Principles and Protection of the Weaker contractual party, in *European Review of Contract Law*, vol. 2 (2006), nr. 2, p. 159-166.

46 See MENDES, L. S.; MARQUES, C. L.; BERGSTEIN, L. Social Diversity in Private Law and Special Law in Brazil, MPI Hamburg, 2023, not yet published, original text, p. 2.

47 SILVA, José Afonso. *Curso de direito constitucional positivo*. 19ª ed. São Paulo: Malheiros, 2001, p. 44ss.

48 PIOVESAN, Flávia. *Direitos humanos e o Direito Constitucional Internacional.* 11. ed. São Paulo: Saraiva, 2010. p. 21.

49 See SARLET, Ingo Wolfgang. *A Eficácia dos Direitos Fundamentais*. 2.ed. Porto Alegre: Livraria do Advogado, 2001, p. 48ss. And BENJAMIN, Antônio Herman, A proteção do meio ambiente nos países menos desenvolvidos: o caso da América Latina, in *Revista de Direito Ambiental*, vol. 0, Jan. 1996, p. 83ss.

50 MIRAGEM, Bruno Nubens Barbosa. O direito do consumidor como direito fundamental: consequências jurídicas de um conceito. São Paulo, *Revista de Direito do Consumidor*, v. 43, p. 111-132, jul./sep., 2002.

51 Accordingly to Luiz Edson Fachin, the Constitution presents a triple dimension: *formal*, consistent in the apprehension of rules and principles expressed in its text;

drive activities of intermediaries, platforms, and providers. The protection of the human rights and the freedom of choice of the consumers are one of the most challenges issue nowadays. Brazil knowns the protection of the fundamental rights to privacy (Art. 5, X)[52] and to the protection of personal data (Art. 5, LXXIX).[53]

Because of this triangle,[54] of consumer protection laws, data protection laws and laws protecting the freedom of choice and other fundamental rights of consumers, in my opinion, this is a mandate to the so called 'source dialogue' ('dialogue des sources', expression of Erik Jayme). The idea is not a 'mono'-'logue', but the simultaneous application of two or more laws or sources in cooperative and coherent manner to achieve the fundamental imperative to protect the users, data-owners and consumers in the Digital Economy. Article 7 of the Brazilian Consumer Code and Article 64 of the Data Law-LGPD are clear, that the rights and principles that can be used to protect consumers-data-owners can be in more than one law. A Dialogue between Consumer Code and Data Law-LGPD is given, but also new legislations like the General Framework Law on the Internet (Marco Civil da Internet) and the future AI-Bill (Bill 2338/2023-'*Marco Legal da Inteligência Artificial*').[55]

Art. 7 of the Brazilian Consumer Codes states:

> "Art. 7. *The rights set forth in this Code do not exclude any others that may come as a result of international treaties or conventions ratified by Brazil, of internal legislation, regulations set forth by administrative authorities*

substantial, apprehended of its effectiveness by the pronouncements of the Constitutional Court and by the incidence of the implicit principles derived from the explicit ones and; *prospective*, which links the actions through an open, porous and plural legal system. (FACHIN, Luiz Edson. *Questões do Direito Civil Contemporâneo*. Rio de Janeiro: Renovar, 2008. p. 6.).

52 See SUPREMO TRIBUNAL FEDERAL translation: "X – personal intimacy, private life, honor and reputation are inviolable; the right to compensation for pecuniary loss or emotional distress due to their breach is ensured". Accessible in: brazil_federal_constitution.pdf (stf.jus.br).

53 See SUPREMO TRIBUNAL FEDERAL translation: "LXXIX - under the terms of the law, the right to protection of personal data is ensured, including in digital media." And also the original text included by the Constitutional Ammedement 115 of 2022: "LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais." Accessible in: brazil_federal_constitution.pdf (stf.jus.br).

54 See also HACKER, Phillip. Manipulation by algorithms. Exploring the triangle of unfair commercial practice, data protection, and privacy law, *Eur Law J.* 2021;1–34.

55 See the text at: PL 2338/2023 - Senado Federal.

with jurisdiction, as well as any other rights that stem from the general principles of Law, analogy, traditions and fairness." [56]

Also Art.5, § 2º of the 1988 Brazilian Constitution states the same idea of coherent application of laws to protect fundamental rights: "Paragraph 2. The rights and guarantees established in this Constitution do not exclude others deriving from the regime and principles adopted by it, or from the international treaties to which the Federative Republic of Brazil is a party."[57]This rule secures that rights and guarantees, not expressly listed in the Constitution, emerge "from the regime and principles adopted by it." The central idea of the proposal is the coexistence of laws that have divergent fields of application and coordination among them, which would no longer be mutually exclusive, but would be incorporated into the system and would start dialoguing with each other to achieve their purposes.[58]

Here we are inspired by the work of Erik Jayme[59], which presupposes the simultaneous application[60] of the rules in conflict, the solution of the dialogue of the sources[61] "under the light of the Constitution". The *dialogue of the sources* is an expression created by this German Professor from Hei-

56 See Translation of PROCONRJ, available in: CDC 2014 - (Novembro 2014) -Inglês - Teste.pmd (procon.rj.gov.br).

57 SUPREMO TRIBUNAL FEDERAL, Translation. Accessible in: brazil_federal_constitution.pdf (stf.jus.br).

58 MARQUES, Claudia Lima; BENJAMIN, Antônio Herman de Vasconcellos e; MIRAGEM, Bruno. *Comentários ao Código de Defesa do Consumidor*. 3. ed. rev., ampl. e atual. São Paulo: Revista dos Tribunais, 2010. p. 31-32.

59 "Dès lors que l'on évoque la communication en droit international privé, le phénomène le plus important est le fait que la solution des conflits de lois émerge comme résultat d'un dialogue entre les sources les plus hétérogènes. Les droits de l'homme, les constitutions, les conventions internationales, les systèmes nationaux: toutes ces sources ne s'excluent pas mutuellement; elles *parlent* l'une à l'autre. Les juges sont tenus de coordonner ces sources en écoutant ce qu'elles disent." JAYME, Erik. *Identité Culturelle et Intégration: Le droit international privé postmoderne. Cours général de droit international privé*. p. 9-268. In: Recueil des Cours: collected courses of the Hague Academy of International Law. Tomo 251. Haia: Martinus Nijhoff Publishers, 1996. p. 259.

60 MARQUES, Claudia Lima. Diálogo entre o Código de Defesa do Consumidor e o novo Código Civil: o "Diálogo das Fontes". *In:* MARQUES, Claudia Lima; BENJAMIN, Antonio Herman V.; MIRAGEM, Bruno. *Comentários ao Código de Defesa do Consumidor*. 3. ed. rev., ampl. e atual. São Paulo: Revista dos Tribunais, 2010.

61 JAYME, Erik. *Identité Culturelle et Intégration: Le droit international privé postmoderne. Cours général de droit international privé*. p. 9-268. In: Recueil des Cours: collected courses of the Hague Academy of International Law. Tomo 251. Haia: Martinus Nijhoff Publishers, 1996. p. 249.

delberg to indicate the simultaneous and coherent application of more than one legal source in time, that no longer 'exclude', on the contrary, 'dialogues' under the guidance of the Constitution. "Dialogue of laws/sources" (di + a = two or more; logos = thinking or logic), meaning the current simultaneous, coherent and coordinated application of plural legislative sources, special laws (such as the CDC) and General (as the CC/2002), with converging fields of application, but not more equal, so that there is no ' conflict of laws ' and any apparent conflicts are resolved by the dialogue between the constitutional values and present in these standards.

II. Symbiotic products and services, Artificial intelligence, and the new digital consumer expectations: The crisis of consumer law effectiveness and the need of new safeguards

Symbiotic products and services are the denomination of goods with services connected or apps (immaterial goods of digital content) or services connected with objects, that only have a function together: the expectation is the interoperability, the many digital functions they serve together and durability that they will have at the market, for example, the consumer market of cell phones that can be used as TV, computers, messengers etc... and also make a call or a visual call. Miragem and I[62] use the idea of a symbiotic quality that define these services and good, and not the quality of been 'smart' (or with AI), but the fact that they have a joint and symbiotic use of the hard and soft ware, of the material and immaterial goods and services at same time, together!

In all digital goods the obligation of data protection by design and by default is relevant, but here is particularly due to the significant risks to the fundamental rights and freedoms of the consumers/persons concerned. But also, the consumer law is significantly affected by these changes.

As I argued before,[63] consumer law is facing a crisis, in a context of a new digital 'Revolution', which is transforming our mass consumer society

62 MARQUES, Claudia Lima; MIRAGEM, Bruno. Serviços simbióticos do consumo digital e o PL 3514,2015 de Atualização do CDC: primeiras reflexões, in MARQUES, C. L.; LORENZETTI, R. L.; CARVALHO, D.F. de; MIRAGEM, B. *Contratos de Serviços em tempos digitais*, São Paulo: RT, 2021, p. 391 e seg.

63 See MARQUES, Claudia Lima. Perspectives for Consumer Protection in the XXI Century, in *Macau Journal of Brazilian Studies*, Vol. 4, Issue 1, Apr. 2021, p. 73-86.

into a digital and 'services society'. which create problems for enforcement agencies and the jurisprudence. The traditional consumer law, with the division between goods and services, built in 'sales' of tangibles goods, is not enough. Especially the traditional division between gratuitous and onerous purchases, between financial services and the main performance – they are been challenged. There is a new emphasis on consumer's services (traditional services, digital services and former 'public utilities') and intelligent (or connected) goods, goods with digital or immaterial content.[64] Because of the increasing convergence/compatibility/interoperability in merging goods with services in intelligent goods, the new variety of goods with digital contents and services that needs a product in order to work (for example, a mobile phone), to be provided, the synergies between goods and services and these two consumer relationship are defying the traditional regulatory and enforcement efforts.

Dogmatically speaking, Consumer Law was built in the XX Century. 14 The first element was the choice to assure freedom and party autonomy for the weaker party, so good faith was the proper principle, allowing re-personalizing the consumers transactions, assuring more information on the market. The focus was to assure freedom, freedom of consumers on the market despite the mass and adhesion contracts. The second element were the fair treatment and the assurance of faire commercial practices and combat fraudulent and misleading practices, so confidence (trust) was the proper principle, allowing the protection of consumers with more contractual cooperation and forbidding to treat different or unfairly any party. The focus here was equality and fairness to all consumers. The third element was the quality of goods and services, which created new legal and implied warranties and the principle of strict liability of the fabricants and the solidarity of the chain of professionals involved gave the response. The focus here was the fight against 'risk society' and to assure a fraternal distributive effect of the consumer protection laws. These legal elements were in all consumer laws on the globe. My last element of this traditional consumer protection is the local enforcement. We built very efficient national enforcement systems to protect consumers, sometimes regional or supranational, like in the EU and now in the Mercosur, but we do not have

64 See the new European Directives, Directive (EU) 2019/770 and 771 'on certain aspects concerning contracts for supply of digital content and digital services.

a truly international binding instrument to consumer protection and this soft system is not working anymore.[65]

In the digital world the consumers have more choice and information than never, but they never know who is controlling the consumer transaction. We spoke about 'framed' autonomy (Norbert Reich)[66] from the professionals; today we should speak about 'framed' information – we have all information, but not those we need… and no control at all about it. And what about fairness? The conformity of services was always a challenge for consumer law and now with goods of digital content the challenge is renewed. Fairness in contract and in commercial (and data) practices in the digital marketplace is also a hot topic. It is necessary to point out that, here, we have old/new contracts, old like 'sale contracts', but with new elements like the digital content. And we have very old contracts, like the roman 'locatio conductio' with new approaches in services contracts of the digital Era. The facilities to identify and to 'profile' the consumer is now allowing new kinds of discrimination, like the geo-blocking and the geo-pricing. With the possibilities of the Big Data, the Internet of Things, the algorithms, the AI, the robot-toys and the intelligent products, these kinds of storage (and treatment) of great number of consumers' data can also be a used to discriminate in the future.[67]

Safeguards are needed to protect the rights of individuals or consumers. As we stated before, the challenges linked to the articulation or dialogue of the current consumer laws and the new legislative framework on data protection is particularly important to give consumers meaningful protection, granting consumers using electronic commerce and new technology applications a level of protection that is no less that afforded in other forms of commerce, avoiding all kind of consumer discrimination and giving some control and information over how their data generated through the use of connected objects and symbiotic services and goods.

65 So, I argued in MARQUES, Claudia Lima. Perspectives for Consumer Protection in the XXI Century, in *Macau Journal of Brazilian Studies*, Vol. 4, Issue 1, Apr. 2021, p. 73-86 p. 76.

66 REICH, Norbert; MICKLITZ, Hans-W; ROTT, Peter; TONNER, Klaus. *European Consumer Law*, Intersentia, Cambridge, 2014.

67 MARQUES, Claudia Lima. Perspectives for Consumer Protection in the XXI Century, in *Macau Journal of Brazilian Studies*, Vol. 4, Issue 1, Apr. 2021, p. 77.

D. Final Observations

The special vulnerability of consumers in the digital economy is a reality. The 7th World Conference on Consumer Law, organized by the IACL-International Association for Consumer Law in Helsinki in 1999 have already mentioned that the Internet have "starts a new era for the consumer" and consumer law.[68] An conclude that consumer law should not accept the lowering of the present level of protection because of these new technologies.

Many years passed, the challenge seems greater with the scale and innovation brought by the Artificial intelligence, smart contracts, the platform society and servicization of consumer goods.[69] The protection of personal data is also a challenge in this digital economy. As Danilo Doneda stated protection of data is in reality protection of an individual.[70] Regulate online platforms and gatekeepers are now an objective of both consumer and constitutional law.

And because Digital Constitucionalism is about methodological innovation, I call the attention of an ILA Resolution 7/2022[71] aiming to raise awareness among responsible business of the digital marketplaces and e-commerce. In the trend of self-compliance and co-regulation this so called "CONSUMER GLOBAL COMPACT IN THE DIGITAL ECONOMY" brings a set of voluntary standards, that can support digital companies to align their activities with fundamental responsibilities in the areas of consumer rights, data protection, new marketing, redress and enforcement of consumer rights:

68 WILHELMSSON, Thomas. Foreword in WILHELMSSON, Thomas; TUOMINEN, Salla; TUOMOLA, Heli. *Consumer Law in the Information Society*, The Hague: Kluwer Law International, 1999, p. XXI.

69 WEI, Dan; NEHF, James P.; MARQUES, Claudia Lima (Org.). *Innovation and the Transformation of Consumer Law*. 1. ed. Singapore: Springer Singapore, 2020.

70 DONEDA, Danilo. *Um Código para a proteção de dados pessoais na Itália*. Disponível em: <http://egov.ufsc.br/portal/sites/default/files/anexos/29727-29743-1-PB.pdf>. Accessed on July 30, 2019: "A própria expressão "proteção de dados" não reflete fielmente o seu âmago, pois é resultado de um processo de desenvolvimento do qual participaram diversos interesses em jogo – não são os dados que são protegidos, porém a pessoa a qual tais dados se referem.".

71 See ccpb_IGECON_Resolution_Lisbon_ILA_en.pdf (unctad.org).

"Principles of the ILA`s Consumer Global Compact in the digital economy

The Principles are:

Consumer Rights

1. *Business should support and respect consumer rights, especially in compliance with the UNGCP (UN-Guidelines on Consumer Protection, 2015) and grant consumers using electronic commerce and new technology applications a level of protection that is no less that afforded in other forms of commerce, avoiding all kind of consumer discrimination.*
2. *Business should uphold freedom of choice and provide the consumer with complete and useful information on time and in an understandable manner.*
3. *Business should develop a unified standard to deal with cross-border consumer transactions and not deprive consumers using e-commerce in cross-border transaction from the most protective provisions afforded to them by the mandatory applicable laws.*
4. *Business should make sure that they are not complicit of frauds or violations of human rights and environmental rights in the marketplace or supply chains.*

Data Protection and New Marketing

5. *Business should control and share responsibility of the behavior of intermediaries, employees, influencers, and the addressable marketing personnel.*
6. *Business should ensure by design, data protection and AI fairness. The processing of the consumers' personal data should be done lawfully, fairly and in a transparent manner, respecting the principles of purpose limitation, data minimization, data accuracy, storage limitation, integrity and confidentiality and accountability, and guaranteeing data subject rights.*
7. *Business should undertake initiatives to promote greater data protection and consumer privacy. It should be assured a fair algorithmic treatment, that does not make unfair discriminations; algorithmic transparency; and the right of the consumer to contest an algorithmic decision.*
8. *Business should consider children and adolescents' weakness, aged persons and other vulnerable consumers and not impose to then burdens or constraints.*

Redress and Enforcement Rights

9. *Business and other stakeholders should work together with national enforcement agencies and seek for consensual and amicable consumer dispute resolution. Business should engage in multiple-stakeholders' discussions and supports international cooperation for cross-border dispute resolution. The introduction of due diligence frameworks would increase the levels of responsible business conduct and international cooperation, enhance information and transparency, increase sustainable development, and enhance confidence amongst consumers.*
10. *Business should encourage accessible consumer ODR platforms and channels for consumer redress including cross-borders disputes.*
11. *Business should ensure the compliance of international standards by the ADR/ODR and other services and platforms for amicable resolution of consumer disputes they use or recommend, fostering the development of fair, transparent, accessible, informed, impartial, free of charge or inexpensive for consumer and expeditious solutions for cross border cases.*
12. *Business should ensure that consumers are free to access voluntarily dispute resolution and redress mechanisms, as well as judicial or administrative redress mechanism for consumers acting individually or collectively, and to benefit from the positive outcomes of such procedures. The ADR/ODR mechanism should be mandatory for business and voluntary for consumers and the decision, if not consensual, should be binding only for business."*[72]

Indeed, considering the expansion of the digital economy and the new global organization of digital big techs and digital global corporations, sharing platforms and chains of providers, organizing marketplaces to reach consumers, reproducing technologies and practices worldwide it is possible to ask these responsible businesses to voluntarily join this principles-based approach to doing business globally. The original ten principles of the UN Global Compact cover human rights, labour, environment, and anti-corruption. These new Principles aim to make up for the 'new vulnerabilities' that global consumers are experiencing in the digital economy and create a voluntary common ground to the worldwide activities in consumer e-com-

72 See https://unctad.org/system/files/non-official-document/ccpb_IGECON_Resolution_Lisbon.

merce, platforms and data driven companies, helping the compliance and enforceability of consumers rights worldwide.

The Brazilian Marco Civil da Internet: Features and the question of liability for content moderation

Fabiano Menke[*]

Abstract: In the year of 2014 Brazil approved the so-called Marco Civil da Internet, its civil legal framework regulating the internet. This work seeks to present the context of the approval of this act and to briefly describe some of its provisions such as the ones concerning net neutrality, data protection and data retention duties by internet service providers. Moreover, the work seeks to inform about the judgement of a crucial case by the Brazilian Supreme Court (STF) which shall take place in the year of 2024 and will define if the provision of the Marco Civil da Internet concerning the civil liability of internet service providers is constitutional. As indicated at the final remarks of the paper, the Brazilian Supreme Court will be ruling if article 19 of the Marco Civil da Internet is still up to date and in which extent international legal initiatives such as the European Digital Services Act (DSA), which establishes heavier duties for the platforms, might influence Brazilian Law.

A. Introduction

In the context of our panel, "consumer protection and digitalization", I intend to approach a rule that came into force in Brazil in the year of 2014, the so-called Marco Civil da Internet[1], which could be translated as Civil Framework for the Internet.

My purpose is to present the context of the approval of this act and a general and a short description of it, as well as briefly deal with one case

* I would like to thank the colleagues Prof. Indra Spiecker gen. Döhmann, Prof. Laura Schertel Mendes and Ricardo Campos for the chance to gather with such a special group of researchers. And I also enjoyed the opportunity to listen to interesting speeches like the ones from Profa. Claudia Lima Marques and Prof. Stefan Grundmann in this panel.

1 Lei nº 12.965, 23.04.2014.

involving perhaps the most important provision in this legal act in Brazil, Article 19, which states rules concerning the liability of internet service providers for illegal content. This case was presented to our Constitutional Court in the year of 2017 and should be decided in the year of 2024 after a long period of internal procedures[2].

I wish to close my remarks summarizing the greatest challenges that are ahead of Brazil in the regulation of the area.

B. Marco Civil da Internet - context of its approval and overview of its content

Let me start by drawing the scenario in which Marco Civil da Internet was discussed and approved.

On the year before the approval of the Marco Civil, 2013, we shall all remember, the Snowden leaks case captured the attention of the world. Edward Snowden as a former National Security Agency consultant leaked highly classified information from the United States of America security agencies.

Brazil was involved in this just like many other countries: the president at that time was Dilma Roussef and the Snowden leaks revealed among other things that the telephone of the presidential airplane was tapped by the NSA.

After these happenings, and especially because of the public statements of President Dilma Roussef demanding for a Brazilian rule on internet, the draft of the Marco Civil that had been in discussion since 2009 went on a fast-track procedure and was approved in April of 2014.

The name Marco Civil is due to the fact that most of the debates on the first decade of the years 2000 in our country were around the discussion of criminal law acts concerning the digital and the internet. These acts were indeed approved but the outcry that we lacked a basis of legislation for the use of the internet got louder. Even President Lula when he was in power in the first decade of this century claimed for a "civil act" for the internet in Brazil. Therefore, the name Marco Civil da Internet is so-called as a counterbalance to the criminal rules that entered into force firstly in Brazil.

At the beginning of the "digital", our country did not react by elaborating new general rules for the "new world". Instead, it awaited the occurrence of

2 The case was filed at the Constitutional Court, Supremo Tribunal Federal, under following identification: RE 1.037.396. For details: www.stf.gov.br.

the facts to trigger the legislation in the areas that claimed for regulation. A different development was chosen by Germany, where the Civil Code was very early adapted for the new ways of establishing relationships as a result of the reform of the law of obligations in the year of 2001.

One example of regulation other than in the field of criminal law, is the electronic signatures act[3], that Brazil approved in 2001, establishing a national public key infrastructure that can be considered as a real success, as it has enhanced the security of online transactions for decades.

When we turn back do Marco Civil, it is relevant to mention that it established many rights for the use of the internet. And among those rights a minimum of data protection was already there. As we know, our general rule for data protection was approved only in 2018[4], but the Marco Civil almost five years before regulated, for instance, consent in the context of data protection, determining some of its conditions.

What really happened is that during the elaboration of the Marco Civil draft, the idea was present of importing some of the data protection rules from the general data protection act that was already being discussed at that time in the Parliament.

Also, interesting to note that the Decree n. 8771 which established detailed regulation of the Marco Civil brought to our legislation the concept of personal data[5], which is very similar to the one that would later on be present in our Data Protection Law and that was also inspired in the European model.

It is clear that these rules were only the beginning of specific general rules in data protection in Brazil. With the enactment of the Data Protection Law, other possibilities of legal basis for the processing of data along with the traditional consent were foreseen and now Brazil has a very modern and updated legislation in the field[6].

---

3 The act is the so called Medida Provisória nº 2.200-2/2001. This act is still in force in Brazil and in the year of 2020 the Lei nº 14.063 established new levels of electronic signatures in the direction of the European regulation.

4 The so called LGPD, Lei Geral de Proteção de Dados: Lei nº 13.709/2018.

5 I mean hereby the idea that personal data is the information related to an identified or identifiable natural person.

6 It is curious to note that inspired by the European tradition the Brazilian data protection act also stated the possibility of processing data on the legal basis of the legitimate interest of the controller or processor (Article 7, X, LGPD).

Marco Civil also established in Brazil the principle of *net neutrality*[7] which states that the internet service providers must treat all internet communications equally, offering users and online content providers consistent rates irrespective of content, website, platform, equipment or application, source or destination address.

The guarantee of a minimum of internet access to the users in Brazil is therefore a big issue in this act and it remains a constant challenge for the regulation to find the balance between the net neutrality principle and the business models of service providers that wish to sell different kinds of data packages.

I mention here two other very important rules that were enacted with the Marco Civil. And these are the ones that assign a term for the data retention duty within the activities of service providers.

In this subject the Marco Civil states a twelve-month term for the retention of the internet access data by internet connection providers (Art. 13). That means that with this information it is possible to know when the user's connection to the internet started and when it stopped.

The second rule on the data retention duty establishes a six-month term for the retention of the information concerning the access to the applications (Art. 14). We deal here with the application layer. With this information it is possible to know when the user's access to a specific application started and when it stopped. This rule was totally new in Brazil when it came into force, because so far only the access information would be collected by internet service providers.

In both cases the service provider will only disclose the retained information upon receipt of a judicial order.

A final remark about the context of the facts during the legislative debate of the draft of the Marco Civil da Internet should be made. At that time, the Brazilian government expressed the intention to design the rules so that internet service providers should be obligated to host their data centers in Brazil and not overseas. The effects of this provision would prevent happenings such as the ones brought about by the Snowden leaks case.

This specific rule suggested by the government was widely rejected by specialists and associations, that considered a step backwards in a world

7 Art. 3, IV and art. 9, Marco Civil da Internet.

that was already and still runs towards globalization: the provision was not included in the approved version of the act[8].

Nonetheless it is interesting to notice that this discussion has gained new impulse in the years that followed the approval of the Marco Civil da Internet. And this not exactly in Brazil, but especially in Europe in the context of the international transfer of personal data.

As broadly known, the European Court of Justice delivered two very relevant judgments in the years 2015 and 2020, when it ruled that the European Commission's adequacy decision for the international data transfers with the United States of America were invalid, respectively, Safe Harbor Framework and Privacy Shield Framework.

The main issue in the discussion is that of the possibility of the access U.S. intelligence authorities may gain by requesting the disclosure of personal data from citizens covered by European data protection legislation to its public entities or to in its territory-based companies.

These concerns have raised the implementation of measures in order to avoid that the communication established in Europe flows to the United States of America, or at least that when this occurs there will be no information request by the NSA. The concept of digital sovereignty describes the possibility of countries, organizations and individuals take independent and self-determined decisions related to the use and design of systems and the information created and processed by these systems[9].

If we take the example of the Commissioner for Data Protection in the State of Hessen in Germany, we will notice that this state has implemented specific measures in order to promote digital sovereignty such as the negotiation with videoconference applications providers so that the information exchanged by this means in Hessen does not flow to servers located in the United States[10].

In July 2023 a new adequacy decision for the United States of America was issued by the European Commission. It is not surprising to notice that

8 SOUZA, Carlos Affonso; LEMOS, Ronaldo. Marco Civil da internet: construção e aplicação. Juiz de Fora: Editora Associada LTDA, 2016.

9 On the matter see: Digitale Souveränität und Künstliche Intelligenz - Voraussetzungen, Verantwortlichkeiten und Handlungsempfehlungen. https://www.de.digital/DIGITAL/Redaktion/DE/Digital-Gipfel/Download/2018/p2-digitale-souveraenitaet-und-kuenstliche-intelligenz.pdf?__blob=publicationFile&v=5.

10 On this, see the Commissioner's Report for Data Protection in the year of 2021 in the State of Hessen. https://www.zaftda.de/tb-bundeslaender/hessen/landesdatenschutzbeauftragter-2/807-50-tb-lfd-hessen-2022-20-8296-vom-08-06-2022/file.

the non-profit organization Non of Your Business, under the leadership from Austrian data protection activist Max Schrems, has announced that they will challenge the decision before the European Court of Justice[11].

What concerns Brazil, the supervision authority for data protection, ANPD, will most likely deliver in the year of 2024 a regulation on international data transfers and the issue of digital sovereignty should be addressed. As we see, the discussions about the location of servers and data centers could be relived in Brazil just like ten years before when Marco Civil da Internet came into force, but this time in the context of the international transfer of personal data.

C. Marco Civil da Internet and the case brought to the Constitutional Court

Getting back to the Marco Civil da Internet, and as mentioned in my introduction, I would like to focus on a case that is under judgement by our Constitutional Court and that comprehend the legal text I have just introduced but that at the same time touches on the consumer protection and on our Code of Consumer Protection[12].

The case has to do with content moderation through platforms. But before I report about this decision, let me shortly come back to Marco Civil da Internet.

Marco Civil rules the matter of content moderation stating as usual that there is no general monitoring or active fact-finding obligations for service providers[13]. They are as a basic principle not liable for illegal content published by other users.

But the most discussed provision of this legal text in this context is Article 19, the one that determines that in honor of the values of freedom of expression and to avoid censorship[14] the service provider will only be liable for the illegal content published on its platform if the provider does

11 https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu.

12 The Brazilian Code of Consumer Protection was enacted by the Lei nº 8.078/1990.

13 Article 18 of Marco Civil da Internet.

14 It can be stated that in general the Brazilian legal system considers the freedom of expression in a preferred position when confronted with personality rights. A very important case in which these values were balanced was the constitutional claim (ADPF 130) against the so-called Brazilian Press Act. This judgement took place in 2009 and the conclusion was that of the unconstitutionality of the act, considering the fact that it was enacted during the military dictatorship in Brazil and contained

not take efforts to remove the publication after a judicial order. I repeat: *an order from a court* is necessary to give knowledge to the service provider and trigger its liability for the damages the publication caused to the internet user.

An exception to the requirement of a judicial order for the removal of the illicit material takes place when the publication encloses sexual material or nudity. In this case the notice submitted by the affected individual should be enough to impose a subsidiary liability on the service provider[15].

As mentioned, we have this rule since 2014. But it is interesting to notice that before its enactment, courts in Brazil including our highest one for the interpretation of federal law, Superior Tribunal de Justiça (STJ), had consolidated the notice and take down principle, according to which the service provider will be liable in case he is directly notified by the user and does not remove the illegal content.

The change promoted by Marco Civil da Internet generated many complaints from consumer protection associations, from academy and other institutions considering that the efforts needed to be made by the users with the new rule would be much higher to remove the illegal content, interfering in the exercise of their rights. The comparison is between the simple notice made directly by the user towards the service provider and the formalities and costs involved with filing a suit in a court.

This gave rise to the aforementioned constitutional complaint. I should here observe that the case was at its origin processed in the courts of the State of São Paulo and the last decision there, which will be tested in the Brazilian Constitutional Court raises the question that the consumer law as a constitutional value should prevail over the Brazilian legal framework for the Internet (Marco Civil da Internet).

It will be decided if although the Marco Civil states the liability of service providers for illegal content only after a judicial order, the rules of the Consumer Code that determine a strict liability for damages for defective services should be or should not be applicable. It is always to be mentioned that since the entry into force of the Consumer Code in 1990, Brazil has developed a very powerful system to protect these relationships. Brazilian law is since then marked by this attribute and whenever a new act or subject

---

some outdated rules such as limitations on the freedom of expression of journalists and even criminal dispositions in order to restraint the press freedom.

15 Article 21 of Marco Civil da Internet.

comes to debate in Parliament, considerable worries are expressed so that the high level of consumer protection should not be affected.

If we take one more time the example of the Brazilian data protection act (LGPD), we get an idea of the importance consumer protection has gained in our country. During the discussion of the LGPD, especially in the subject of the rule of civil liability, the concern of not interfering in the strict liability rules of consumer law was present. For this reason, the new rule was designed in such a way that consumers would face no disadvantages.

The specific article states that any violation of rights in the field of data protection will still remain subject to the consumer liability dispositions already in force.

These interfaces between consumer law and the rules that followed it, such as LGPD and Marco Civil da Internet, make so challenging for lawyers and courts to find the reasonable approach that guarantees harmony to the system.

This is a reason why the case dealing on the constitutionality of Marco Civil da Internet was supposed to have a public hearing so that the society and judges would plunge into the details and complexity involved in the matter. But on the exact week in the year of 2020 when the hearing should take place the covid pandemic was declared in Brazil and thus the activities suspended. The public hearing eventually took place in March 2023. As usual in Brazil, and the same happens when judgements of the Constitutional Court occur, the hearing was also r live stream broadcasted and remains recorded in the internet.

These moments are a very rich experience for the constitutional judges and for the society as a whole. Just like many other countries of the Roman Germanic system, the weight of judicial decisions has considerably increased in Brazil in the last decades. As argued by constitutional law scholars, some of the debate that usually takes place at the legislative houses has been brought to the Judiciary, as the decisions in many of its procedures affect the entire population and not only the demanding parties of the concrete case.

A handful of *amici curiae* were admitted contributing with their perspective regarding the matters in dispute.

One interesting remark made by the lawyers of the social media providers is that along the years their services have evolved considerably. As argued, nowadays the platforms monitor and remove most of the illicit content that is published. This seems to be a true fact but it is still questionable if all this effort made by social media platforms covers many cases

where agility and uncomplicated measures are needed, especially when individuals face violations to their personality rights.

Another aspect that is usually pointed out in the debate is that Marco Civil da Internet facilitates the access to courts when claims for content removal or for damages are necessary. In this case, the Internet users may file their suits at the specialized courts for the popularly called "small claims". This means that the suits are processed in a fast track, with no costs and reduced possibilities of appealing against a sentence.

The judgement of this case is anxiously awaited in Brazil and involves, a general repercussion, meaning that lawsuits on this subject are suspended and await this decision that will have *erga omnis* effects, confirming that the work of the courts and especially of our Constitutional Court draws much of the attention in the field of law.

D. Final Remarks

Marco Civil da Internet was recognized as a modern legal initiative when it was approved in Brazil (2014) and it opened a broader path for the regulation of the digital world. The issues raised at that time such as the location of data centers of service providers are not abandoned and now gain a new impulse with the legislation of data protection and the chapter that deals with international data transfers.

Nonetheless, it is appropriate to ask if Marco Civil da Internet could be by any means modernized, as we consider the facts that have been attracting the attention of courts and legislators around the globe.

One of the questions that raise after the approval of the Digital Services Act in Europe and its approach for the continuity of the notice and take down model is if we will have an influence in Brazil of the Brussels effect when our Constitutional Court decides the subject.

We shall here remember that according to the DSA, following the steps of the E-commerce Directive, the responsibility for the platform is triggered upon the user's notification of the illegal content without the need for a judicial decision.

The European Model based today on the DSA and in this context, we could also exemplify through the German NetzDG (Netzwerkdurchsetzungsgesetz), which is in force for over five years, is based on setting heavier duties for the platforms such as:

– Transparency reporting obligations on content moderation;
– Run mechanisms to allow users to notify them of illegal content;
– Provide statement of reasons for suspensions of services;
– Provide internal complaint-handling systems to the decisions that are made in the work of moderation.

As we have seen, the Brazilian legal system at this moment does not impose such duties like the European legal system, although we should not forget the intense effort that has been made by the social media platforms in order to monitor the violations of its terms of use that prohibit illicit content.

The crucial question still emerges: Is the Brazilian system and Article 19 of the Marco Civil still up to date?

And I should mention here not only the Brussels effect but also the UNESCO effect. UNESCO is also elaborating its guidelines for regulating digital platforms, aiming to safeguard freedom of expression and access to information.

And in this initiative duties imposed to the service providers shall also be present.

In this context we should also consider the value of democracy. The UNESCO Guidelines set a list of specific measures to guarantee the integrity of elections in an open fight against disinformation.

And as we have seen in Brazil in the last presidential election, in the year of 2022, content moderation in the electoral context is of an immense importance. For someone who lives in Brazil and votes in the elections it is quite confusing and challenging to get real information and true facts especially during presidential campaigns. A war of fake news usually takes place at this decisive event of the democracy. The Brazilian Electoral courts and mainly the Superior Electoral Tribunal face an overload of work during elections and the fake news issue in this area has turned to be one of the greatest challenges of the country.

Targeting the Brazilian population, the Superior Electoral Tribunal has been working intensively to promote campaigns that help the voters to recognize and to avoid being influenced by disinformation during the election period.

But the efforts shall not stop: with the growing sophistication of generative artificial intelligence tools, democracy will face enormous challenges in order to maintain its foundations of justice and freedom when people exercise one of their most valuable rights such as the one to elect representatives.

The next steps are to be followed in Brazil: new law drafts, new judicial decisions and new facts are to come. But if an opinion would be asked, there should be no doubt that a tendency is currently present in our country: Brazil will most likely be influenced by the Brussel effect and raise the level of duties to internet platforms.

This tendency expresses the widespread inspiration of the European legal tradition in Brazilian Law, what can be confirmed through examples listed in this work, such as data protection, electronic signatures, and others, and remembering the European influences in our Consumer Protection and in our Civil Code.

Digital constitutionalism as an online speech governance framework: A critical approach

Clara Iglesias Keller and Jane Reis G. Pereira

Abstract: This chapter advances a critical approach to the theories of "digital constitutionalism", in particular as a theoretical framework for recent initiatives targeting online speech governance. We build on previous work where we demonstrated overarching risks of borrowing from the symbolic load of the constitutionalist tradition to name and explain transnational normative phenomena that take place in private digitalised environments. We apply these critiques to the case of online speech governance by looking at two policy initiatives: the Meta Oversight Board, a private sector self-regulatory initiative implemented by the company Meta; and the European Digital Services Act. Our goal is to shed light on contradictions and misperceptions embedded in labelling online speech governance mechanisms as manifestations of digital constitutionalism.

A. Introduction

Intermediation by global private actors cuts through various socio-political challenges associated with the digital world. Digital platforms exert power over what and how we communicate, also determining access to information and all sorts of cultural goods. They have preponderant access to users' personal data, thereby leveraging one's ethnicity, gender, sexual orientation, religion, and political ideologies. They concentrate possibilities for market inclusion, as their infrastructure allows for several commercial transactions – all while steering these different spheres of social, political, and economic organisation according to their own governance mechanisms. Ultimately, there is an inherent democratic deficit to the private ordering of these virtual spaces, which "refers to the fact that private companies make the choices that set norms and directly influence the behavior of billions of users", raising concerns about the "interests behind these choices, the pro-

cesses that led to them and their binding nature"[1]. While this deficit does affect the exercise of fundamental rights in general, digital platforms' role as communications infrastructure raises the stakes especially for freedom of expression, because "decisions about what we can do and say online being made behind closed doors by private companies is the opposite of what we expect of legitimate decision-making in a democratic society"[2]. The democratic deficit in speech governance is embodied by the lack of transparency and predictability of platform's interventions in user-generated content, notably because such interventions are based on unilaterally and asymmetrically set terms of use.

Modern liberal democracies rest broadly on a right to freedom of expression, as a precondition for both individual self-development and partaking in collective institutional and meaning-making processes. Media and communications fora are key dimensions of political participation, as they co-shape forms and possibilities for engaging in and influencing political processes. For this reason, guaranteeing a fair public sphere – with equal access to information and freedom of expression prerogatives – has long inspired theoretical and regulatory approaches aimed at the maintenance and development of democracies.

As a continuation of this movement, the expansion of digital communications has inspired interdisciplinary literature to understand the transformations in the public sphere that accrue from this intermediation of private and collective communications, as well as their implications for freedom of expression and political participation[3]. This includes theoretical and governance approaches for the insertion of public values – be it by state regulation, multi-stakeholder, or private governance – in an environment

1 Blayne Haggart and Clara Iglesias Keller, "Democratic Legitimacy in Global Platform Governance," *Telecommunications Policy* 45, no. 6 (July 1, 2021): 102–52, https://doi.org/10.1016/j.telpol.2021.102152.

2 Nicolas P. Suzor, *Lawless: The Secret Rules That Govern Our Digital Lives* (Cambridge, United Kingdom; New York, NY: Cambridge University Press, 2019), 8.

3 Andreas Jungherr and Ralph Schroeder, "Disinformation and the Structural Transformations of the Public Arena: Addressing the Actual Challenges to Democracy," *Social Media + Society* 7, no. 1 (January 2021), https://doi.org/10.1177/2056305121988928; Jack M. Balkin, "Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation," *SSRN Electronic Journal*, 2017, https://doi.org/10.2139/ssrn.3038939; Amélie Heldt, "Merging the Social and the Public: How Social Media Platforms Could Be a New Public Forum," *Mitchell Hamline Law Review* 46, no. 5 (January 1, 2020), https://open.mitchellhamline.edu/mhlr/vol46/iss5/1.

where information and attention fluxes are determined by commercial practices.

This is the background against which digital constitutionalism has gained momentum, notably in political and legal sciences, as a framework for making online interactions conform to constitutional requirements[4]. The term is broadly applied to distinct situations that relate to the protection of constitutional rights in the context of digital technologies, and it often conveys mitigation of power over technological infrastructure as a response to the above-mentioned democratic deficit. However, its many applications express theoretical and institutional perceptions of the constitutional phenomenon that often diverge from the meanings and ends that inform modern constitutionalism itself.

In previous work, we advanced a critical analysis of "digital constitutionalism" theories, where we focused on the risks involved in taking up and taking over the symbolical load of the constitutionalist tradition to name and explain transnational normative phenomena and events that take place in private digitalised environments[5]. In the present contribution, we apply these critiques to the case of online speech governance by looking at two policy initiatives aimed at improving legitimacy standards in online freedom of expression enforcement: the Meta Oversight Board, a private sector self-regulatory initiative implemented by the company Meta, in contrast to the European Digital Services Act (DSA), a supranational regulation enacted by the European Parliament[6]. While they both originated in distinct institutional settings – private and public – each of these experiences can

4 Edoardo Celeste, "Digital Constitutionalism: A New Systematic Theorisation," *International Review of Law, Computers & Technology* 33, no. 1 (January 2, 2019): 76–99, https://doi.org/10.1080/13600869.2019.1562604; Giovanni De Gregorio, *Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society*, 1st ed. (Cambridge University Press, 2022), https://doi.org/10.1017/9781009071215.

5 Jane Reis G Pereira and Clara Iglesias Keller, "Digital Constitutionalism: Contradictions of a Loose Concept," *Revista Direito e Praxis* 13, no. 4 (2022): 2648–2689, https://doi.org/10.1590/2179-8966/2022/70887.

6 The Digital Services Act focuses on content regulation across different digital platforms and is aimed at "a safer digital space in which the fundamental rights of all users of digital services are protected". The Digital Markets Act regulates the consumerist and competition dimension of online exchanges, with the declared purpose of establishing "a level playing field to foster innovation, growth, and competitiveness, both in the European Single Market and globally" European Commission, "The Digital Services Act Package," September 25, 2023, https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package.

be framed as institutional innovations aimed at implementing legitimacy standards for online speech governance. Moreover, each of them has been related to "digital constitutionalism"[7], even though their features are mostly inconsistent with the premises of modern constitutionalism. Beyond the fact that each of these cases represent imprecise notions of constitutionalism encompassed by "digital constitutionalism", comparing the two leads to further misunderstanding. This is because current digital constitutionalism theories include them in the same category, despite each having distinctive features and entailing different degrees of power (im)balance.

Our goal is to tease out the contradictions and misperceptions embedded in labelling online speech governance mechanisms as manifestations of digital constitutionalism. Ultimately, a fair assessment of such initiatives – of which the Meta Oversight Board and the European DSA are two examples – also depends on unravelling what the choice of constitutional metaphors reveals (in terms of the intended narratives) and what it hides.

Our reflection takes place in two parts. In the first one, we organise our set of critiques according to current uses of the expression "digital constitutionalism", while highlighting relevant risks and inconsistencies in applying the term to explain recent online speech governance initiatives. In the second part, we apply this critique to our exemplary cases of Meta's Oversight Board and the European Digital Services Act. The chapter concludes with a summary of the arguments we cover.

B. Digital constitutionalism: a critical approach

In previous work[8], we have proposed a discussion on the risks involved in borrowing from the symbolical value of the constitutionalist tradition to name and explain transnational normative phenomena and events that take place in private digitalised environments. This critical approach stems from the tradition of modern political theory, where the idea of constitutionalism refers to a specific political and legal movement that emerged amidst the

7 Luciano Floridi, "The European Legislation on AI: A Brief Analysis of Its Philosophical Approach," *Philosophy & Technology* 34, no. 2 (June 2021): 215–22, https://doi.org/10.1007/s13347-021-00460-9; De Gregorio, *Digital Constitutionalism in Europe*; Angelo Jr Golia, "Beyond Oversight: Advancing Societal Constitutionalism in the Age of Surveillance Capitalism," *SSRN Electronic Journal*, 2021, https://doi.org/10.2139/ssrn.3793219.

8 Pereira and Iglesias Keller, "Digital Constitutionalism: Contradictions of a Loose Concept."

XVIII century liberal revolutions. In this realm, constitutionalism emerges as a particular doctrine of political organisation centred on a legal constitution, which is understood as a normative instrument that institutes and regulates government and is designed to limit the exercise of state power and protect individuals.

However, both changes in the exercise of state power – influenced by transnational forces – and the expansion of private power on a global scale have given constitutionalism new applications and conceptualisations. There is a group of theories that uses the terms constitution and constitutionalism to define normative and institutionalising efforts in the international sphere and in private spaces, notably constitutional pluralism, societal constitutionalism, and global constitutionalism[9]. Differences aside, these approaches share the use of constitutionalism to define processes of institutionalisation of powers and legal structures that emerge outside and beyond the nation-state. Contrary to the meaning attributed to constitutionalism in the modern state, these uses employ the concept of constitution as a label that gives non-state normative processes the stability and legitimacy normally associated with liberal constitutions. Despite their value in identifying normative spaces beyond state authority, this strain of literature has been criticised for approaching constitutions as "a metaphor"[10]. We understand digital constitutionalism as a continuation of these theories; in fact, they are utilized as their theoretical framework. Therefore, we will return to this and other sets of criticism of this theoretical matrix shortly, when debating the risks and limitations in current approaches to digital constitutionalism.

Against a backdrop of shifting state powers and expanding private powers, the concept of constitutionalisation has recently been used to describe legal practices and the protection of rights in the realm of digital technologies. In fact, this set of theories that underpins digital constitutionalism – the theoretical matrix above – has often referred to the digital sphere as an experimental paradigm of norm enforcement that exceeds the capacities of the state[11]. Although the concept of constitutionalisation has appeared in

9 Pereira and Iglesias Keller.

10 Marcelo Neves, "(Não) Solucionando Problemas Constitucionais: Transconstitucionalismo Além de Colisões," *Lua Nova: Revista de Cultura e Política*, no. 93 (December 2014): 201–32, https://doi.org/10.1590/S0102-64452014000300008.

11 Pereira and Iglesias Keller, "Digital Constitutionalism: Contradictions of a Loose Concept," 2656.

debates about digital technologies conforming to the rule of law since the early 2000s, the term has recently gained further currency. Recent calls for digital constitutionalism have emerged in a political, social, and economic context largely shaped by the idea of the "platform society", a concept that. captures the pervasive technological mediation through private digital platforms that have "penetrated the heart of societies"[12], affecting institutions, economic transactions, and social and cultural practices.

In this context, digital constitutionalism is generally presented as an interpretative framework to theorise the emergence of measures that mitigate the concentration of economic and political power by such platforms, be such measures public, private, or hybrid. In the face of private companies that run their own infrastructure and make decisions that affect billions of people, regulatory and academic debates seek solutions to protect rights and ensure individual and collective self-determination in those environments. They often appeal to ideas like the rule of law[13], sovereignty[14], representative democracy, and constitutionalism[15] as means of (re)introducing, into the digital realm, the values that inspired democratic and liberal political arrangements in the first place. This means that constitutional metaphors pervade public and theoretical debates on the role digital platforms play in our societies. For the case of digital constitutionalism, we find that – beyond being applied in a sometimes contradictory, sometimes redundant manner – the expression functions as a veil of legitimacy for policy initiatives that are not necessarily in tune with the ideals or the essence that distinguish the constitutionalist movement. Ultimately, these uses might function as a mere rhetorical device that legitimates normative systems whose operation and effects deviate vastly from the values that inform liberal constitutional systems. Thus, we argue that digital constitutionalism is ultimately (i) a term of low epistemic value and (ii) one that can often be instrumentalised to legitimise the concentration of private power.

12 Jose van Dijck, Thomas Poell, and Martijn de Waal, *The Platform Society: Public Values in a Connective World* (Oxford: Oxford University Press, 2018), 2, https://doi.org/10.1093/oso/9780190889760.001.0001.

13 Nicolas Suzor, "Digital Constitutionalism: Using the Rule of Law to Evaluate the Legitimacy of Governance by Platforms," *Social Media + Society* 4, no. 3 (July 2018), https://doi.org/10.1177/2056305118787812.

14 Julia Pohle, "Digitale Souveränität," in *Handbuch Digitalisierung in Staat und Verwaltung*, ed. Tanja Klenk, Frank Nullmeier, and Göttrik Wewer (Wiesbaden: Springer VS, 2020), 241–53, https://doi.org/10.1007/978-3-658-23669-4_21-1.

15 Celeste, "Digital Constitutionalism.".

The first argument accrues from conceptual inconsistency. Digital constitutionalism is used as a label for several approaches to the protection of fundamental rights on digital platforms, which entails various theoretical and empirical implications. We have identified at least three different approaches to the term. The first one is descriptive: "a constellation of initiatives that have sought to articulate a set of political rights, governance norms, and limitations on the exercise of power on the Internet"[16]. This set of normative instruments is varied and includes those of public, private, or hybrid origin. They mostly aim to consolidate principles of public interest applicable to the digital realm and repackage these as a constitution: from charters that express agreements between non-profit associations or other sectors to official statements by private companies or hybrid institutions, guidelines, terms of service, and even legislative acts (for which the Brazilian Internet Civil Rights Framework is a paradigmatic example). In other words, these approaches are concerned with imparting "constitutional elements"[17] to the content of regulatory norms aimed at the digital environment. Encompassing movements that go beyond the state's official actions, this current of thought amounts to a bolder attempt than what traditional constitutionalism would pursue[18]. Criticisms of this form of digital constitutionalism have revolved around its rhetorical use, calling it a possible marketing strategy[19] due to the lack of binding force that potential "Internet Bills of Rights" impose on digital companies[20]. In other words, the symbolic value exceeds its tangible effectiveness by far.

16 Lex Gill, Dennis Redeker, and Urs Gasser, "Towards Digital Constitutionalism? Mapping Attempts to Craft an Internet Bill of Rights," *Berkman Center Research Publication* 2015, no. 15 (November 9, 2015): 2, https://doi.org/10.2139/ssrn.2687120.

17 Anne Peters, "Compensatory Constitutionalism: The Function and Potential of Fundamental International Norms and Structures," *Leiden Journal of International Law* 19, no. 3 (October 2006): 582, https://doi.org/10.1017/S0922156506003487.

18 Luiz Fernando Marrey Moncau and Diego Werneck Arguelhes, "The Marco Civil Da Internet and Digital Constitutionalism," in *Oxford Handbook of Online Intermediary Liability*, ed. Giancarlo Frosio (Oxford University Press, 2020), 189–213, https://doi.org/10.1093/oxfordhb/9780198837138.013.10.

19 Edoardo Celeste, "Terms of Service and Bills of Rights: New Mechanisms of Constitutionalisation in the Social Media Environment?," *International Review of Law, Computers & Technology* 33, no. 2 (May 4, 2019): 124, https://doi.org/10.1080/13600869.2018.1475898.

20 Kinfe Micheal Yilma, "Digital Privacy and Virtues of Multilateral Digital Constitutionalism—Preliminary Thoughts," *International Journal of Law and Information Technology* 25, no. 2 (2017): 115–38, https://doi.org/10.1093/ijlit/eax001.

A second group of theories addresses digital constitutionalism as the rearrangement of constitutional protections in the wake of techno-social shifts related to digitalisation processes. It encompasses processes of and calls for improvement in the protection of rights threatened by the structures and practices that define digital environments. The transformations and challenges brought by technology would justify new rights and the extension of constitutional protection in the face of a new paradigm. It is the case, for instance, of understanding a constitutional right to data protection as an imperative of privacy protections in the current technological paradigm (Mendes and Oliveira 2020, 3); or even of a possible "right to encryption"[21]. It is worth noting that these versions of digital constitutionalism do not contradict classical views of constitutionalism, which showcases its dynamic reality. In a way, they acknowledge a demand for expansion of constitutional protections by adding a new topic and normative content to the traditional constitutionalist agenda, similar to the way other historical phenomena have led to the emergence of social constitutionalism, economic constitutionalism, and environmental constitutionalism.

In the third group are the theories that address digital constitutionalism as a theoretical framework for both state and non-state means of potentially enforcing constitutional rights in digital environments. Between the ineffectiveness of existing regulatory frameworks to mitigate the concentration of power of digital platforms and the absence of legal provisions aimed at innovative practices, digital platforms are assumed to have developed with no concern for legal and social responsibilities about the constitution of virtual spaces and how the exercise of power may be limited inside them[22]. In this sense, the label of digital constitutionalism encompasses a variety of mechanisms aiming to transfer the values of liberal constitutionalism to relations in the digital world. Ultimately, digital constitutionalism is used as a lens to explain what actually regulatory measures are initiated by different agents. In this realm, we find the digital constitutionalism framework referred to in terms of "the principles of the rule of law"[23] and applied to recent European regulatory trends[24] or even to self-regulatory institutions,

21 Miriam Wimmer and Thiago Guimarães Moraes, "Quantum Computing, Digital Constitutionalism, and the Right to Encryption: Perspectives from Brazil," *Digital Society* 1, no. 2 (September 2022): 12, https://doi.org/10.1007/s44206-022-00012-4.

22 Suzor, "Digital Constitutionalism," 2.

23 Suzor, 2.

24 Floridi, "The European Legislation on AI"; De Gregorio, *Digital Constitutionalism in Europe*.

of which the Oversight Board would be an example. The inconsistencies in these uses of the expression will be further approached in our analysis of the latter and of the European DSA.

It may be argued that the above-mentioned theoretical approaches all share the same concern about digital platforms' compliance with the values and purposes of constitutional protections. However, their implications are quite distinct. Each one is relevant to a specific type of (public or private) agent and thus inspires different sets of democratic legitimacy criteria. They create two groups of problems, which are intertwined and overlapping: (i) the discussion concerning the explanatory and normative value of expanding the constitutional concept to include legal forms that differ from those shaped by modern political theory and (ii) the risks and impacts entailed by such a conceptual expansion and by recent uses of digital constitutionalism as a heading.

This leads to our second argument: in the face of conceptual inconsistencies and detachment from constitutionalism's substantive load, digital constitutionalism can serve to endorse, rather than mitigate, concentration of power in the digital sphere. There is a conversation to be had on whether the symbolic credentials of modern constitutionalism can be appropriated to describe and analyse political and social phenomena that take place outside the context of nation-states. Here, we return to the criticism of digital constitutionalism's theoretical matrix, as this discussion already takes place within constitutional pluralism, global constitutionalism, and societal constitutionalism. Let us take, for instance, critical approaches to constitutional pluralism in the context of the European Union. From a perspective grounded in modern tradition, non-state agents are structurally unfit for constitutionalisation, because they are devoid of the essential elements that would enable them to operate constitutionally, both from a functional and a symbolic point of view. In this sense, Martin Loughlin argues that "constitutional pluralism is an oxymoron"[25], because the idea of constitutionalism itself assumes a single system that emanates authority and organises power in a society. In the case of societal constitutionalism, the meaning of "constitution" is expanded in an inordinate way to encompass the "rationality of global systems that are quite independent of democracy for their reproduction"[26]. Furthermore, invoking constitutionalism outside the state

25 Martin Loughlin, "Constitutional Pluralism: An Oxymoron?," *Global Constitutionalism* 3, no. 1 (March 2014): 23, https://doi.org/10.1017/S2045381713000166.

26 Marcelo Neves, *Transconstitucionalismo* (Sao Paulo: WMF Martins Fontes, 2009), 3.

also entails a debate on the deficit of democratic legitimacy, which has already been acknowledged as the Achilles' heel of transnational regimes[27]. In this sense, new models being proposed would be devoid of foundational elements inseparable from the constitutionalist ideal, manifested in the dichotomy of constituent power versus constituted powers.

The multiple applications of digital constitutionalism can undermine the idea of constitutionalism itself, especially when they are conflated to encompass industry regulation and self-regulation. Moreover, the current definitions contain conflicting ideas. However, even if the founding principles of those initiatives were substantively the same, their lack of democratic legitimacy would still contradict the very notion of constitutionalism. This is because the balance of powers embedded in those arrangements would remain asymmetric, forged by private agents operating pervasive infrastructures and unilaterally imposing rules that apply to billions of users.

It is not a matter, then, of calling for a semantic purism or ignoring the existence of new phenomena that traditional concepts cannot accurately describe. The problem is to show what the terminology hides and what it reveals. In attempting to minimise the concentration of private power in digital spaces, most uses of the term "digital constitutionalism" ultimately function as theories that place a cloak of legitimacy over asymmetric power dynamics. Except for those usages that simply indicate the fact that constitutional law must now deal with the topic, both the subsystems of principles that operate outside the state and the regulatory mechanisms currently associated with digital constitutionalism can potentially produce effects that run counter to their promise, namely preventing the concentration of power. Thus, they subvert the original goals of constitutionalism because they conceive of the "constitution" as a mere institutionalisation of the given order of things, validating the activity of actors that already have effective power with no democratic participation. This is quite different from the goals of democratic freedom: to reshape power correlations and found new social and political orders that are at the core of the normative sense of constitutions.

27 Gunther Teubner, "Quod Omnes Tangit: Transnational Constitutions Without Democracy?," *Journal of Law and Society* 45, no. 1 (July 2018): 7, https://doi.org/10.1111/jols.12102.

C. Digital constitutionalism and online speech governance

Theoretical debates and policy initiatives aimed at remedying the democratic deficit in online freedom of expression make for a fine example of the inconsistencies described above. In this section, we analyse two policy initiatives aimed at improving legitimacy standards in online speech governance related to the framework of digital constitutionalism: the Meta (Facebook) Oversight Board, a private sector self-regulatory initiative implemented by the company Meta, and the DSA, a supranational regulation enacted by the European Parliament and in force since 2022. Our goal is to show how conceptual inconsistencies – i.e., a misunderstanding of constitutionalism's defining traits; or how the label is used to refer to institutional initiatives that entail different power imbalances – can ultimately lead to a legitimisation, rather than mitigation, of platform power.

I. The Meta Oversight Board

The Meta Oversight Board (MOB) was developed and implemented by the company Facebook in 2020, before becoming Meta in 2021. It was created as a self-regulatory body meant to serve as an appeals instance to (its headliner platform) Facebook's content moderation practices (a concept that we will expand on shortly). The MOB took the shape of a board of experts responsible for enforcing Facebook's Community Standards when revising its decisions on what sort of user-generated content should be removed or not. The board's declared goal is to protect "free expression by making principled, independent decisions about important pieces of content and by issuing policy advisory opinions on Facebook's content policies"[28]. The board has since been financed through a trust fund set up by Meta and designed as an independent entity as regards management.

Constitutional metaphors have accompanied the Oversight Board since its early development. Before its institutional model was officially announced, in a 2018 interview, Meta's CEO Mark Zuckerberg was questioned about democratic accountability of Facebook's content moderation decisions, to which he replied, envisioning

28 Facebook, "Oversight Board Charter," September 2019, 5, https://about.fb.com/wp-content/uploads/2019/09/oversight_board_charter.pdf.

> some sort of structure, almost *like a Supreme Court*, that is made up of independent folks who don't work for Facebook, who ultimately make the final judgment call on what should be acceptable speech in a community that reflects the social norms and values of people all around the world. [29]

Despite there already being sound academic criticism of the use of this metaphor[30], the association of the Oversight Board with constitutional phenomena pervaded the narrative around it. Besides the frequent reference to "Facebook's Supreme Court"[31], the Oversight Board has also been linked to the digital constitutionalism framework as part of an "expansive quest for reversing the complicity of the law in the development of an informational capitalism"[32]. However, the many references to digital constitutionalism have not necessarily reversed this complicity. Quite to the contrary, the misappropriation of the symbolic value of constitutionalism by initiatives managed and operated by the digital private platforms themselves may have worked towards legitimising such structures, despite of how effectively they might have contributed to building a public-values sphere of debate. In the next paragraphs, we will discuss the (im)pertinence of associating the MOB with constitutionalism, considering: (i) its limited potential to mitigate Facebook's power over defining the scope of freedom of expression, and (ii) its focus on improving internal procedural legitimacy, while overlooking democratic participation and the board's operations' actual results.

---

29 Ezra Klein, "Mark Zuckerberg on Facebook's Hardest Year, and What Comes Next," *Vox* (blog), April 2, 2018, https://www.vox.com/2018/4/2/17185052/mark-zuckerberg-facebook-interview-fake-news-bots-cambridge our emphasis.

30 Josh Cowls et al., "Constitutional Metaphors: Facebook's 'Supreme Court' and the Legitimation of Platform Governance," *New Media & Society*, April 5, 2022, https://doi.org/10.1177/14614448221085559; Anna Sophia Tiedeke and Martin Fertmann, "A Love Triangle? Mapping Interactions between International Human Rights Institutions, Meta, and Its Oversight Board," *European Journal of International Law*, Forthcoming.

31 Lorenzo Gradoni, "Constitutional Review via Facebook's Oversight Board: How Platform Governance Had Its Marbury v Madison," *Verfassungsblog* (blog), February 10, 2021, https://verfassungsblog.de/fob-marbury-v-madison/; Golia, "Beyond Oversight.".

32 Matija Miloš and Toni Pelić, "Constitutional Reasoning There and Back Again: The Facebook Oversight Board as a Source of Transnational Constitutional Advice," in *European Yearbook of Constitutional Law 2021*, ed. Jurgen De Poorter et al., vol. 3, European Yearbook of Constitutional Law (The Hague: Springer & T.M.C. Asser Press, 2022), 198, https://doi.org/10.1007/978-94-6265-535-5_9.

First, we argue that the MOB has not had much potential to mitigate Facebook's power over online speech, notably due to its self-regulatory nature and its limited scope. Implemented over a decade after the social network Facebook was launched, the MOB could be interpreted as privately-led response to years of criticism, notably from civil society and academia, of Facebook's, and other digital platforms', "unchecked system" for users' speech governance[33]. This "unchecked system" is epitomised by the practice of content moderation, itself an inherently vague notion. Minimalist approaches argue that content moderation happens merely when platforms review user-generated content and decide whether to keep it up or take it down[34]. This is in line with the board's competences since it is meant to review Facebook's decisions to remove or keep users' publications online upon flagging. This specific decision-making process is, nevertheless, far from representing the widespread influence that content moderation exerts on the broader realm of online freedom of expression, or indeed on different layers of social interaction both on- and offline. Timeline algorithmic curation, automated tools, shadow banning, and labour practices (which affect human content moderators) are only some of the different ways through which digital platforms' standards for freedom of expression are enforced in a broader sense. Thus, Gillespie et al. define content moderation as

> the detection of, assessment of, and interventions taken on content or behaviour deemed unacceptable by platforms or other information intermediaries, including the rules they impose, the human labour and technologies required, and the institutional mechanisms of adjudication, enforcement, and appeal that support it.[35]

While these broader aspects of content moderation remain mostly outside the board's scope, during its tenure, the MOB has also shown little potential to act as a check on Facebook's actions even within its (already restricted)

33 Kate Klonick, "The Facebook Oversight Board: Creating an Independent Institution to Adjudicate Online Free Expression," *The Yale Law Journal* 129, no. 8 (2020): 2476; Evelyn Douek, "Facebook's 'Oversight Board': Move Fast with Stable Infrastructure and Humility," *North Carolina Journal of Law and Technology* 1, no. 21 (2019): 46.

34 Klonick, "The Facebook Oversight Board: Creating an Independent Institution to Adjudicate Online Free Expression," 2427.

35 Tarleton Gillespie et al., "Expanding the Debate about Content Moderation: Scholarly Research Agendas for the Coming Policy Debates," *Internet Policy Review* 9, no. 4 (October 21, 2020), https://doi.org/10.14763/2020.4.1512.

competences. In previous work co-authored with Haggart, Iglesias Keller[36] noted obstacles to the board's ability to contribute to a public-value-based online content governance, including its narrow scope. The MOB is meant to only decide on *appeals* regarding content that had been removed for infringing Facebook's Community Standards. This means removals based on illegality would not be up for appeal and do not fall within the MOB competencies.

One could argue that this association of the MOB with constitutional phenomena ought to be justified by its role as a second instance adjudicator whose operations are guided by the principles of the rule of law – in particular, the procedural ones, like transparency and due process. Indeed, in terms of its legitimacy claims, the board clearly does invoke and emphasise procedural legitimacy – understood here as the sphere of legitimacy that refers to the quality of governance process, i.e., transparency, efficacy, accountability, and inclusiveness as well as openness to civil society participation[37]. This shows, for instance, in its promotion of procedural and

36 "Democratic Legitimacy in Global Platform Governance," 7.

37 This approach to procedural legitimacy reflects Vivian Schmidt's concept of "throughput legitimacy", which is "process-oriented, and based on the interactions – institutional and constructive – of all actors engaged in (…) governance" (Schmidt 2013, 5). It "demands institutional and constructive governance processes that work with efficacy, accountability, transparency, inclusiveness and openness" Vivien A. Schmidt, "Democracy and Legitimacy in the European Union Revisited: Input, Output and 'Throughput,'" *Political Studies* 61, no. 1 (March 2013): 7–8, https://doi.org/10.1111/j.1467-9248.2012.00962.x. Schmidt developed a democratic legitimacy theory for the European Union by building on "Fritz Scharpf's (1970) typology of input and output legitimacy. Input legitimacy refers to the 'EU's responsiveness to citizen concerns as a result of participation by the people,' while output legitimacy refers to the 'effectiveness of the EU's policy outcomes for the people', input legitimacy refers to the 'EU's responsiveness to citizen concerns as a result of participation by the people" Schmidt, 2. To this, Schmidt adds a third category, 'throughput legitimacy,' which highlights the quality of the governance process and 'is judged in terms of the efficacy, accountability and transparency of the EU's governance processes along with their inclusiveness and openness to consultation with the people' Schmidt, 2." Haggart and Iglesias Keller, "Democratic Legitimacy in Global Platform Governance," 5.

governance transparency[38][39] and in concerns regarding due process[40]. At the same time, the board's design understates other legitimacy standards, like facilitating control of content moderation by democratic oversight or implementing significant participation instruments in Facebook's decision-making and norm-setting processes[41].

In this sense, even the asserted procedural legitimacy is non-existent with respect to its origin and is limited in scope. With respect to origin, the moderation rules, procedures, and case selection criteria are not designed to allow for meaningful participation by those affected by Meta's content moderation rules. Thus, from a procedural standpoint, the chosen model reinforces the democratic deficit already inherent in the private regulatory system. At best, the architecture of the board serves to give the outcome greater internal legitimacy, qualifying it as a self-regulatory decision that has gone through a special procedure. These features do not correspond to the democratic constitutional architecture that would justify describing them in terms of "court" and "constitution".

Another element that distinguishes democratic constitutional processes from private self-regulation is an essential element of constitutionalism: the political concept of self-constraint. It is entirely inapplicable to the MOB. The idea of self-constraint, understood as the commitment of a political community to entrench certain decisions and limit future actions, presupposes a collective commitment involving both the citizens affected by the normative commands and those who circumstantially exercise the

38 Klonick, "The Facebook Oversight Board: Creating an Independent Institution to Adjudicate Online Free Expression," 2479–80.

39 Including publication of the applicable rules; notification of infringement and review procedure; explanation of what this process entails; and notification of the ultimate decision Klonick, 2479–80. Also, the by-laws commit the board to making all case decisions publicly available, archiving them in a database and publishing annual reports with metrics on the cases reviewed, cases submissions by region, and timelines of decisions Haggart and Iglesias Keller, "Democratic Legitimacy in Global Platform Governance," 8.

40 The Meta Oversight Board "can make a strong claim for legitimacy with respect to due process. Due process is in fact perceived as one of the Oversight Board's defining characteristics" Douek, "Facebook's 'Oversight Board': Move Fast with Stable Infrastructure and Humility," 6. The central goal of the board is to grant Facebook users the possibility of having their content controversies examined by a selection of experts from different world regions who are allegedly independent from Facebook Haggart and Iglesias Keller, "Democratic Legitimacy in Global Platform Governance," 8.

41 Haggart and Iglesias Keller, "Democratic Legitimacy in Global Platform Governance," 8–9.

powers to enforce those commands. It therefore does not apply to private self-regulation initiatives, which merely involve a promise to self-limit by those who hold de facto power. By its very origin and nature, it does not entail alternation in its ownership and exercise. At this stage, it is important to highlight that, even though the board is structured to be institutionally independent from the Meta corporation, funding does come from Facebook's owner[42] and ultimately depends on the company's willingness to maintain its operation.

As such, the board's design shows weak compliance with three defining features of constitutional legal structures: (i) stability, (ii) mechanisms of separation of powers and checks and balances, and (iii) mechanisms for enforced compliance with decisions. Regarding stability, the board's normative structure is precarious due to its private nature, ultimately dependent on Meta's financial and institutional support. There is always the possibility that these structures will be unilaterally and suddenly dismantled. For this very reason, the idea of separation of powers, essential to the concepts of rule of law and constitutionalism, simply does not apply to private structures writ large. If the corporation's leaders have the mechanisms to reverse the division of tasks it has established, there is no way to see in such a review board a genuine mechanism of checks and balances.

II. The European Digital Services Act (DSA)

The European Digital Services Act is a European regulation that provides a comprehensive regulatory framework for online content governance, by creating a "wide-ranging set of standards for how technology companies operating user-generated content platforms in Europe would need to report upon, audit, and design their content moderation frameworks"[43]. As a continuation of European digital policy initiatives – notably, the 2000/31/EC E-Commerce Directive –, the DSA represents a paradigmatic shift towards binding rules directed at many of the practices through which digital platforms exert influence on online content, and thus, on freedom of speech and access to information. It adds to the liability rule provided in the E-Commerce Directive, according to which digital platforms are liable

42 Facebook, "Oversight Board Charter" section 3.

43 Robert Gorwa, *The Politics of Platform Regulation: Trust and Safety, Content Moderation, and the State* (Oxford: Oxford University Press, Forthcoming).

for infringing user-generated content once they are aware of its existence. Through a broader set of mechanisms, the DSA aims to hold platforms accountable for content moderation beyond the removal or maintenance of infringing content. Concerns with remedying information asymmetry, as well as for due process standards, cut through many of the different obligations provided in the DSA[44]. Suzor has already referred to this simply as "certain procedural safeguards" whose abidance by digital platforms would guarantee that their governance is "legitimate according to the rule of law"[45]. Among the mechanisms implemented by the DSA are a series of transparency obligations regarding user-generated content visibility; the implementation of complaints processing and abidance by due process-like standards; and the prohibition of misleading and opaque decision making, such as shadow banning and dark-patterns.

The DSA is presented in the literature as a piece of "European constitutionalism", more specifically, a form of digital constitutionalism that serves as a "reaction to new digital powers" after a period in which the EU had neglected and forgot "the role of constitutionalism, and then constitutional law, in protecting fundamental rights and limiting the rise and consolidation of unaccountable powers abusing constitutional values"[46]. In this vein, digital constitutionalism has gained momentum as an explanatory label of not only the DSA but a whole group of recent European digital policy initiatives. In what can be interpreted as an image of "the EU's digital constitution"[47], Luciano Floridi speaks of a "hexagram of EU digital constitutionalism", where the DSA figures along with other European regulatory

44 See, for instance: digital platforms obligations to designate points of contact with which users may communicate directly, while also making public the information necessary for users to identify and communicate with such points of contact (Article 12); the obligation to include all information on content moderation policy and procedures in their Terms of Service "in clear, plain, intelligible, user-friendly and unambiguous language" (Article 14); to make clear, easily comprehensible reports publicly available in a machine-readable format and in an easily accessible manner about content moderation that they engaged in the period of one year (Article 15); material and formal requirements for the implementation of mechanisms through which users can report on supposedly illegal content (Article 16); and to provide justification for content removal (Article 17).

45 "Digital Constitutionalism," 2.

46 De Gregorio, *Digital Constitutionalism in Europe*, 3.

47 Alexandru Circiumaro, "EU Digital Constitutionalism, Digital Sovereignty and the Artificial Intelligence Act - A Network Perspective," *European Law Blog* (blog), December 23, 2021, https://europeanlawblog.eu/2021/12/23/eu-digital-constitutionalism-digital-sovereignty-and-the-artificial-intelligence-act-a-network-perspective/.

initiatives dedicated to conforming digital technologies to the European legal framework, i.e. the General Data Protection Regulation (GDPR), the Digital Markets Act, the Data Governance Act, the Artificial Intelligence Act, and the bill for regulating the European Health Data Space[48].

The DSA currently stands as an *avant-garde* initiative, a regulatory framework that attempts to reign in digital platforms' opaque and steamroller business practices, after years of debate (and why not, public outrage) that occupied governments around the globe[49]. It promotes regulatory innovations with potential to enhance our understanding and mitigation of the mechanisms through which these platforms accumulate and exercise power over data and public communications (like the systemic risk assessments provided by Article 26). However, applying the constitutionalism tag to this framework without further reflection might overlook conceptual and normative inconsistencies, as well as potential shortcomings of the regulation's results.

First, we highlight that the concepts of the rule of law and constitutionalism should not be understood as equivalent and interchangeable. The idea of the rule of law is broader, more controversial, and more indeterminate than that of constitutionalism. There is no single definition of the "rule of law", let alone agreement on the formal, procedural, and substantive principles it entails. In a formal sense, the rule of law refers to the formal aspects of governing according to law[50]. The principles that this notion requires concern the generality, clarity, publicity, stability, and prospectivity of the law that rules a society[51]. The concept of the rule of law also includes some procedural requirements, such as the right to be heard by an independent court and the guarantee of due process[52]. In substantive terms, the concept of the rule of law involves principles of justice. From this perspective, citizens have moral rights and duties towards each other

48 "The European Legislation on AI," 220.

49 In fact, some of these governments have also attempted to improve digital platforms' accountability by approving further liability regulations that speak to the DSA's principles in different extent. See, for instance, the German NetzDG.

50 Jeremy Waldron, "The Rule of Law and the Importance of Procedure," in *Getting to the Rule of Law*, ed. James Fleming, vol. 50, Yearbook of the American Society for Political and Legal Philosophy (New York: New York University Press, 2011), 3–31, https://www.jstor.org/stable/24220105.

51 Lon Luvois Fuller, *The Morality of Law* (New Haven: Yale University Press, 1964).

52 Waldron, "The Rule of Law and the Importance of Procedure."

and political rights against the state as a whole[53]. While the formal, procedural, and substantive contents of the rule of law are usually secured by a constitution, the idea behind it is not the same as that of constitutionalism. The notions of the rule of law and constitutionalism are closely linked, even if they do not encompass the same structures or refer to the same processes. As a political ideology and movement, constitutionalism requires democracy, checks and balances, and, in its late model that has spread around the world, constitutional supremacy and judicial control of laws. For this reason, constitutionalism is not the same as applying the principles of the rule of law to regulatory systems. In this sense, securing abidance by the principles of the rule of law is not enough to mitigate these private agents' concentration of power. In fact, binding digital platforms to such a framework of principles implies, to a certain extent, a recognition and validation of their influence over online speech governance. When doing so without challenging the technical and institutional mechanisms that enable this influence, "regulatory attempts to introduce public values into the structure of powerful private agents end up formalising and reinforcing their role as 'rulers' of online discourse, and may, as such, reinforce their political power"[54].

The question of what would, indeed, challenge this concentration of power, is one that cuts across global debates on how to regulate digital platforms. The DSA represents a milestone in the European debate (and some will argue, globally), as the first piece of legislation directed at digital platforms that transcends a legal paradigm where platforms were seen as mere intermediaries of communication, to recognise their influence in content, speech, and behaviour while attempting to hold them accountable for such influence. As other policy proposals and initiatives do – e.g. in Brazil, India, North America –, the DSA pursues a policy agenda that is reactive to contemporary socio-political phenomena expressed and supported by digital technologies. This includes the spread of hate speech and terrorist content, threats to child safety, and the expansion of digital disinformation practices around elections. While different political contexts hold their specificities, there is an overall feeling that recent regulatory trends tagged as digital constitutionalism are meant to fill a decades-long regulatory void

53 Ronald Dworkin, *A Matter of Principle* (Cambridge, Mass: Harvard Univ. Press, 1985).

54 Natali Helberger, "The Political Power of Platforms: How Current Attempts to Regulate Misinformation Amplify Opinion Power," *Digital Journalism* 8, no. 6 (July 2, 2020): 848, https://doi.org/10.1080/21670811.2020.1773888.

that allowed big tech companies to become extremely powerful economic and political actors. In this context, the use of constitutional metaphors also serves as a rhetorical appeal to constitutional law in a field where administrative and regulatory law have failed us. As we intended to show in this chapter, however, as appealing as it may sound, this semantic resource does not come without a price.

D. Final remarks

This chapter presented a critique on the use of "digital constitutionalism" theoretical frameworks to approach recent policy initiatives aimed at improving democratic legitimacy standards in online content governance. Our argument is centred on the inadequacy of transposing the vocabulary of constitutionalism into the realm of (public and private) regulatory initiatives that do not necessarily share the features that define constitutionalism as a theory and a political movement. In fact, as we intended to show, the use of the "digital constitutionalism" label can, in some cases, imprint legitimacy where institutional design heads, in fact, towards concentration of private power.

The AI Act:
A realpolitik compromise and the need to look forward

Alessandro Mantelero

Abstract: First-generation technology regulation typically attempts to strike the right balance between rights protection and innovation. This tension is evident in the EU AI Act and in the way the risk management, the core element of any technology regulation, is framed. This chapter outlines the rationale behind the compromise solution adopted by the EU legislator to reconcile the protection of fundamental rights with the expected benefits of AI. It also discusses the decision to depart from a more holistic approach centred on the societal acceptability of AI, in terms of alignment with the values of the communities in which AI solutions are to be implemented. The chapter highlights the weakness of a primarily risk-based approach that does not place at the heart of the regulation the definition of key principles specifically tailored to the AI context and aimed at underpinning its development. Against this background, the role of fundamental rights in guiding the development of a human-centred AI in line with EU values is crucial. However, the implementation of the fundamental rights impact assessment in the AI Act is still underway. A more coherent framework is needed, combining the different assessments outlined in the AI Act, as well as a better definition of the scope and relevant criteria for the assessment. Finally, an appropriate model should be developed and made available AI providers and deployers, adopting a lean assessment design and combining expert-based evaluation and stakeholder/rightsholder participation.

A. Introduction

After a long debate on the impact of Artificial Intelligence (AI) on society, the European Union has decided to adopt the first legal instrument specif-

ically focused on this technology,[1] whose recent development, despite its many benefits, has raised several concerns in a variety of areas.

The EU was the first mover in this field within the global geo-political regulatory scenario, but this is not the only initiative to establish some rules for AI development and use. From Brazil[2] to the US,[3] many other lawmakers are outlining specific provisions for AI, and a number of charters providing key principles for AI development have been adopted by a variety of entities in recent years.[4] This is the typical scenario for a first generation of new technology regulation, as was the case with data protection in the late 1960s and early 1970s.

As discussed in the next section, a common problem for many first-generation technology regulations is finding the right balance between rights protection and innovation. This tension is also evident in the EU AI Act

1 More details on the AI Act and its approval process can be found here (all online resources referred to in the footnotes to this chapter have been consulted prior to 1 September 2023):
https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence?&at_campaign=20226-Digital&at_medium=Google_Ads&at_platform=Search&at_creation=RSA&at_goal=TR_G&at_advertiser=Webcomm&at_audience=artificial%20intelligence%20act&at_topic=Artificial_intelligence_Act&at_location=IT&gclid=EAIaIQobChMI9Z__pIqJgQMVsZ1oCR2jvw1ZEAAYASAAEgL6mfD_BwE.

2 See here the progress of the proposal: https://www25.senado.leg.br/web/atividade/materias/-/materia/157233?_gl=1*cqpafr*_ga*NzcyNDkwNDc3LjE2NTc2MzI1OTk.*_ga_CW3ZH25XMK*MTY4NDI0NDk5Mi4xMS4xLjE2ODQyNDU0NTcuMC4wLjA.#publicacoes. See also Belli, Luca, Yasmin Curzi, e Walter B. Gaspar. «AI regulation in Brazil: Advancements, flows, and need to learn from the data protection experience». *Computer Law & Security Review* 48 (1 April 2023): 105767. https://doi.org/10.1016/j.clsr.2022.105767.

3 For an overview of the different US regulatory initiatives, see also https://www.ravitdotan.com/us-ai-regulation.

4 For a more detailed analysis see Mantelero, Alessandro. Beyond Data: Human Rights, Ethical and Social Impact Assessment in AI. Vol. 36. Information Technology and Law Series. The Hague: T.M.C. Asser Press, 2022. https://doi.org/10.1007/978-94-6265-531-7 (Open Access), 93-101. See also Jobin A, Ienca M, Vayena E (2019) The Global Landscape of AI Ethics Guidelines. 1 Nature Machine Intelligence 389; Hagendorff T (2020) The Ethics of AI Ethics: An Evaluation of Guidelines. 30 Minds and Machines 99; Ienca M, Vayena E (2020) AI Ethics Guidelines: European and Global Perspectives. In: Council of Europe. Towards regulation of AI systems. Global perspectives on the development of a legal framework on Artificial Intelligence systems based on the Council of Europe's standards on
human rights, democracy and the rule of law. Council of Europe, Strasbourg, pp 38–60.

and in the way the core element of all technology regulation, namely risk management, is framed. In addition, despite a significant debate on the societal impact of AI – mainly from the point of view of AI ethics[5] – the AI Act is not (yet?) part of a holistic approach that combines legal and non-legal issues revolving around AI.[6]

Finally, the focus on the risk-based approach has paid less attention to the definition of key principles specifically tailored to the AI context, which are neither the core of the AI Act[7] nor adequately elaborated in the other regulatory initiatives and in the many guidelines on AI. As noted in the analysis of the proposed principles carried out in the fourth section, these principles are often vague, overlap with similar principles set out in in other regulations, without clarifying their relationship with them, and in any case require specific guidelines for their consistent and concrete implementation in AI design and development.

In the absence of a sound set of guiding principles underpinning the EU way to AI and with a regulatory focus primarily centred on risk management, the last section emphasises the key role played by human rights (fundamental rights within the EU context) in the development of a truly human-centred AI that embodies EU values. Given the structure of the AI Act and the pivotal role of the risk-based approach, the impact assessment on fundamental rights becomes crucial in order not to restrict this regulation to a mere safety and security perspective.

The issues briefly listed here and discussed in more detail in the following sections urge law-makers to make further efforts to define the core elements of a methodology for assessing the impact of AI on fundamental rights and to support its implementation, avoiding simplistic solutions

5 See fn. 4. See also European Data Protection Supervisor (2015b) Opinion 4/2015b. Towards a new digital ethics:
Data, dignity and technology, https://edps.europa.eu/sites/edp/files/publication/15-09-11_data_ethics_en.pdf; European Data Protection Supervisor, Ethics Advisory Group (2018) Towards a digital ethics.
https://edps.europa.eu/sites/edp/files/publication/18-01-25_eag_report_en.pdf; Independent High-Level Expert Group on Artificial Intelligence set up by the European Commission (2019) Ethics Guidelines for Trustworthy AI. https://ec.europa.eu/futurium/en/ai-alliance-consultation.1.html.

6 See below Section C.

7 See European Parliament, P9_TA(2023)0236, Artificial Intelligence Act. Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD))1, Article 4a.

based on delegation to standard-setting bodies that do not have the appropriate profile to deal with fundamental rights.

B. The AI Act: two reasons for a compromise solution

In the early stages of the Industrial Revolution, explosions and fires were common due to the limited ability to control steam power at the time. Similarly, the large-scale production of goods resulted in a number of defective products that harmed their users. In both these scenarios, the most effective response of the legal system in order to protect the injured parties would have been to introduce a strict liability regime to minimise the side effects of innovation and industrial development. However, it was only when these technologies reached a higher level of maturity and it became easier and cheaper to put in place safety measures to prevent their side effects that fault-based models were replaced by stricter forms of liability.

Decades later, at the dawn of the information society era, both US and EU legislators decided that it was better to limit the liability of Internet service providers, despite the fact that online BBSs and webpages hosted illegal or defamatory content. The rise of dominant platforms and their better position (and wider availability of resources) in content management later changed the initial scenario and recently led lawmakers to set specific obligations focused on competition, consumer protection and fundamental rights.[8]

Other examples of the relationship between technological development and regulation could be added. However, the pattern remains the same: the early stages of implementation of innovations require a kind of 'tolerance' from the legal system, accepting a certain degree of side effects on individuals and society in return for future benefits from investment in new technologies.

In addition, limiting the legal requirements for innovative technologies facilitates the entry of more players into the new industry and increases the investment of major players. Both of these effects contribute to a more

8 See Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) and Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act).

mature technology and, ultimately, to an easier reduction of side effects, which makes it possible to adopt stricter liability rules.

It is only by taking into account this logic, based on 'the gift of the evil devil',[9] that it is possible to understand the main reason for the regulatory approach adopted by the EU legislator in addressing the issues raised by AI. The minimalist approach to the protection of individual rights and society in the AI Act – as shown by its focus on only the most dangerous scenarios, i.e. prohibited and high-risk applications – clearly contradicts the earlier debate on the ethics of AI (see Section C), the Council of Europe's early work on the core role of human rights in AI development, and the growing interest in human rights in business regulation. However, it represents a compromise solution in dealing with the risks of a promising new industry sector.

Setting some redlines and introducing a general reference to the impact on human rights is rather far from the idea of a human-centred AI, and departs from the debate of recent years on the empowerment of citizens in the digital society. In the same way, a regulation based on the traditional industrial risk approach (conformity assessment, standards, market surveillance) is rather far from a principles-based and risk-focused law centred on human rights, such as the GDPR.

Looking at the GDPR, a long-celebrated EU success in digital regulation due to its global impact,[10] and comparing it to the AI Act, the different approaches become clear. While the GDPR has addressed potential personal data processing concerns by providing some principles along the line of a cautious approach to the use of personal information (e.g. purpose limitation, minimisation, storage limitation), the AI Act does not set any principles to guide AI development,[11] focusing only on risk mitigation. The emphasis on European values to be embedded in AI (although human rights are more properly universal values), which characterised the initial academic and regulatory debate, has been lost in favour of a risk-centred and mainly safety-oriented regulation.

9 See Calabresi, Guido. 1985. Ideals, Beliefs, Attitudes, and the Law: Private Law Perspectives on a Public Law Problem (Syracuse, New York: Syracuse University Press) 1985, Ch. 1.

10 See, e.g, Greenleaf, Graham, Now 157 Countries: Twelve Data Privacy Laws in 2021/22 (March 15, 2022). (2022) 176 Privacy Laws & Business International Report 1, 3-8, UNSW Law Research, Available at SSRN: https://ssrn.com/abstract=4137418.

11 But see the European Parliament's proposal in this regard below in Section D.IV below.

Nor is the risk-based approach comparable to the way in which risk has been framed over the years in data protection, i.e. the main regulatory framework of the digital society so far. While Article 35 of the GDPR takes a broad approach to risk identification and is rather demanding in risk mitigation, the AI Act is less strong in this direction. The paradigm shift is evident in the different way of addressing the key points of risk management, namely the classification of high-risk cases and the consequences of such classification.

Although both the regulations focus on high risk, the AI Act sets out a closed list of cases classified as high risk, while the GDPR leaves the obligation to assess the level of risk for each operation to the duty bearers (i.e. data controllers). The difference is significant: a closed list is less effective in identifying high-risk cases in the context of a rapidly evolving technology such as AI at this stage, as confirmed by the debate on LLMs and the 'last minute' amendments to the AI Act.[12] Moreover, Annex III of the AI Act identifies high-risk areas using rather broad descriptions that may include cases that are not high-risk.[13] This is only partly mitigated by the proposed 'reasoned notification' to the competent national supervisory authority,[14] which will result in a cumbersome process and does not preclude future litigations on the applicability of AI to specific products/services.

Looking at the legislative process and its democratic legitimacy, the Commission's power to amend this list raises some concerns about the unilateral role the Commission will play, given the direct impact of listed cases on the scope and applicability of the AI Act.

12 See European Parliament, P9_TA(2023)0236 (fn. 7), Article 28b (Obligations of the provider of a foundation model). See also Bertuzzi, Luca. «Leading EU Lawmakers Propose Obligations for General Purpose AI». www.euractiv.com, 14 March 2023. https://www.euractiv.com/section/artificial-intelligence/news/leading-eu-lawmakers-propose-obligations-for-general-purpose-ai/.

13 For example, the category of AI systems "intended to be used for the purpose of assessing students in educational and vocational training institutions" (Annex III, AI Act, Commission Proposal) may also include AI-supported examination systems that automate some assessment procedures, but without involving high risk.

14 See European Parliament, P9_TA(2023)0236 (fn. 7), Article 6 (2a) ("[providers] shall submit a reasoned notification to the national supervisory authority that they are not subject to the requirements of Title III Chapter 2 of this Regulation. […] Without prejudice to Article 65, the national supervisory authority shall review and reply to the
notification, directly or via the AI Office, within three months if they deem the AI system to be misclassified").

If we look at the consequences of this high-risk classification, they are necessarily milder in the AI Act than in the GDPR. Whereas in the later the non-negotiable protection of human rights led the EU legislator to put data processing applications entailing a high risk to individual rights off the market (Articles 35.7.d and 36.1), in the AI Act the legislator opted for an 'acceptable' risk, which means that risky applications can be used even though the level of risk remains high.

Finally, the AI Act does not provide clear criteria for a methodology to assess the impact on fundamental rights, as discussed further in Section E. In this respect, the similarity with the GDPR is only apparent. While it is true that Article 35 of the GDPR does not set out a methodology for DPIA, it is worth noting that the GDPR builds on more than four decades of data protection regulation and practice, during which several robust methodologies have been developed, starting with PIA models.[15] On the contrary, the AI Act builds on Human Rights Impact Assessment, which has only recently been developed in the business sector and does not fit properly with AI applications.[16] Nor does the idea of delegating the definition of this methodology to standards and standardisation bodies seem any more promising (see Section E).

This brief comparison between the AI Act and the GDPR shows how different the maturity of these two regulations is, as well as the different maturity of the industry they regulate. While several generations of data protection laws preceded the GDPR,[17] gradually increasing the level of protection hand in parallel with the development of more privacy-enhancing technologies, the AI Act is a first regulation at an early stage in the development of the AI sector on a large scale.

Recalling Reidenberg's six ways of shaping technology,[18] the EU cannot use the 'bully pulpit', has limited resources to fund AI innovation, and –

15 See also Wright D, De Hert P (eds) (2012) Privacy Impact Assessment. Springer, Dordrecht.

16 While traditional Human Rights Impact Assessment (HRIA) models are usually territory-based, considering the impact of business activities in a given local area and community, in the case of AI applications this link with a territorial context may be less significant. For a broader analysis of HRIA in AI see Mantelero. Beyond Data (fn. 4), Ch. 2.

17 See Mayer-Schönberger V (1997) Generational Development of Data Protection in Europe. In: Agre PE, Rotenberg M (eds) Technology and Privacy: The New Landscape. The MIT Press, Cambridge, pp 219–241.

18 Joel R. Reidenberg, 'Lex Informatica: The Formulation of Information Policy Rules Through Technology', Texas Law Review 76, no. 3 (1998): 553–84.

due to the fragmentation of its national and regional strategies – it faces some difficulties in using participation and bargaining power in procurement to shape an AI industry dominated by non-EU players. Regulation is therefore the main way in which the EU can influence the design of AI products and services provided to EU citizens and users.

However, regulating a market with weak regional champions necessarily requires a more industry-friendly approach than in the case of a more balanced market composition. For this reason, the first generation of EU regulation on AI must combine safeguarding the development of the AI industry with a minimum level of consistency with the EU's fundamental rights framework.

As was the case with the Industrial Revolution and the Internet revolution, it is not surprising that in the AI revolution the first regulatory framework only partially addresses the demand for the protection of individual and societal rights. This is why the high-level commitment to ethics and human rights of the early AI debate in Europe has more pragmatically ended up in an industry-focused regulation, centered on conformity assessment, with limited emphasis on fundamental rights.

However, as has been the case in other fields and given the rapid development of the AI industry, it is worth considering alternative paths that have now been discarded, but which may be part of the further development of the AI regulation or complement its implementation. From this perspective, the following section focuses on the role that ethics and human rights could play in a more holistic and mature AI regulation, which could represent the next horizon for an EU model with the ambition to replicate the so-called Brussels effect achieved with the GDPR.

C. The solutions left behind: an ethical and socially conscious approach, a principles-based model focused on human rights

Considering the alternative paths that the EU legislator has left open when framing the first AI regulation is not just a theoretical exercise, but a way to reflect on possible options to improve a regulation that does not fully address the main concerns about the impact of AI on society.

On the one hand, the focus on risk/conformity assessment reveals a techno-solutionist approach. Simply mitigating risks to make them acceptable is far less than creating a framework to support developers in shaping

human-centred AI that addresses the challenges AI poses to human rights, societal and ethical values.[19]

This is not only a general issue, but also an important part of the EU debate on AI regulation before the Commission set a different paradigm with the AI Act proposal. A similar path can be seen in the work of the Council of Europe, where the initial broad approach focused on ethical issues and human rights has been replaced by a more risk-focused approach.[20]

The outcome of the EDPS expert group,[21] the guidelines of the Independent High-Level Expert Group on Artificial Intelligence,[22] and the first draft of the EU Parliament on AI regulation, which refers to ethical values,[23] have clearly taken a different and more holistic view of regulating the impact of AI on society. Although current industrial policy issues have led to a different outcome in the AI Act, limiting the regulation of a technology so relevant to societal change to risk management, this does not seem entirely in line with EU values and orientation (see also Section D).

In this respect, although the AI Act does not take into account the ethical and social consequences of the use of AI, the reflections and proposals elaborated in recent years should be considered in order to complement this industry-focused regulation. This can be done by translating the reflections on the societal aspects of AI into best practices that can provide specific tools for value-oriented AI design and thus fill the gap in this first generation of AI regulation.

In 2015, facing the challenges of Big Data, IoT and cloud computing (three core components of the latest AI revolution), the EDPS considered

19 On the social and ethical component of AI systems design see also Mantelero. Beyond Data (fn. 4), Ch. 3, for further discussion and references.

20 Alessandro Mantelero and Francesca Fanucci. 2022. The International Debate on AI Regulation and Human Rights in the Prism of the Council of Europe's CAHAI: Great Ambitions. In: European Yearbook on Human Rights 2022 / Czech P., Heschl L., Lukas K., Nowak M., Oberleitner G., Cambridge, Intersentia, pp. 225-252.

21 See European Data Protection Supervisor, Ethics Advisory Group (2018) Towards a digital ethics.
https://edps.europa.eu/sites/edp/files/publication/18-01-25_eag_report_en.pdf.

22 Independent High-Level Expert Group on Artificial Intelligence set up by the European Commission (2019) Ethics Guidelines for Trustworthy AI. https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai.

23 See, e.g., European Parliament. 2020. Draft Report with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies (2020/2012(INL)). See also Matos Pinto, Inês de. «The Draft AI Act: A Success Story of Strengthening Parliament's Right of Legislative Initiative?. 22(4) ERA Forum 2021: 619–41. https://doi.org/10.1007/s12027-021-00691-5.

that "an ethical framework needs to underpin the building blocks of this digital ecosystem"[24] and set up an Ethics Advisory Group (EAG) to open the debate on the ethical dimension of data-intensive technologies. This group of experts emphasised that the challenges posed by these technologies had only been partially addressed by the law and "ethics allows this return to the spirit of the law and offers other insights for conducting an analysis of digital society, such as its collective ethos, its claims to social justice, democracy and personal freedom."[25] Rejecting an instrumental approach to ethics, based on ethical checklists and a set of measures, the EAG encouraged "proactive reflection about the future of human values, rights and liberties, including the right to data protection, in an environment where technological innovation will always challenge fundamental concepts and adaptive capabilities of the law".

Despite a critical overlap between ethical and legal values, the outcome of the EAG clearly highlighted the tension between the challenges posed by data-intensive technologies and the response provided by the law, where the latter only partially addresses the diversity of societal consequences.[26] Responsible innovation and value-sensitive design, based on co-shaping of ethical considerations and design solutions in a case-by-case approach, were proposed[27] as methodological path towards digital ethics.

Unfortunately, this focus on methodology was largely neglected in the next widely promoted initiative of the European Commission, the Independent High-Level Expert Group on Artificial Intelligence set up by the European Commission.[28] Leaving aside certain critical issues in the compo-

24 European Data Protection Supervisor. «Opinion 4/2015 Towards a new digital ethics», 2015, 12. https://edps.europa.eu/sites/default/files/publication/15-09-11_data_ethics_en.pdf.

25 European Data Protection Supervisor, Ethics Advisory Group (2018) Towards a Digital Ethics, 7.
https://edps.europa.eu/sites/edp/files/publication/18-01-25_eag_report_en.pdf.

26 European Data Protection Supervisor, Ethics Advisory Group (fn. 11), 15 ("The new digital age generates new ethical
questions about what it means to be human in relation to data, about human knowledge and about the nature of human experience. It obliges us to re-examine how we live and work and how we socialise and participate in communities. It touches our relations with others and perhaps most importantly, with ourselves").

27 European Data Protection Supervisor, Ethics Advisory Group (fn. 11), 22.

28 Independent High-Level Expert Group on Artificial Intelligence set up by the European
Commission (2019) Ethics Guidelines for Trustworthy AI. https://ec.europa.eu/futurium/en/aialliance-consultation.1.html.

sition and working methodology of this group[29] and (as with the EAG) the overlap between ethical and legal values, the main output of this group (The Assessment List For Trustworthy Artificial Intelligence (ALTAI) for Self-Assessment[30]) is a questionnaire-based self-assessment tool.[31]

Although ALTAI emphasises the importance of a multidisciplinary team in carrying out the assessment,[32] the proposed model only provides only a few questions on societal impact with a very narrow focus,[33] unable to address the wide range of societal consequences of the use of AI in many fields.

This limitation and the long list of questions, which only partially address ethical and societal issues,[34] show the inherent weaknesses of using a questionnaire-based model to address these issues, whereas relying on

29 See also Thomas Metzinger. 2019. Ethics washing made in Europe, available at https://www.tagesspiegel.de/politik/eu-guidelines-ethics-washing-made-in-europe/24195496.html, accessed on April 11, 2019. Thomas Metzinger was a member of the expert group.

30 Independent High-Level Expert Group on Artificial Intelligence set up by the European Commission. «The Assessment List For Trustworthy Artificial Intelligence (ALTAI) for Self-Assessment», 2020. https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment.

31 The overlap with legal values is evident in the questions on fundamental rights, privacy and data governance, technical robustness and safety, diversity, non-discrimination and fairness, and environmental impact. The self-assessment checklist also includes questions on AI and risk management, such as those on technical robustness and safety, transparency (traceability), and accountability. The latter refers in part to legal issues, where accountability questions relate to auditing and redress in the event of harm.

32 Independent High-Level Expert Group on Artificial Intelligence set up by the European Commission. «The Assessment List For Trustworthy Artificial Intelligence (ALTAI) for Self-Assessment» (fn. 16), 4.

33 These are the proposed questions: Could the AI system have a negative impact on society at large or democracy?; Did you assess the societal impact of the AI system's use beyond the (end-)user and subject, such as potentially indirectly affected stakeholders or society at large?; Did you take action to minimize potential societal harm of the AI system?; Did you take measures that ensure that the AI system does not negatively impact democracy?

34 Some ethical and social issues are considered by the questions of the assessment model in the following areas: human agency and autonomy, human oversight (this part also includes questions on risk management), transparency (with regard to the question on traceability of the outcomes of the algorithmic system and some questions on explainability and communication, which are ancillary to stakeholder and right holder participation), diversity, non-discrimination and fairness (as far as universal design and shareholder participation are concerned), and accountability (limited to the question on the establishment of an ethics review board).

expert evaluation combined with a participatory approach is more appropriate, as initially pointed out by the EDPS.[35] In addition, reducing ethics to a checklist largely limits the consideration of ethical issues by turning them into a functional risk-centred analysis with a very limited role for value design.

Based on this experience, some suggestions can be made for the future implementation of the AI Act or, more generally, for a future holistic approach to AI.

First, a regulatory model centred on conformity assessment, while including human rights, leaves out important issues that need to be taken into account in the implementation of AI projects. AI applications cannot be considered as given, unquestionable and only assessed to minimise their high risk. First of all, it is necessary to examine their social acceptability and, if confirmed, the way in which societal values (including ethical values) are embedded in the solutions adopted while avoiding conflicts with the values of the target communities. Real cases have shown that projects are likely to fail if these aspects are ignored.[36]

The AI Act should therefore be accompanied by appropriate solutions to integrate ethical and societal issues into the evaluation of potential uses of AI. The AI Act should not be seen as the end of the ethical debate: while it makes a positive contribution to avoiding improper overlaps between ethics and law, it does not address the societal issues that need to be faced before the development of an AI capable of passing the AI Act's conformity assessment. In this respect, acceptability is not just a matter of safety, security and respect for fundamental rights.

35 On participation see also European Center for Not-for-Profit Law Stichting (ECNL). 2023. «Framework for Meaningful Engagement: Human Rights Impact Assessments of AI | ECNL», https://ecnl.org/publications/framework-meaningful-engagement-human-rights-impact-assessments-ai; Data Justice Lab. 2022. «Civic Participation in the Datafied Society: Towards Democratic Auditing?», https://datajusticelab.org/wp-content/uploads/2022/08/CivicParticipation_DataJusticeLab_Report2022.pdf; Mantelero. Beyond Data (fn. 4), 127-130.

36 See, e.g., Scassa T (2020) Designing Data Governance for Data Sharing: Lessons from Sidewalk Toronto.
Technology & Regulation, Special Issue: Governing Data as a Resource, Technology and
Regulation 44–56; Goodman EP, Powles J (2019) Urbanism Under Google: Lessons from Sidewalk Toronto.
Fordham L. Rev. 88(2):457–498.

Second, in putting the ethical and societal impact of AI at the heart of the debate, it is important to avoid turning the assessment exercise into a mere technical tool, where an in-depth analysis of guiding values and their integration into AI solutions is replaced by standardised questions. As in the long-lasting experience of ethics boards and committees, including some recent implementations of this practice in the AI industry, it is important to understand individual and societal needs and be able to mediate them through technology, building a value-oriented AI design that is aligned with the characteristics of the context in which AI will be deployed.

Three elements are crucial to achieve this result: independent experts, the commitment of AI developers, and the active engagement of the community where AI solutions will be implemented. The latter are not necessarily territory-based communities but often large and distributed communities of end users.

Without repeating considerations expressed elsewhere, it is worth noting that societal impact assessment is more complicated than human rights impact assessment because it cannot benefit from a well-defined and, to a large extent, universal benchmark.[37] The key elements are therefore contextualisation, based on expert insights into the values to be taken into account, and participation, which is useful to complement and verify this expert assessment.

There is no one-size-fits-all way to implement this model centred on these two elements, and we should also be aware that the structure, composition and internal organisation of expert committees are not neutral elements, nor is the way in which stakeholders and rightsholders are involved. In both cases, the manner in which the assessment is carried out influence its outcome in terms of quality and reliability of the results.

Given the contextual nature of the AI projects and their impacts, it is possible to identify some key elements that characterise these expert bodies (e.g. independence, multidisciplinarity, and inclusiveness; transparency of internal procedures and decision-making processes; provisional nature of their decisions), but a variety of structures and types of organisation are possible in terms of (i) member qualifications, (ii) rights-holder, stakeholder, and layperson participation, and (iii) internal or external experts.

With regard to the commitment of AI developers, it is important to build a bridge between these expert bodies and the day-to-day activities of

37 See fn. 19.

AI development. In this respect, an ethical body or advisory team should neither be seen as a control body, making it difficult to accept its role, nor as a body to which all ethical and social issues can be delegated, with the implicit lack of a by-design approach by developers from the early stages of AI projects.[38]

Finally, regarding the role of the participatory approach in dealing with societal issues, it is worth emphasising that participation not only contributes to a better understanding of the societal and ethical issues, but is also essential for effective democratic decision-making in AI.

D. In search of a principles-based core for AI regulation

Looking at the framework for the development of AI set out by the EU legislator in the AI Act, it is not only the societal issues that are critical, but also the way in which the focus on fundamental rights has been framed.

In other crucial areas of technological development, such as biotechnologies and digital information, the European legislators have usually developed more elaborate regulatory instruments that establish a set of principles to guide operators in shaping technology, rather than simply affirming human rights and societal values. This was the case with the Oviedo Convention and the EU regulation and practice on clinical trials, as well as in the case of the information society where Convention 108+[39] and the GDPR set out guiding principles to embed key values in the design of medical, biomedical, and ICT products and services.

A general part focusing on key principles was absent from the debate on the AI Act and was only proposed at the end in the amendments adopted by the European Parliament (see Section D.IV). However, given the pervasive nature of AI and the wide range of its applications, defining a set of common principles is not an easy task.

In the following sub-sections three different contexts are considered in the search for possible guiding principles. First, the main principles that

38 One possible solution is to appoint an internal advisor on societal issues (also known as Chief Ethics Officer) as a permanent contact for day-to-day project development and as a trait d'union with the external experts.

39 See also Mantelero, Alessandro; Stalla-Bourdillon, Sophie, and Kwasny, Sophie (eds). 2021. Convention 108 and the future data protection global standard. Computer Law & Security Rev., Special Issue, https://www.sciencedirect.com/journal/computer-law-and-security-review/special-issue/10FW5NWHJFK.

have emerged in the ethical debate on AI will be considered, as they often have a legal dimension. This is followed by an examination of two other specific initiatives: the Council of Europe's draft framework convention on AI and the principles set out by the NIST and the Blueprint for an AI Bill of Rights in the US. The potential impact of these two initiatives on global trends in the regulation of AI and in the definition of its core principles is related to the international scope of the Council of Europe's approach and the prominent position of US companies in AI development, respectively.

I. The principles set out in the ethical charters

Growing concerns about the impact of AI on individuals and society have stimulated a wide range of initiatives to outline key guiding values for AI development.[40] Looking at this corpus of ethical charters can provide some suggestions for relevant values to be included in AI regulation, to be translated into legal values or be considered as part of the legal assessment, as is the case in the regulation of biomedicine and scientific research.

Several studies[41] have focused on the key values of these guidelines identifying a small core of values that are common to most of the documents. according to a first study,[42] five of them are ethical values with a strong

40 See also Raab, Charles D. «Information Privacy, Impact Assessment, and the Place of Ethics». Computer Law & Security Review 37 (6 March 2020): 105404. https://doi.org/10.1016/j.clsr.2020.105404 ("a bewildering array of ethics boards, panels, committees, groups, centres, frameworks, principles, templates, guidelines, protocols, projects and the like have all popped up like woodland mushrooms in a wet Autumn").

41 It is worth pointing out some of the limitations of these studies: the use of grey literature, the use of search engines for content selection, linguistic biases, and a quantitative text-based approach that underestimates the policy perspective and contextual analysis. From a policy and regulatory perspective, their main limitation is the quantitative approach adopted, which considers differing sources at the same level, without taking into account the differences between the guidelines adopted by governmental bodies, independent authorities, private or public ad hoc committees, big companies, NGOs, academia, intergovernmental bodies etc. When the focus is on values for future regulation, the different relevance of the sources in terms of political impact is important, and the mere frequency of occurrence does not take this impact into account.

42 Jobin et al. 2019. The authors identified ten key ethical values within a set of 84 policy documents with the following distribution: transparency 73/84; non-maleficence 60/84; responsibility 60/84; privacy 47/84; beneficence 41/84; freedom and autonomy 34/84; trust 28/84; sustainability 14/84; dignity 13/84, and solidarity 6/84.

legal implementation (transparency, responsibility, privacy, freedom and autonomy) and only two come from the ethical discourse (non-maleficence and beneficence). Another study[43] identified several guiding values and the top nine are: privacy protection; fairness, non-discrimination and justice; accountability; transparency and openness; safety and cybersecurity; common good, sustainability and well-being; human oversight, control and auditing; solidarity, inclusion and social cohesion; explainability and interpretability. As in the previous study, the aggregation of these principles is necessarily influenced by the categories used by the authors to reduce the diversity of principles.

If we take a qualitative approach, limiting the analysis to the documents adopted by the main European organisations and those with a general and non-sectoral perspective,[44] we can better identify the key values that are most popular among rule makers.

looking at the four core principles[45] identified by the High-Level Expert Group on Artificial Intelligence,[46] respect for human autonomy and fairness are widely developed legal principles in the field of human rights and law in general, whereas explicability is a technical requirement rather than a principle. With regard to the seven requirements[47] identified by the HLGAI on the basis of these principles, human agency and oversight are further specified as respect for fundamental rights, informed autonomous decisions, the right not to be subject to purely automated decisions, and the adoption of oversight mechanisms. These are all requirements that are already present in the law in various forms, particularly in relation to data processing. The same applies to the remaining requirements (technical robustness and safety, privacy and data governance; transparency; diversity, non-discrimination and fairness; accountability; and environmental well-being).

43 Hagendorff (fn. 4), p 102.

44 E.g. Council of Europe – European Commission for the Efficiency of Justice (CEPEJ) 2018.

45 Respect for human autonomy, Prevention of harm, Fairness, Explicability.

46 Independent High-Level Expert Group on Artificial Intelligence set up by the European Commission 2019.

47 Human agency and oversight; Technical robustness and safety; Privacy and data governance; Transparency; Diversity, non-discrimination, and fairness; Societal and environmental wellbeing; Accountability.

Another important EU document identifies the following nine core principles and democratic prerequisites:[48] human dignity; autonomy; responsibility; justice, equity, and solidarity; democracy; rule of law and accountability; security, safety, bodily and mental integrity; data protection and privacy; sustainability.

Based on the results of these different (quantitative, qualitative) methods of analysis, we can identify three main sets of values that are relevant from a regulatory perspective and can form a set of principles-based references for a more holistic implementation of AI regulation.

The first consists of the contextual application of principles that are already enshrined in law but play a crucial role in AI, such as privacy and data protection, fairness, non-discrimination, justice, freedom, and autonomy. A second group covers general legal principles that are relevant in the AI context and includes transparency, explainability, interpretability, accountability, and responsibility. The last group, which includes safety and cybersecurity, control and auditing, transparency, openness and human oversight, consists of principles that deal with technical and procedural issues.[49]

II. Principles identified by the Council of Europe

In 2019, the Council of Europe started a reflection on the adoption of a future convention on AI. On the basis of preliminary studies on the legal[50] and ethical dimensions[51] of AI regulation, the Ad Hoc Committee on Artifi-

48 European Commission - European Group on Ethics in Science and New Technologies 2018.

49 In a way that is consistent with the nature of these ethical charters, they also include specific ethical values derived from ethical and sociological theory (e.g., common good, well-being, solidarity) and principles from applied ethics and research/medical ethics (e.g., non-maleficence, beneficence). These principles can play a crucial role in addressing societal issues related to the use of AI, but need to be properly contextualised to avoid the potential risk of 'transplanting' of ethical values.

50 Mantelero A (2020) Analysis of international legally binding instruments. In Council of Europe. Towards regulation of AI systems. Global perspectives on the development of a legal framework on Artificial Intelligence systems based on the Council of Europe's standards on human rights, democracy and the rule of law. DGI (2020)16, pp 61–119.

51 Ienca M, Vayena E (2020) AI Ethics Guidelines: European and Global Perspectives. Ibidem, pp 38–60.

cial Intelligence (CAHAI) elaborated its feasibility study[52] and developed a participatory process among its members and with the involvement of external stakeholders. This led to a first draft of the Possible elements of a legal framework on artificial intelligence, based on the Council of Europe's standards on human rights, democracy and the rule of law.[53]

After this first phase of the drafting process, a new committee (the Committee on Artificial Intelligence - CAI) took over from the CAHAI with the task of providing an "appropriate legal instrument on the development, design, and application of artificial intelligence systems based on the Council of Europe's standards on human rights, democracy and the rule of law, and conducive to innovation, in accordance with the relevant decisions of the Committee of Ministers".[54]

This analysis focuses on the Revised Zero Draft [Framework] Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law, which was prepared by the Chair of the CAI with the assistance of the Secretariat to serve as a basis for the drafting of the future convention on AI and "does not reflect the final outcome of negotiations in the Committee".[55]

The proposed draft included six guiding principles: equality and non-discrimination; privacy and personal data protection; accountability and

52 Council of Europe, Ad hoc Committee on Artificial Intelligence (CAHAI). 2020a. Feasibility
Study, CAHAI(2020)23. https://rm.coe.int/cahai-2020-23-final-eng-feasibility-study-/1680a0c6da.

53 The text of the proposal is available here https://rm.coe.int/possible-elements-of-a-legal-framework-on-artificial-intelligence/1680a5ae6b. For a critical analysis of the CAHAI work and results, see also Mantelero, A. and Fanucci, F. 2022. Great ambitions. The international debate on AI regulation and the human rights in the prism of the Council of Europe's CAHAI. In Philip Czech et al. (eds). European Yearbook on Human Rights 2022 (Intersentia: Cambridge), pp. 225-252.

54 See the CAI's Terms of Reference available here: https://rm.coe.int/terms-of-reference-of-the-committee-on-artificial-intelligence-for-202/1680a74d2f.

55 Adopted in Strasbourg, on 6 January 2023 CAI(2023)01, and available here https://rm.coe.int/cai-2023-01-revised-zero-draft-framework-convention-public/1680aa193f.
At its 4th Plenary meeting, the CAI decided to make the revised "Zero Draft" [Framework] Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law public. A more recent document was prepared by the Chair of the CAI, see Committee on Artificial Intelligence. Consolidated working draft of the Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law, Strasbourg, 7 July 2023 CAI(2023)18, https://rm.coe.int/cai-2023-18-consolidated-working-draft-framework-convention/1680abde66 (last accessed 11.08.23). This document does not reflect the outcome of the negotiations in the Committee and is therefore not considered here as the main reference.

responsibility; transparency and oversight; safety; safe innovation. Apart from the last one (safe innovation), which is not a principle but only a provision to legitimise the use of the so-called regulatory sandbox for AI, the others mainly recall existing principles[56] without any specific contextualisation with regard to AI.

In addition, accountability, responsibility and legal liability, as well as safety, cannot be considered as principles but as general rules or operational legal requirements. Incidentally, it is worth noting that their specific application in the field of AI is much debated, both in terms of how to allocate AI liability and how to ensure safety through standards or other solutions.[57] Against this background, a general reference to these criteria does not provide any specific regulatory guidance to the states.

Only the specific requirement to develop "adequate oversight mechanisms as well as transparency and auditability requirements tailored to the specific risks arising from the context in which the artificial intelligence systems are applied are in place" seems to provide a specific contribution to AI regulation in terms of broad transparency and oversight obligations.

Building on the Council of Europe's legal framework, a different approach could have been adopted by contextualising the principles already enshrined in the legal instruments of the Council of Europe in relation to the challenges posed by AI. For example, the principle of beneficence enshrined in Article 6 of the Oviedo Convention[58] can be applied to AI in a context-specific way, where the complexity or opacity of AI-based solutions places limits on individual consent, which therefore cannot be the exclusive basis for intervention.[59]

Comparing the Revised Zero Draft with the Oviedo Convention and Convention 108/108+, the difference between conventions that establish a

56 See, e.g., Article 12 of the Revied Zero Draft which merely states that "Each Party shall, within its jurisdiction and in accordance with its domestic law, ensure that the design, development and application of artificial intelligence systems respect the principle of equality, including gender equality and rights related to discriminated groups and individuals in vulnerable situations".

57 See European Commission, Proposal for a Directive of the European Parliament and the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive). COM/2022/496 final. See also The European AI Liability Directives – Critique of a Half-Hearted Approach and Lessons for the Future, Computer Law and Security Review, forthcoming, https://arxiv.org/abs/2211.13960.

58 See also Oviedo Convention, Articles 16 and 17.

59 For a proposal in this regard, see Mantelero Beyond (fn. 4), Ch. 4, para 4.2, and Mantelero. Analysis of international legally binding instruments (fn. 50).

specific framework of principles focused on their specific scope and the CAI proposal, which simply recalls for the respect for existing rights and principles without any contextualisation to address the challenges of the AI environment, is clear.

III. The principles set out by the US National Institute of Standards and Technology (NIST)

The NIST framework is characterised by a peculiar approach to risk, as the report clearly states (emphasis in the original text): "While risk management processes generally address negative impacts, this Framework offers approaches to minimize anticipated negative impacts of AI systems *and* identify opportunities to maximize positive impacts". In defining these opportunities, the Framework refers to "potential benefits to people (individuals, communities, and society), organizations, and systems/ecosystems".[60]

These general statements about the core of the risk assessment model are consistent from a risk analysis perspective, but raise some key issues from a legal perspective, which become relevant when – as in the AI Act – risk assessment is part of a regulatory compliance framework with associated obligations, sanctions for non-compliance, and potential liability.[61]

The first main issue concerns the decision to include benefits in the risk assessment. Leaving aside the difference between a purely risk-based approach and a rights-based approach to risk, a key issue is who is entitled to define the "benefits to people (individuals, communities, and society), organizations, and systems/ecosystems" that may justify exposure to risk, including potential prejudice to human rights.

The balancing of competing interests is common in law, but is based on a legal assessment that, in accordance with the relevant legal system, wights the interests of individuals, communities, and society as defined through a democratic process that results in legal provisions and their interpretation by the courts.

Here, in the Framework, this balancing exercise between the negative impacts of the use of AI – which includes restrictions or prejudice to individual and collective rights and freedoms – and its benefits is carried out

60 National Institute of Standards and Technology. 2023. Artificial Intelligence Risk Management Framework (AI RMF 1.0), https://doi.org/10.6028/NIST.AI.100-1, 4.

61 See also European Commission, AI Liability Directive (fn. 57) and its relation to the AI Act.

by AI developers outside any democratic and participatory framework. In short, a company will decide what are the individual/collective benefits and restrict individual/collective rights and freedoms without any legitimacy.

Different considerations could be made for the public sector, where the nature of public bodies and their mandate may legitimise them to conduct an assessment of individual and collective interests based on the power vested in them by law and the associated democratic scrutiny of the exercise of that power.

Against this background, while assessing the negative impacts of AI is an exercise that can be carried out by AI developers as the framework is given (i.e. human rights, mandatory security and conformity rules and principles), this framework is not given for the potential benefits. Given the trade-off between benefits and negative impacts, and the variety of potential benefits – which could include purely economic benefits – this exercise differs from the traditional balancing test between competing interests protected by law, and opens the doors to self-assessment by AI developers, who end up deciding what the societal benefits of AI are.[62]

Although this concern can be mitigated by the participatory approach proposed by the Framework,[63] which involves experts and civil society in the evaluation, the lack of a model for participatory assessment[64] seriously hampers the possibility of using this broader engagement to mitigate the concerns outlined above.

The NIST document sets out some principles for AI development, but – with some exceptions on fairness and privacy – they do not focus on societal needs in relation to AI and the legal and societal values that should underpin AI development and its use. They are mainly technical requirements, according to which an AI system must be valid, reliable,[65]

62 These critical considerations can also be extended to the amendment proposed by the European Parliament regarding the risk management system in the AI Act, see European Parliament, P9_TA(2023)0236, Article 9.5 ("High-risk AI systems shall be tested for the purposes of identifying the most appropriate and targeted risk management measures and weighing any such measures against the potential benefits and intended goals of the system. Testing shall ensure that high-risk AI systems perform consistently for their intended purpose and they are in compliance with the requirements set out in this Chapter").

63 See pp. 11, 17, and 24.

64 See p. 24.

65 i.e. ability of an item to perform as required, without failure, for a given time interval, under given conditions.

robust,[66] safe, secure, resilient, accountable, transparent, explainable and interpretable.

Meeting these technical requirements can certainly help to design of a human-centered AI that is more respectful of individual and collective rights, as well as the values and needs of society, but they are not in themselves capable to pave the way for value-oriented design that outlines the goals and boundaries of AI use in our society.

IV. A late addition: the European Parliament's general principles applicable to all AI systems

In the last round of amendments to the AI Act, the European Parliament tried to fill the gap in the act regarding to the lack of guiding principles for AI development. Although this was a critical shortcoming, the solution of copying the principles outlined by the Independent High-Level Expert Group on Artificial Intelligence set up by the European Commission[67] does not fully address the criticisms that characterise the AI Act on this issue.

First, these principles were the result of a controversial drafting process.[68] Second, as noted above, they largely repeat requirements that already exist in various forms in the law. Although the proposed provision introduces some contextualisation of these principles, a broader analysis based on the main existing international legal instruments[69] could have helped to outline a more comprehensive framework of principles.

Looking at the individual principles, some of them seem superfluous. This is the case with the principle of 'privacy and data governance', which simply refers to existing privacy and data protection rules. It is also the case with the principles of 'diversity, non-discrimination and fairness' which refers to the promotion of gender equality and cultural diversity, and the prevention of discriminatory effects and unfair biases prohibited by Union

66 i.e. ability of a system to maintain its level of performance under a variety of circumstances.

67 See above Section D.I. There are still some misunderstandings and improper overlap between legal and ethical perspectives in the amendments proposed by the European Parliament, see e.g. European Parliament, P9_TA(2023)0236 (fn. 8), Recital 9a in relation to Article 4a.

68 See Thomas Metzinger. «Ethics washing made in Europe». Tagesspiegel 8 April 2019, https://www.tagesspiegel.de/politik/eu-guidelines-ethics-washing-made-in-europe/24195496.html.

69 See fn. 50.

or national law. Here, the only element specifically relevant as a guiding principle for AI development and use is inclusiveness ("AI systems shall be developed and used in a way that includes diverse actors").

Similar considerations can be made with regard to the principle of 'human agency and oversight' where it requires AI systems to be developed and used "as a tool that serves people, respects human dignity and personal autonomy", which are either vague references (serving people) or general principles already enshrined in the EU framework.

Other principles are vague and cannot easily be adapted to the legal framework or contextual AI applications. This is the case with the principle of social and environmental well-being. On the one hand, the reference to sustainability and an environmentally friendly approach seems redundant within the broader EU legal framework, also in view of the rough description given for this principle. On the other hand, the commitment "to benefit all human beings, while monitoring and assessing the long-term impacts on the individual, society and democracy" sounds too ambitious and inconsistent with the uses of AI which, by their very nature, do not necessarily benefit all human beings and may also produce outcomes that adversely affect certain individuals, including in terms of legal effects.

To a large extent, this list of principles is mainly a vademecum, recalling principles and values that are already present in EU law or, if new, that can hardly guide AI developers and deployers due to their vagueness and wide scope.

The principles of transparency, technical robustness and safety are an effective contribution in terms of contextualisation of already existing general principles, especially with regard to the requirement for an AI design that allows for appropriate human control and oversight.

Even in this case, while technical robustness and safety are appropriately and contextually framed, the transparency principle refers to traceability and explainability but both these two requirements can be implemented in many different ways, leaving a wide margin for manoeuver to operators.[70]

While the definition of general principles is always a difficult exercise, in balancing the need for sufficient detail on their content with the nature of general principles, the list proposed by the European Parliament seems to be of limited help in guiding those who have to design, develop and deploy

70 Only a few obligations are listed specifically and in a rather general way (awareness of human-AI interaction, notification of the capabilities/limitations of the individual AI system, information on user rights).

AI products and services. Principles on aspects such as individual and community participation in AI design, public debate on the need to choose an AI-based solution over other possible options,[71] respect for community values and diversity in AI applications with a social impact are just some of the possible improvements for a human-centric approach to AI.

E. Towards a full implementation of the risk-based approach: the role of fundamental rights

Over the years, various technologies with a major impact on society and innovation have been regulated through international and regional instruments, establishing common principles and rights to pave the way for innovation in a manner consistent with societal values and aspirations.

These legal instruments have not only established general principles, nor have they simply emphasised the importance of ensuring human rights protection, but have also outlined guiding principles centered on the specific technological context to be regulated in order to support its values-oriented development, rather than being limited to its technical efficiency and safety nature.

Based on the brief analysis carried out in the previous sections, the ethical charters on AI, the Council of Europe's approach and the framework provided by the NIST have identified some common values for AI development (e.g. respect for equality and non-discrimination, protection of personal data, transparency, accountability, security), as has the European Parliament, but these are, to a large extent, general statements that are not contextualised in the specificity of the AI environment. It is therefore difficult to see in these various initiatives a clear approach capable of establishing principles that will effectively guide the development and use of AI.

Although a more contextual exercise was possible, it seems that at this early stage of AI regulation the elaboration of a tailored set of principles is not yet mature. In this regard, initiatives such as the European Declaration

71 See Council of Europe, Consultative Committee of the Convention for the Protection of Individuals
with regard to Automatic Processing of Personal Data (Convention 108) (2019) Guidelines on
Artificial Intelligence and Data Protection, T-PD(2019)01. https://rm.coe.int/guidelines-onartificial-intelligence-and-data-protection/168091f9d8, paras II.9 and III.8.

on Digital Rights and Principles for the Digital Decade may suggest that a longer journey towards a principles-based regulation is possible, but for now a pragmatic, risk-focused approach prevails.

This does not mean that, in the absence of guiding principles, legal issues related to AI only concern traditional industrial and product safety. On the contrary, the lack of adequate guiding principles call for the human centric-AI proposed by European legislators to be built on the existing human/fundamental rights framework. A framework that, even if not used to outline guiding principles, will necessarily feed into impact assessment models.

However, it is important not to overestimate the scope of the risk-based approach. An example of this is the Council of Europe's decision to develop an impact assessment model that can cover not only human rights (HRIA), but also democracy, and the rule of law. While the HRIA is not new and, with some modifications, can be used in AI, the inclusion of democracy and the rule of law is challenging in its transition from theoretical vision to concrete implementation.[72]

The democratic process and democracy in its various manifestations cover a wide range of issues, making it methodologically difficult to assess the impact of a technology and its various applications on them. Even more so since it is difficult to assess the level of democracy itself. This does not mean that it is impossible to carry out an impact assessment on specific areas of democratic life, such as the right to participation or access to pluralist information, but this remains a HRIA, albeit one centered on civil and political rights.

Different considerations apply to the rule of law, where the more structured field of justice and the limited application of AI make it easier to envisage uses and foresee their impact on a more uniform and regulated set of principles and procedures than in democracy. However, even in this case, the specificity of the field and the interests at stake may raise some doubts about the need for an integrated risk assessment model – encompassing human rights, democracy, and the rule of law – as opposed to a more limited assessment of the impact of specific AI applications on the rule of law.

72 The same consideration can be applied to the amended text of Article 9 adopted by the European Parliament, which has extended risk management to democracy and the rule of law.

While Human Rights Impact Assessment can be implemented in AI applications, it is still largely more a goal rather than a specific response provided by the legislators, who refer to it without providing concrete methodological solutions. As noted elsewhere, the traditional HRIA is primarily a policy tool rather than a regulatory tool, and it is usually territory-based and covers a wide range of rights and freedoms.[73] HRIA therefore needs to be reshaped to serve the purposes of AI regulation, which focuses on risk thresholds and risk management obligations.

In this respect, although the discussion and proposals on AI regulation are quite mature, the core issues relating to the model for carrying out such an assessment have not yet been worked out in such a way that provides meaningful input to companies and other actors that will have to comply with the AI Act.

Several limitations affect the proposed models: (1) use of lengthy questionnaires following an awareness-raising model rather than an impact assessment model;[74] (2) misunderstandings about the key parameters to be considered for impact assessment;[75] (3) an aggregate impact on fundamental rights regardless of their specific nature; (4) little focus on how to quantify the risk, which is at the heart of AI Act conformity assessment.

Based on the DPIA (Data Protection Impact Assessment)/PIA (Privacy Impact Assessment) experience, more streamlined proposals are needed providing a methodology rather than a fixed scheme that cannot cover the full range of AI applications. Self-assessment is possible but must be based on an independent expert evaluation, which is the only way to contextualise how specific AI applications may affect fundamental rights. An expert-based evaluation, combined with appropriate tools for stakeholder

73 See Mantelero. Beyond Data (fn. 4), Ch. 2.

74 See, e.g., Government of the Netherlands. 2022. Fundamental Rights and Algorithms Impact Assessment (FRAIA) https://www.government.nl/documents/reports/2021/07/31/impact-assessment-fundamental-rights-and-algorithms.

75 See, e.g., Government of the Netherlands (fn. 74), 74-75; The Alan Turing Institute. 2021. Human Rights, Democracy,
and the Rule of Law. Assurance Framework for AI Systems: A proposal prepared for the Council of Europe's Ad hoc
Committee on Artificial Intelligence, https://rm.coe.int/huderaf-coe-final-1-2752-6741-5300-v-1/1680a3f688 62-(where, e.g., the indices are calculated summing heterogeneous variables, using different scales, and including variables for the affected right-holders considered in total numbers rather than in proportion to the total number of the right-holders).

and rightsholder participation, can easily rely on a lean assessment model, which also improves the transparency of the assessment.

Such an approach is possible, not by using a 300-page impact assessment model, but by outlining the key elements to be considered and developing a methodology to combine and assess the different risk components of AI in relation to fundamental rights.[76]

Unfortunately, the current debate seems likely to complicate the way in which AI regulation, and the AI Act in particular, will be implemented. Unrealistic standards for HRIA/FRIA (Fundamental Rights Impact Assessment), rather than a general methodology, and lengthy and cumbersome assessment models (including misunderstandings in risk assessment) are not in line with the previous experience of DPIA/HRIA and are likely to turn FRIA into a box-ticking and bureaucratic exercise.

It would therefore be important for the EU bodies (including the European Union Agency for Fundamental Rights and CEN/CENELEC) to engage in a serious and inclusive discussion on FRIA, avoiding inner circles and including real domain experts and critical voices.

In this context, the European Parliament's proposal to introduce a Fundamental Rights Impact Assessment for high-risk AI systems[77] was intended to highlight the role of FRIA, but if not properly developed, FRIA risks to complicate the regulatory framework rather than addressing its limitations.

More specifically, the AI Act provides for three different forms of impact assessment: (i) a technological assessment based on a general evaluation of certain AI-based technologies in order to list them as high-risk applications (Annex III and Articles 6 and 7); (ii) a conformity assessment, focused on the specific AI applications and carried out by AI providers according to standards to be defined (Articles 9, 17 and 40); (iii) a FRIA, carried out by deployers, focused on the contextual use of the specific AI application and not based on standards. This combination of assessment procedures of different scope and nature gives rise to several internal conflicts.

First, the methodological criteria for carrying out the impact assessment are not defined or are (in the Parliament's text[78]) outlined in an unclear manner, focusing on the two main variables traditionally used in risk as-

76 These were the key elements of the methodology for HRIA in AI described in Mantelero. Beyond Data (fn. 4), Ch. 2, where a methodology for assessing the level of impact on the rights potentially affected by a given AI application is proposed.

77 See Article 29a of the text of the AI Act amended by the European Parliament.

78 See Article 3(1a) and 3(1b).

sessment (i.e., likelihood of harm and the severity of that harm) but adding other parameters in the definition of 'significant risk' – namely severity, intensity, probability of occurrence, duration of effects, ability to affect an individual, a plurality of persons or to affect a particular group of persons – which should be considered as sub-categories within the two main variables (e.g., the duration of negative effects should be included in severity).

Second, these three forms of assessment show a different approach to the assessment criteria and their setting: for the technology assessment to be carried out by the Commission (Annex III and Articles 6 and 7) the main variables are the severity and probability of occurrence of the risk;[79] no variables are provided for the conformity assessment to be carried out by AI providers, which is largely left to future harmonised standards (Article 40); no variables are provided for the performance of the FRIA by the natural or legal person, public authority, agency or other body using an AI system under its authority, and no standards are planned for this case (Article 29a).

Although, according to the general risk assessment theory, we can assume that the two criteria set for technology assessment (severity and probability) should be the same for the other forms of assessment, the lack of a clear guidance and the confusion in considering these criteria should lead the EU legislator to provide a common general framework of relevant parameters for impact assessment.

Moreover, there is a risk of methodological conflict in assessing the same AI application against specific standards (in the case of the AI provider) and pure self-assessment (in the case of the entity using an AI system under its authority), where the two methodologies may diverge. Nor does a generalisation of standards seem to be a better option.

The lack of experience of EU standardisation bodies in the field of fundamental rights,[80] their business-oriented composition and the lack of transparency in their procedures,[81] as well as the absence of an effective and

79 See Article 7 of the AI Act proposal.

80 See also European Commission, A Notification under Article 12 of Regulation (EU) No 1025/20121 on a standardisation request to the European Committee for Standardisation (CEN) and the European Committee for Electrotechnical Standardisation (CENELEC) in support of safe and trustworthy artificial intelligence, draft, Brussels, 5.12.2022.

81 Veale, Michael and Zuiderveen Borgesius, Frederik, Demystifying the Draft EU Artificial Intelligence Act (July 31, 2021). Computer Law Review International (2021) 22(4) 97-112.

broad democratic participation in standard-setting are clear limitations of this solution. Furthermore, it should be made clear that the standard for impact assessment should be a methodological standard that outlines the variables to be used in the assessment process and how they are quantified and combined: a methodological standard that is suitable for all the different contexts in which AI is used, and not just an awareness tool based on a long list of questions.[82]

Given the uniformity of risk assessment procedures based on the common theory of risk assessment, the easiest way to address the criticism discussed above is to provide a clear list of key parameters for risk assessment. These should be the same for all the forms of assessment, but with a different implementation in the technology assessment to be performed by the European Commission and in the contextual impact assessment to be carried out by providers and deployers, the former being a general ex ante evaluation based on case scenarios or similar tools, while the latter are contextual impact assessments related to a specific AI application. In addition, given the established elaboration of risk assessment and the previous experience in regulating data protection impact assessment, these criteria should be further implemented in a specific general methodology by AI supervisory bodies.

The feasibility and effectiveness of this approach is confirmed by the implementation of the GDPR, where supervisory authorities have played a key role in establishing uniform methodologies for DPIA. This solution, also in view of the composition of the proposed European Artificial Intelligence Office, can provide more competence, transparency and integration with the existing institutional bodies – including on fundamental rights issues – than delegation to standardisation bodies, which lack sufficient expertise and legitimacy to deal with fundamental rights issues.

The overall regulatory framework for risk assessment should therefore be based on three different layers: (i) common general criteria and variables to be used in impact assessment, defined for all types of assessment; (ii) impact assessment methodologies, defined by an ad hoc EU supervisory body (which also ensure EU-wide harmonisation); (iii) technical standards, set by standardisation bodies, covering the safety and security of the AI systems, but not their impact on fundamental rights.

As far as the AI providers and deployers are concerned, risk assessment should be an integrated tool with a proportionate distribution of burdens

82 See fn. 76.

based on the actual risk introduced into society and the ability of each actor to manage that risk, as generally accepted in the legal theory of risk. The AI provider should therefore carry out the initial assessment of a given AI product/service, taking into account all its potential uses, but the AI deployer using that product/service in a given context and for specific purposes should integrate this initial assessment with the analysis of the contextual impact and associated risks. This necessarily requires a flow of information between providers and deployers about the characteristics of the AI system and the risks associated with it.

Finally, a common methodology will facilitate not only the integration of assessments by AI providers and AI deployers, but also the integration of different AI products, thus making it possible to assess their cumulative risks.

F. Conclusions

Several initiatives around the world and at different levels are focusing on the regulation of AI. Lawmakers are trying to provide an first response to the challenges posed by the AI revolution. Focusing on the EU AI Act, this chapter has highlighted three main elements that characterise this first generation of AI laws.

First, the proposed solutions represent a compromise between the protection of fundamental rights and the expected benefits of AI. This has led lawmakers to respond only partially to the demands of individuals and society for the protection of their rights and freedoms, so as not to slow down the development of AI. This is even more evident in those contexts where there is no strong AI industry.

Second, also in the light of this compromise, it is crucial to provide guiding principles for the development of AI. These should not simply repeat existing legal requirements and principles, but contextualise them in the field of AI and only introduce new ones where necessary to address new challenges.

Third, the crucial role of the risk-based approach (made all the more important in the absence of detailed guiding principles) requires both a harmonised approach consistent with risk management theory – for all cases where risk is assessed – and the development of a specific methodology for the impact on fundamental rights. The latter should be based on

key criteria and variables and be properly implemented by the competent authorities and not be delegated to standardisation bodies.

At the current stage of the regulatory debate (August 2023), it is not possible to say whether all these objectives will be achieved in the AI Act, or whether they will be part of a further implementation strategy for AI laws that will pave the way for a second generation of such laws.

G. Epilogue

In revising the proofs of this chapter, it is worth noting that the final version of the AI Act does not address the two main issues mentioned in the conclusions, nor has the Council of Europe's Framework Convention on AI[83] provided a more robust and methodologically accurate response.

The AI Act, in its final version, has maintained the risk-based approach focused on high-risk categories and self-assessment, abandoning the mechanism based on a reasoned notification to the competent national supervisory authority for those systems that the AI providers do not consider to pose high risks, in favour of an explicit derogation provided for in Article 6(3) for those systems that do "not pose a significant risk of harm to the health, safety or fundamental rights of natural persons".[84]

Moreover, the general list of principles proposed by the Parliament is no longer present in the final text, but given the shortcomings mentioned above, this does not significantly change the situation and confirms the central role of the FRIA.

With regard to impact assessment, the final version of the AI Act does not solve the problem of the lack of harmonisation between the different impact assessment procedures, nor does it provide guidance on specific

83 The text of the Convention is available here: https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence.

84 According to this Article, this is the case where one of the following conditions is met: (i) the AI system is intended to perform a narrow procedural task; (ii) the AI system is intended to improve the result of a previously completed human activity; (iii) the AI system is intended to detect decision-making patterns or deviations from prior decision-making patterns and is not meant to replace or influence the previously completed human assessment, without proper human review; or (iv) the AI system is intended to perform a preparatory task to an assessment relevant for the purposes of the use cases listed in Annex III. A provider who considers that an AI system is not high risk under these conditions shall document its assessment and shall be subject to the registration obligation set out in Article 49(2) of the AI Act.

criteria and methodology for the FRIA. Worse, the trilogue weakened and made less precise the Parliament's proposal on the FRIA.

Although the European Parliament's proposal did not outline the key parameters for risk assessment, it included many elements of the FRIA and provided for a higher level of detail compared to the final text of the AI Act,[85] where some elements are implicit (e.g., the mitigation plan, the consideration of vulnerability, a clear description of the components of risk assessment).

Another important part of the European Parliament's proposal was the role of participation in risk assessment.[86] Unfortunately, as with the GDPR, the final version of the AI Act does not give due attention to participation, contrary to best practice in risk assessment.

However, the main difference between the European Parliament's proposal and the adopted text concerns the scope of the FRIA. Under pressure from the other two co-legislators, it was restricted to a limited area, whereas the text proposed by the Parliament referred to all high-risk AI systems as defined in Article 6(2), with the sole exception of systems used for management and operation of critical infrastructure. The final text maintains this exception but significantly narrows the general scope of the FRIA, which now covers only (i) deployers that are bodies governed by public law and private entities providing public services, and (ii) AI systems used to evaluate the creditworthiness of natural persons or for credit scoring (with the exception of AI systems used for the detection of financial fraud), and for risk assessment and pricing in life and health insurance.[87]

Although this narrow scope of the FRIA is less satisfactory from the perspective of the protection of fundamental rights and creates an imbalance between the general obligation for AI providers to assess the impact on fundamental rights of all high-risk AI systems in the context of the confor-

85 See Article 27 of the final version of the AI Act.

86 See Article 29a.4, AI Act EP ("In the course of the impact assessment, the deployer, with the exception of SMEs, shall notify national supervisory authority and relevant stakeholders and shall, to best extent possible, involve representatives of the persons or groups of persons that are likely to be affected by the high-risk AI system, as identified in paragraph 1, including but not limited to: equality bodies, consumer protection agencies, social partners and data protection agencies, with a view to receiving input into the impact assessment. The deployer shall allow a period of six weeks for bodies to respond. SMEs may voluntarily apply the provisions laid down in this paragraph. In the case referred to in Article 47(1), public authorities may be exempted from this obligations.").

87 See Annex III, 5 (b) and (c), AI Act.

mity assessment procedure and the specific obligation for deployers, it does not prevent the adoption of a broader use of this instrument based on the obligation to protect fundamental rights established at EU and national level, and facilitating the accountability of AI operators in this respect.

Given the nature of fundamental rights and the level of protection afforded to them by the Charter of Fundamental Rights of the European Union and national constitutional charters, this assessment must necessarily avoid any prejudice to them. This means that the FRIA cannot simply be a final check without influence on the AI design. On the contrary, potential impacts must be properly addressed on the basis of a sound methodological approach in order to meet the obligations to protect fundamental rights.

In this regard, academia can actively contribute to filling the existing gaps in the theoretical and methodological elaboration of the FRIA, as outlined in the AI Act, in order to facilitate the future work of EU and national authorities and AI operators in placing this key tool for human-centric and trustworthy AI at the heart of the EU approach to AI design and development.[88]

88 For a more detailed analysis and methodological guidelines for FRIA see Mantelero, Alessandro. «The Fundamental Rights Impact Assessment (FRIA) in the AI Act: roots, legal obligations and key elements for a model template». *Computer Law & Security Review* 54 (2024): 106020, https://doi.org/10.1016/j.clsr.2024.106020, which aims to fill existing gaps in the theoretical and methodological elaboration of the FRIA, as outlined in the AI Act, by defining the building blocks of a model template for the FRIA in a manner consistent with the rationale and scope of the AI Act.

Brussels to Brasilia: Brazil's Distinct Path in AI Regulation

Laura Schertel Mendes and Beatriz Kira

Abstract: The global rise of Artificial Intelligence (AI) systems across sectors has fueled urgent calls for effective regulation. While legal discussions on AI regulation have largely focused on comparisons between developed economies, this chapter focuses on a Global South jurisdiction, analyzing Brazil's innovative AI regulation proposal (Bill No. 2338/2023). Distinct from a mere adoption of existing models, the Brazilian proposal offers a unique perspective, combining a risk-based approach with a strong emphasis on protecting fundamental rights. A central innovation is the National System for the Regulation and Governance of Artificial Intelligence (SIA). This hybrid, tiered oversight model empowers both sectoral regulators and a central coordinator to ensure responsible AI development, seeking to strike a balance between traditional market-oriented regulation and robust safeguards for human rights.

A. Introduction

The regulation of artificial intelligence (AI) systems has become a focal point for regulators and policymakers across various jurisdictions. In the past twelve months, a notable surge in regulatory initiatives has occurred, exemplified by the Bletchley Declaration following the UK AI Safety Summit,[1] the comprehensive AI governance strategy outlined in Biden's Executive Order,[2] and the G7's statement on the Hiroshima process, endorsing

1 UK Government, 'The Bletchley Declaration by Countries Attending the AI Safety Summit' (2023) <https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023> accessed 22 January 2024.

2 The White House, 'Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence' <https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/> accessed 22 January 2024.

an AI 'Code of Conduct'.[3] Particularly noteworthy is the EU AI Act, a comprehensive legislative piece agreed upon in December 2023.[4] Common among these proposals are concerns about AI safety, rooted in the notion that inherent risks accompany the development and deployment of AI applications, emphasising the need for transparency and accountability. However, existing proposals diverge in their approach to identifying and prioritising risks, determining appropriate risk management systems, and striking a balance between preventing harms and fostering innovation—fundamental issues at the core of the ongoing regulatory debate.[5]

Analysing the diverse approaches employed by different jurisdictions in regulating AI is crucial for identifying common concerns and nuanced rule choices specific to each context. Legal analyses have primarily centred on single case studies – with a significant focus on the EU AI Act,[6] but also on the AI rules adopted in China[7] – examining the rules proposed and adopted, identifying potential limitations, and proposing avenues for improvement. Legal scholars have also discussed differences in regulatory strategies, examining how state-led command-and-control regulatory strategies con-

3 G7, 'G7 Leaders' Statement on the Hiroshima AI Process' (2023) <https://www.mofa.go.jp/ecm/ec/page5e_000076.html> accessed 22 January 2024.

4 References to the EU AI Act text in this chapter refers to European Parliament 'Corrigendum' of 16 April 2024, which is the latest version of the agreed text. EU AI Act final draft. Available at < https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138-FNL-COR01_EN.pdf> accessed 25 April 2024.

5 Christina Todorova and others, 'The European AI Tango: Balancing Regulation Innovation and Competitiveness', *Proceedings of the 2023 Conference on Human Centered Artificial Intelligence: Education and Practice* (ACM 2023) <https://dl.acm.org/doi/10.1145/3633083.3633161> accessed 23 January 2024; Michael Veale, Kira Matus and Robert Gorwa, 'AI and Global Governance: Modalities, Rationales, Tensions' (2023) 19 Annual Review of Law and Social Science 255.

6 See, for example, Irena Barkane, 'Questioning the EU Proposal for an Artificial Intelligence Act: The Need for Prohibitions and a Stricter Approach to Biometric Surveillancel' (2022) 27 Information Polity 147; Johann Laux, Sandra Wachter and Brent Mittelstadt, 'Trustworthy Artificial Intelligence and the European Union AI Act: On the Conflation of Trustworthiness and Acceptability of Risk' (2024) 18 Regulation & Governance 3; Rostam J Neuwirth, 'Prohibited Artificial Intelligence Practices in the Proposed EU Artificial Intelligence Act (AIA)' (2023) 48 Computer Law & Security Review 105798; Michael Veale and Frederik Zuiderveen Borgesius, 'Demystifying the Draft EU Artificial Intelligence Act — Analysing the Good, the Bad, and the Unclear Elements of the Proposed Approach' (2021) 22 Computer Law Review International 97.

7 See, for example, Huw Roberts and others, 'The Chinese Approach to Artificial Intelligence: An Analysis of Policy, Ethics, and Regulation' (2021) 36 AI & SOCIETY 59; Matt Sheehan, 'China's AI Regulations and How They Get Made' (2023) 24 Horizons.

trast with industry-led initiatives and the emergence of co-regulatory models.[8] While scholars have compared contrasting approaches to AI,[9] there are comparative fewer legal studies that contrast the concrete regulatory choices made by different jurisdictions.[10] Notably, there is limited legal analysis that considers proposals under discussion in countries in the Global South.[11] With the predominant focus on Global North jurisdictions in scholarly and regulatory discussions, there is a genuine risk that emerging frameworks may be skewed by the perspectives of more affluent nations.

This chapter aims to contribute to ongoing debates by scrutinising the Brazilian AI regulation proposal, a comprehensive bill that shares similarities with the EU AI Act but has garnered comparatively less attention. Bill No. 2338/2023, developed by a commission of legal experts, is currently under examination by the Brazilian Congress. This proposal aims to establish principles, rules, and guidelines for regulating the development and application of AI in the country. Contrary to notions of legal transplant or an example of the Brussels Effect,[12] we argue that the Brazilian bill positions

8 Christian Djeffal, Markus B Siewert and Stefan Wurster, 'Role of the State and Responsibility in Governing Artificial Intelligence: A Comparative Analysis of AI Strategies' (2022) 29 Journal of European Public Policy 1799; Kira JM Matus and Michael Veale, 'Certification Systems for Machine Learning: Lessons from Sustainability' (2022) 16 Regulation & Governance 177; Roger Clarke, 'Regulatory Alternatives for AI' (2019) 35 Computer Law & Security Review 398.

9 Djeffal, Siewert and Wurster (n 10); Emmie Hine and Luciano Floridi, 'Artificial Intelligence with American Values and Chinese Characteristics: A Comparative Analysis of American and Chinese Governmental AI Policies' [2022] AI & SOCIETY <https://link.springer.com/10.1007/s00146-022-01499-8> accessed 23 January 2024; Deborah Morgan, 'Anticipatory Regulatory Instruments for AI Systems: A Comparative Study of Regulatory Sandbox Schemes', *Proceedings of the 2023 AAAI/ACM Conference on AI, Ethics, and Society* (ACM 2023) <https://dl.acm.org/doi/10.1145/3600211.3604732> accessed 23 January 2024.

10 Jakob Mökander and others, 'The US Algorithmic Accountability Act of 2022 vs. The EU Artificial Intelligence Act: What Can They Learn from Each Other?' (2022) 32 Minds and Machines 751; Luca Nannini, Agathe Balayn and Adam Leon Smith, 'Explainability in AI Policies: A Critical Review of Communications, Reports, Regulations, and Standards in the EU, US, and UK', *2023 ACM Conference on Fairness, Accountability, and Transparency* (ACM 2023) <https://dl.acm.org/doi/10.1145/3593013.3594074> accessed 23 January 2024.

11 Marie-Therese Png, 'At the Tensions of South and North: Critical Roles of Global South Stakeholders in AI Governance', *2022 ACM Conference on Fairness, Accountability, and Transparency* (ACM 2022) <https://dl.acm.org/doi/10.1145/3531146.3533200> accessed 23 January 2024.

12 Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (Oxford University Press 2020).

the country on par with more developed economies, striving to carve out a distinctive path in AI regulation.

To contextualise this analysis, we begin by exploring the academic debate on policy diffusion and the role played by the EU. We then provide the background and rationale behind the EU AI Act, contrasting it with the ongoing legislative process of the Brazilian bill – where the proposal was originally drafted by a commission of legal experts formed in February 2022, specifically tasked with tailoring the proposal to address Brazil's challenges and opportunities in AI. After its introduction to Congress, the bill was examined by a special committee in the Brazilian Senate. In April 2024, rapporteur Senator Eduardo Gomes introduced a revised version (replacement bill). The subsequent section of the chapter examines the Brazilian revised proposal, focusing on its innovative institutional design. The analysis is structured around five pillars: principles, rights of individuals, risk assessments, obligations, and innovation. This examination aims to highlight the specific choices made within the Brazilian proposal to address critical debates surrounding AI regulation, and where it differs from the EU AI Act. The final section of the chapter then outlines the legislative steps ahead.

B. Drivers of policy diffusion and the Brussels effect

While various jurisdictions globally have grappled with developing AI rules, the EU AI Act distinguishes itself as one of the most comprehensive sets of proposed regulations yet – and one that has been under scrutiny for longer, since 2021. The EU is also regarded as a catalyst for policy diffusion, with its newest legislative initiative seen as seeking to establish a 'global standard' for AI governance [13] with the potential to exert worldwide influence through the Brussels Effect.[14] However, understanding the influence of the Brussels Effect on regulatory proposals – and in particular to how

13 Luca Bertuzzi and Oliver Noyan, 'Commission Yearns for Setting the Global Standard on Artificial Intelligence' *Euroactiv* (15 September 2021) <https://www.euractiv.com/section/digital/news/commission-yearns-for-setting-the-global-standard-on-artificial-intelligence/> accessed 22 January 2024.

14 Charlotte Siegmann and Markus Anderljung, 'The Brussels Effect and Artificial Intelligence: How EU Regulation Will Impact the Global AI Market' (arXiv, 2022) <https://arxiv.org/abs/2208.12645> accessed 22 January 2024.

it affects Global South countries like Brazil – requires examining in more detail the mechanisms of policy diffusion.[15]

The literature on policy diffusion delineates four primary mechanisms through which policies adopted in one jurisdiction spread to others: social construction facilitated by expert epistemic communities and international organisations, coercion involving powerful nation-states and international financial institutions leveraging sanctions or aid, competition where countries vie to attract investment and boost exports through business-friendly policies, and learning as countries draw lessons from their experiences and the policy experiments of their peers.[16] In the context of the European Union's role, Bradford's Brussels Effect provides an additional framework for understanding policy diffusion. This concept posits that the EU, leveraging its substantial market size and regulatory influence, can drive the global adoption of similar rules. Bradford contends that the EU can act as a significant global regulator, advancing its social preferences while ensuring the competitiveness of its companies on the global stage.[17]

An illustrative case study identified by Bradford is in the field of data protection. Around the 2010s, the European Commission explicitly acknowledged that promoting EU data privacy laws was as a benchmark for global standards and advocated for universal principles based on EU norms in various trade agreements.[18] With the enactment of the EU General Data Protection Regulation (GDPR), a comprehensive data protection law with extraterritorial commitments, Bradford argues that market players adapted their global business practices, leading other jurisdictions to develop similar rules to facilitate compliance. For instance, in Brazil, the Brazilian General Data Protection Law (LGPD – Law No. 13709/2018) is considered to have been heavily influenced by EU discussions on data protection and

15 Shu Li, Béatrice Schütte and Suvi Sankari, 'The Ongoing AI-Regulation Debate in the EU and Its Influence on the Emerging Economies: A New Case for the "Brussels Effect"?' in Mark Findlay, Li Min Ong and Wenxi Zhang (eds), *Elgar Companion to Regulating AI and Big Data in Emerging Economies* (Edward Elgar Publishing 2023) <https://www.elgaronline.com/view/book/9781785362408/chapter1.xml> accessed 22 January 2024.

16 Frank Dobbin, Beth Simmons and Geoffrey Garrett, 'The Global Diffusion of Public Policies: Social Construction, Coercion, Competition, or Learning?' (2007) 33 Annual Review of Sociology 449; Herbert Obinger, Carina Schmitt and Peter Starke, 'Policy Diffusion and Policy Transfer in Comparative Welfare State Research' (2013) 47 Social Policy & Administration 111.

17 Bradford (n 14).

18 ibid.

the text of the GDPR, with several provisions mirrored in both laws.[19] Notably, the diffusion effect is not merely mimicking; it depends not only on the adoption of rules by national policy but also on the market response to those rules. Bradford emphasises that the Brussels Effect arises from a combination of "bestowed market size, political decision-making, and market forces shaping corporate behaviour".[20]

In the domain of artificial intelligence, discussions often invoke the Brussels Effect to speculate on the potential diffusion of the model proposed in the EU AI Act. However, at this stage of policy development, a more accurate assertion is that the EU is contributing to debates, through learning mechanisms, rather than exhibiting a Brussels Effect. Learning processes significantly shape the information political actors have about policy instruments and effectiveness, with evidence showing that other countries' experiences can influence expectations regarding the costs and benefits of a specific policy reform [21]. As the following sections will demonstrate, the case of Brazil's draft legislation strongly supports the argument of policy diffusion through learning rather than the Brussels Effect.

C. Contextual background in the EU and Brazil

In the EU, the impetus for AI regulation can be traced back to 2019 when Ursula von der Leyen, the President of the European Commission, emphasised the need for new rules governing AI. In 2018, the European Commission established the High-Level Expert Group on Artificial Intelligence (AI HLEG) to provide strategic advice on the matter.[22] The AI HLEG offered insights into ethics, policy, and investment, sectoral considerations, and key requirements for AI development. The resultant white paper and the

19 Renan Gadoni Canaan, 'The Effects on Local Innovation Arising from Replicating the GDPR into the Brazilian General Data Protection Law' (2023) 12 Internet Policy Review <https://policyreview.info/articles/analysis/replicating-gdpr-into-brazilian-general-data-protection-law> accessed 22 January 2024.

20 Bradford (n 14).

21 Covadonga Meseguer, 'Policy Learning, Policy Diffusion, and the Making of a New Order' (2005) 598 The ANNALS of the American Academy of Political and Social Science 67; Covadonga Meseguer and Fabrizio Gilardi, 'What Is New in the Study of Policy Diffusion?' (2009) 16 Review of International Political Economy 527.

22 European Commission, 'High-Level Expert Group on Artificial Intelligence' (7 June 2022) <https://digital-strategy.ec.europa.eu/en/policies/expert-group-ai> accessed 22 January 2024.

updated Coordinated Plan on AI outlined a risk-based regulatory approach that was later developed into the formal legislative proposal introduced in April 2021, in the form of the proposed EU AI Act.[23] Since then, the text has been debated by the EU institutions, and a final text was agreed upon at the end of a trialogue on 8 December 2023, with the European Commission, the Council of the European Union, and the European Parliament reaching a political agreement on its wording and on 13 March 2024, the EU Parliament approved the text, and final draft of the text was made public.[24] At the time of writing, the Act was awaiting to be formally endorsed by the Council.

In Brazil, the need for AI regulation has grown in parallel with global discussions, emphasising indigenous perspectives linked to the widespread use of technology in one of the world's most economically unequal nations. Evidence shows that the impact of these technologies exacerbates existing disparities in income, race, gender, and territories.[25] Notably, predictive algorithms and facial recognition systems have led to wrongful arrests, with 90% of individuals arrested through facial recognition in Brazil in 2019 being from the Black population.[26]

Against this backdrop, a Commission of Jurists for the Drafting of the Brazilian AI Bill (CJUSBIA) was established by the Brazilian Senate in February 2022. The CJUSBIA sought to develop a more comprehensive approach than that proposed in previous bills – including Bills No. 5051/2019, No. 21/2020, and No. 872/2021 – which were deemed insufficient in addressing essential aspects of AI regulation. Led by Ricardo Villas Bôas

23 European Commission, 'White Paper on Artificial Intelligence: A European Approach to Excellence and Trust' (2020) <https://commission.europa.eu/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en> accessed 22 January 2024; European Commission, 'Coordinated Plan on Artificial Intelligence' (2022) <https://digital-strategy.ec.europa.eu/en/policies/plan-ai> accessed 22 January 2024.

24 European Parliament, 'Artificial Intelligence Act: MEPs Adopt Landmark Law' (13 March 2024) <https://www.europarl.europa.eu/news/en/press-room/20240308IPR19015/artificial-intelligence-act-meps-adopt-landmark-law> accessed 25 April 2024.

25 Ana Bottega and others, 'NPE 18: Quanto Fica Com as Mulheres Negras? Uma Análise Da Distribuição de Renda No Brasil' (Made centro de pesquisa em macroeconomia das desigualdades FEA/USP 2021) <https://madeusp.com.br/publicacoes/artigos/quanto-fica-com-as-mulheres-negras-uma-analise-da-distribuicao-de-renda-no-brasil/> accessed 22 January 2024; Laura Robinson and others, 'Digital Inequalities 2.0: Legacy Inequalities in the Information Age' [2020] First Monday <https://journals.uic.edu/ojs/index.php/fm/article/view/10842> accessed 23 January 2024.

26 Silvia Ramos, *Pele alvo: a bala não erra o negro* (CESec 2023).

Cueva, a Minister from the Superior Court of Justice (STJ), the CJUSBIA conducted public hearings and workshops to explore various topics related to AI regulation – engaging over 50 experts in the process.[27]

Through this consultative process, the commission aimed to gather views from different actors and develop a multisectoral perspective on AI regulation.[28] The discussions encompassed essential aspects such as defining the object of a future AI regulation, establishing foundational principles, incorporating socio-economic considerations, evaluating sectoral experiences, devising risk evaluation methodologies, preventing biases and discrimination, ensuring AI reliability, determining rights and duties, establishing civil liability regimes, devising institutional arrangements for enforcement, and formulating regulatory instruments for innovation. Apart from the public hearings, the CJUSBIA received 102 written contributions and organised an international seminar, involving perspectives from foreign experts.[29] The CJUSBIA then published a report and a draft regulatory proposal that formed the basis for Bill No. 2338/2023, presented to the Brazilian Senate in May 2023.[30]

In the Senate, a special committee examined the Bill alongside other legislative proposals on AI regulation and amendments from senators. The committee held public hearings, considering the perspectives of various stakeholders. This input informed the report by Rapporteur Senator Eduardo Gomes and the development of a revised bill, which was introduced in early 2024.[31] On December 20, 2024, the bill was approved by the Senate. The text must now be voted by the Chamber of Deputies.

The following section examines the structure and innovations of this revised text, now the central proposal for AI regulation in Brazil. It will

27 Brasil, 'Comissão de Juristas Responsável Por Subsidiar Elaboração de Substitutivo Sobre Inteligência Artificial No Brasil' (Brazilian Senate 2022) <https://legis.senado.leg.br/comissoes/comissao?codcol=2504>.

28 ibid.

29 ibid.

30 STJ, 'Projeto que Regula IA é Apresentado ao Senado Após Trabalho da Comissão Liderada Pelo Ministro Cueva' *Superior Tribunal de Justica* (Brasília, 2023) <https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2023/04052023-Projeto-que-regula-IA-e-apresentado-ao-Senado-apos-trabalho-da-comissao-liderada-pelo-ministro-Cueva.aspx>.

31 Agência Senado, 'Relator de Projeto que Regulamenta IA Quer Buscar Texto de Convergência' *Senado Federal* (1 November 2023) <https://www12.senado.leg.br/noticias/materias/2023/11/01/relator-de-projeto-que-regulamenta-ia-quer-buscar-texto-de-convergencia> accessed 22 January 2024.

discuss the bill's distinctive features and how Brazil aims to forge its own path in this domain.

D. The structure of the Brazilian bill

As the result of this process, the Brazilian AI regulation bill No. 2338/2023 adopts a multifaceted approach to AI regulation, combining a risk-based model with a distinctive emphasis on a rights-based framework. A key element is its innovative institutional design, establishing a hybrid, tiered oversight model with enforcement powers shared between sector regulators and a central coordinator. Specifically, the bill proposes a National System for the Regulation and Governance of Artificial Intelligence (SIA – *Sistema Nacional de Regulação e Governança de Inteligência Artificial*).[32] This system would be coordinated by an authority designated by the federal government. The rapporteur suggested the National Data Protection Authority (ANPD – *Autoridade Nacional de Proteção de Dados Pessoais*), could fulfil this role, but it would require strengthening and expansion.[33] The coordination authority would work alongside other Brazilian regulatory bodies, such as the Central Bank, the competition authority (CADE), and regulatory agencies including ANATEL (the telecommunications regulator), ANVISA (the health regulator), among others.

The SIA supervisory system is likely the hallmark of the Brazilian bill and aims to reconcile the existing market-oriented system with the protection of fundamental rights. In Brazil, sector regulators, with their expertise in overseeing specific sectors, are well-placed to intervene within their areas. However, their focus is primarily on market regulation, and they may have less expertise in protecting and enforcing fundamental rights, a key concern for the Brazilian bill. This gap would be addressed by empowering a central coordinator with more expertise in this area, such as the data protection authority.[34] Data protection authorities are naturally geared towards protecting individual rights. Therefore, this hybrid tiered model is seen

32 Art. 40, *Bill No. 2338/2023*.

33 Agência Senado, 'IA: Relator Apresenta Proposta Alinhada com Regulamentos da Europa e dos EUA' *Senado Federal* (24 April 2024) <https://www12.senado.leg.br/noticias/materias/2024/04/24/ia-relator-apresenta-proposta-alinhada-com-regulamentos-da-europa-e-dos-eua> accessed 11 May 2024.

34 If ANPD were assigned as the regulator, it would require significant investments in capacity and autonomy. For a discussion on the limitations of the ANPD in the current setting, see Beatriz Kira, 'Inter-Agency Coordination and Digital Platform

as essential to strike a balance between fostering innovation and safe AI development, while also protecting citizens and their fundamental rights. Crucially, this hybrid approach permeates the entire structure of the bill and informs the logic behind the five pillars we discuss in the next section.

I. The foundations of the proposal: scope, definitions, and principles

The first pillar of the bill encompasses the scope of the regulation, key definitions and fundamental principles that underpin its framework. The proposal aims to create norms for AI systems in Brazil, prioritising the protection of fundamental rights, fostering responsible innovation, and ensuring the implementation of safe and reliable systems. These systems should benefit individuals, the democratic regime, and economic, scientific, and technological development.[35] The bill defines AI systems as: "machine-based system that, with varying degrees of autonomy and for explicit or implicit objectives, infers from input data or information it receives, how to generate outputs, in particular, prediction, recommendation or decision that can influence the virtual or real environment".[36]

The proposal clearly outlines exceptions to the future law, setting forth that it will not apply to AI systems used by an individual for a non-economic private purpose, developed and used exclusively for national defence, testing, development and research activities that are not placed on the market, open and free standards and formats (with the exception of those considered high-risk or falling under the governance standards for foundational models and generative AI, addressed in a separate chapter).[37]

The Brazilian bill establishes a comprehensive set of principles that guide its framework.[38] These principles emphasise a commitment to inclusive

Regulation: Lessons from the Whatsapp Case in Brazil' [2024] International Review of Law, Computers & Technology 1.

35 Art. 1, Bill No. 2338/2023, replacement text introduced by Senator Eduardo Gomes on 24 April 2024 [hereinafter *Bill No. 2338/2023*].

36 Art. 4, I, *Bill No. 2338/2023*. This aligns with the OECD new definition describing an AI system as "machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments". OECD, 'Recommendation of the Council on Artificial Intelligence' <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449> accessed 22 January 2024.

37 Art. 1, sole paragraph, *Bill No. 2338/2023*.

38 Art. 2 and art. 3, *Bill No. 2338/2023*.

growth, sustainable development, and the overall well-being of society, including the protection of workers. They emphasise self-determination and the freedom of individuals to make informed choices. Human participation throughout the AI life cycle, coupled with effective supervision, underscores the importance of maintaining a human-centric approach. The principles address issues of non-discrimination, ensuring justice, fairness, and inclusion in AI systems. Transparency, explainability, and auditability are considered integral components of the proposed legislation, given the role they play in fostering trustworthiness and robustness in AI, along with a focus on information security.[39]

Notably, the Brazilian bill includes principles that are designed to protect individuals and grant them legal rights when they are affected by AI systems. Legal due process, contestability, and an adversarial character are highlighted to safeguard individual rights. Traceability of decisions aims at ensuring accountability and attributing liability to suppliers and operators. Additionally, provisions for reporting, accountability, and full damages compensation are set forth. The principles also encompass preventive measures, precautionary actions, and mitigation strategies to address systemic risks arising from intentional or non-intentional uses and unforeseeable effects of AI systems. Lastly, adherence to the principles of non-maleficence and proportionality underscores the importance of aligning AI methods with legitimate and determined purposes.

II. Granting rights to individuals and groups affected by AI systems

In Brazil, the foundation of any regulatory framework is rooted in the incorporation of constitutional rights, and this notion holds true for the proposed AI regulation. The bill places significant emphasis on establishing rights and responsibilities in response to the impact of artificial intelligence systems on individuals' lives, dedicating an entire chapter to this aspect. The bill guarantees three core rights for individuals and groups affected by AI systems:[40]

- *Right to prior information:* Individuals have the right to be informed in advance regarding their interactions with AI systems.

39 Brasil (n 29).
40 Art. 8, *Bill No. 2338/2023*.

- *Right to privacy and data protection:* Individuals are entitled to privacy and protection of personal data in accordance with relevant legislation.
- *Right to non-discrimination and correction of biases:* Individuals are protected against direct, indirect, illegal, or abusive discriminatory biases, and have the right to have biases corrected.

These rights are further strengthened in the context of high-risk AI systems. The overarching goal is to ensure a fair and comprehensive defence mechanisms, akin to an informational due process, for those whose rights and freedoms may be affected by decisions made by automated means. Therefore, individuals affected by high-risk AI systems would have the following additional rights:[41]

- *Right to explanation:* Individuals are entitled to an explanation of decisions, recommendations, or predictions made by AI systems.
- *Right to contest:* Individuals can contest decisions or predictions made by AI systems.
- *Right to human supervision:* The right to human intervention in decision-making processes is guaranteed, considering the context, technological advancements, and associated risks.

The bill grants individuals and groups affected by AI decisions the right to explanation and to request additional information, including:

- *System rationale and logic:* The reasons, logic, and anticipated consequences of decisions for the affected individual.
- *AI system's contribution:* The degree and level of the AI system's contribution to decision-making
- *Processed data details:* Information about processed data, its source, decision-making criteria, and relevant weighting applied.
- *Mechanisms for contestation:* Available processes for contesting decisions.
- *System rationale and logic:* The reasons, logic, and anticipated consequences of decisions for the affected individual.
- *Level of human supervision:* The level of human supervision and the possibility of requesting human intervention

Notably, many of the rights outlined in the proposed AI bill are not entirely new within the Brazilian legal framework. In fact, as observed by the Brazilian Data Protection Authority (ANPD), there is a connection be-

41 Art. 9, *Bill No. 2338/2023.*

tween these proposed rights and those already established in the LGPD.[42] Enacted in 2018, the LGPD governs personal data processing across various contexts, whether physical or digital, public or private.[43] The protection of rights outlined in the proposed AI bill aligns with the LGPD's emphasis on the right of access, as detailed in Article 9. This ensures individuals receive clear and comprehensive information about the processing of their personal data. Similarly, the right to contest and request a review in the proposed bill mirrors the right to review automated decisions outlined in Article 20 of the LGPD. These alignments highlight the importance of integrating AI regulation with existing data protection legislation. Furthermore, the close relationship between proposed AI rights and those overseen by the ANPD suggests the agency might be well-positioned to coordinate the bill's proposed supervisory system – SIA.

III. Levels of risks in AI systems: high-risk, excessive risks and general-purpose AI systems

The Brazilian bill employs a risk-based, asymmetric approach,[44] calibrating the legal obligations in response to the potential risks associated with the application of the technology. Similarly to the approach adopted in the EU AI Act, the Brazilian bill establishes certain general and specific obligations applicable to AI systems in proportion to the degree of risk they present. The highest risk categorisation operates with two distinct classifications that receive differentiated treatment throughout the proposed legislation: AI systems classified as "high risk" and those deemed "excessive risk". It falls upon the system provider, prior to market placement, to conduct a preliminary assessment for risk classification.

---

42 ANPD, 'Análise Preliminar Do Projeto de Lei Nº 2338/2023, que dispõe sobre o uso da Inteligência Artificial' (Autoridade Nacional de Proteção de Dados 2023) <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-analise-preliminar-do-projeto-de-lei-no-2338-2023-que-dispoe-sobre-o-uso-da-inteligencia-artificial> accessed 22 January 2024.

43 Miriam Wimmer, 'Foreword: Advancements and Challenges for Latin American AI and Data Governance' (2022) 47 Computer Law & Security Review 105759.

44 Marie-Anne Frison-Roche, 'Asymmetry: Asymmetric Regulation / Asymmetry of Information' (*The Journal of Regulation and Compliance*, 4 March 2024) <https://thejournalofregulation.com/en/article/asymetrie-regulation-asymetrique-asymetrie-dinform/> accessed 4 March 2024.

From a comparative perspective, in the original EU Commission's proposal of the EU AI Act, AI systems were considered high-risk if: i) the AI system is intended to be used as a safety component of a product, or is itself a product, covered by the Union harmonisation legislation listed in Annex II *and* pursuant to that legal framework it is required to undergo a third-party conformity assessment to be placed on the market[45]; ii) the AI system is one of the kind referred to in Annex III (i.e., biometric identification and categorisation of natural persons; management and operation of critical infrastructure; education and vocational training; employment, workers management and access to self-employment; etc.).[46] However, during the trialogue negotiations, the Commission proposal's classification rules for high-risk AI systems were amended significantly. The agreed text introduces a derogation from the general rule that AI systems referred to in Annex III shall be considered high-risk: if systems do not pose a significant risk of harm, to the health, safety or fundamental rights of natural persons, and if they do not perform profiling of natural persons, they shall not be considered high-risk.[47] This approach, however, has inherent complexities. While it strives to strike a delicate balance between industry autonomy and the need for effective oversight in the rapidly evolving AI landscape, assigning risk categories presents inherent challenges.

The Brazilian AI bill acknowledges this challenge and recognises that a one-size-fits-all approach might not work. Instead, it adopts a more flexible system. The legislation provides a base risk classification for different AI applications, encompassing areas like security, critical infrastructure (like water and electricity), education, recruitment, autonomous vehicles, healthcare, and criminal justice, among others.[48] However, it empowers enforcement agencies, working alongside the Supervisory System, to adjust the risk

45 Art. 6(1) AI Act.

46 Art. 6(2) AI Act.

47 Art. 6(2a) AI Act, Draft Agreement. The new derogation contains an assessment of instances where AI systems do not pose significant risks of harm to fundamental goods, that is, when the AI system is intended to: a) perform a narrow procedural task; b) improve the result of a previously completed human activity; c) detect decision-making patterns and is not meant to replace or influence the previously completed human assessment without proper human review; d) perform a preparatory task to an assessment relevant for the purpose of Annex III uses cases.

48 Art. 53, *Bill No. 2338/2023*.

classification based on specific cases. The SIA also retains the authority to update the entire list of AI systems altogether.[49]

Moreover, the Brazilian bill enumerates situations constituting "excessive risks", where the use of technology is prohibited due to the involvement of non-negotiable rights. These scenarios involve the use of AI that could be harmful to security, physical safety, and ultimately, a person's right to self-determination. The bill mentions systems employing subliminal techniques, those exploiting human vulnerabilities, the controversial practice of social scoring that assigns universal rankings for access to goods, services, and public policies, AI used to generate child sexual exploitation material, predicting crime or recidivism risk, and the development of autonomous weapons.[50] Furthermore, continuous, remote, and publicly accessible biometric identification systems, deemed highly perilous in multiple committee contributions, necessitate specific federal legislation adhering to the proposed requirements.[51]

IV. Obligations

The fourth pillar of the proposed bill revolves around AI governance measures, encompassing a range of obligations of due diligence and internal processes to be adopted by agents providing or operating AI systems. General measures include transparency measures about the use of artificial systems in interaction with natural persons and data management obligations to prevent discriminatory bias.[52]

The Brazilian bill imposes stricter requirements on high-risk AI systems. These systems must conduct a risk assessment and maintain a continuously updated record of it, subject to reassessment by the Supervisory System.[53] In addition, high-risk systems are subject to a range of additional governance measures. These include appointing dedicated officer responsible for overseeing compliance with regulations; documentation that outlines the system's operation, design decisions, implementation details, and usage throughout its lifecycle; the use of tools for automatic recording of system

49 Art. 16, *Bill No. 2338/2023*.
50 Art. 13, *Bill No. 2338/2023*.
51 Art. 14, *Bill No. 2338/2023*.
52 Art. 17, *Bill No. 2338/2023*.
53 Art. 12 and art. 22, *Bill No. 2338/2023*.

operations; and conducting performance tests evaluating reliability based on the sector and application type. These tests encompass robustness, accuracy, precision, and coverage. The bill also requires high-risk AI systems to adopt data management measures to mitigate and prevent discriminatory biases, and technical measures must be in place to facilitate the explainability of AI system results.[54]

Additionally, when an AI system generates synthetic content, the content itself, considering the state of the art in technological advancements, should include a clear and reliable identifier. This identifier would facilitate verification of authenticity, provenance, and any modifications or transmissions the content may undergo.[55] This concern with authenticity is particularly important in light of concerns around the risks AI can pose to political processes, and debates around how to mitigate them.[56]

Furthermore, the Brazilian bill imposes additional requirements on public entities that deploy high-risk AI systems. Before implementation, these entities must conduct a public consultation to gather feedback on the system's purpose and potential impacts, particularly on vulnerable populations. Additionally, clear protocols for data access need to be established, along with a registry that logs who accessed the system and for what purpose. The bill further emphasises the protection of the rights of individuals affected by the system, including the right to explanation and review of decisions made by the AI. To promote interoperability and transparency, the use of APIs or other interfaces is encouraged. Finally, public entities must disclose information about the AI systems they use, along with their corresponding risk assessments, on official government websites.[57]

The Brazilian bill recognizes the unique challenges posed by foundational AI models, including Large Language Models (LLMs). Due to the difficulty of pre-identifying their risk levels, these models are subject to a specific regulatory framework. The bill requires developers of general-purpose foundational AI models to fulfil several objectives before market release or use. These include conducting thorough testing and analysis to identify and mitigate "reasonably foreseeable" risks to fundamental rights, the en-

54 Art. 18, *Bill No. 2338/2023*.

55 Art. 19, *Bill No. 2338/2023*.

56 Danielle Allen and E Glen Weyl, 'The Real Dangers of Generative AI' (2024) 35 Journal of Democracy 147; Sarah Kreps and Doug Kriner, 'How AI Threatens Democracy' (2023) 34 Journal of Democracy 122.

57 Art. 21, *Bill No. 2338/2023*.

vironment, democratic processes, and the spread of disinformation, hate speech, and violence. Unmitigable risks must be documented. In addition, these models can only process and incorporate data only in accordance with data governance and data protection laws. Furthermore, they must adhere to sustainability standards that minimise energy consumption and resource use while promoting energy efficiency during model development. Crucially, the bill mandates the registration of all foundational models in a government-regulated database and developers are required to retain model-related documentation for ten years to facilitate oversight by relevant authorities.[58]

V. Fostering innovation

The fifth pillar of the bill focuses on supporting technological innovation and development in AI. This includes mandating public sector investment in R&D (Research and Development) and resource allocation for AI system development.[59] In a unique move to promote cultural creation and innovation, the Brazilian bill integrates copyright protection measures within its framework. This stems from the recognition of two key issues. The first is the critical role of input data and information for AI systems. The second is the potential tension between this use and the rights of content creators whose work feeds these systems, in light of the fact that Brazil's copyright legislation, from 1998, is probably unfit to effectively protect copyright holders in the context of AI systems.

As such, the Brazilian bill strives to strike a balance between fostering innovation and protecting copyright. To achieve this, it requires the provider of AI systems that utilise content protected by copyright to disclose which content was used to train the AI system.[60] The bill acknowledges fair use exceptions for legitimate data processing activities, such as research, journalism, archives, libraries, and educational purposes.[61] In most circumstances, the bill grants copyright holders the right to opt out of having their work used to train AI systems.[62] This empowers creators to control how

58 Art. 29, *Bill No. 2338/2023*.
59 Art. 50, *Bill No. 2338/2023*.
60 Art. 53, *Bill No. 2338/2023*.
61 Art. 54, *Bill No. 2338/2023*.
62 Art. 55, *Bill No. 2338/2023*.

their content is used. Additionally, the bill protects copyright holders from discrimination if they choose to opt out, framing such actions as a violation of Brazilian competition law.[63]

A crucial topic of discussion in the AI and copyright debate is whether the copyright holder should have a right to compensation when their creation is used to train AI systems.[64] The bill does not settle this debate but establishes that the SIA will establish a regulatory sandbox to test solutions on how AI systems could fairly remunerate artists and copyright holders.[65]

E. Conclusion

In conclusion, with the continuous expansion of AI technologies, governments worldwide are actively pursuing regulatory measures to address the varied implications of AI applications across diverse sectors. The Brazilian AI Bill No. 2338/2023 serves as an example of such regulatory efforts, embodying a risk-based and rights-oriented approach. While subject to amendments, the revised text of bill discussed in this chapter enjoys broad support across government, industry, academia, and civil society. This legislative initiative underscores Brazil's endeavour to strike a delicate balance between safeguarding individuals and institutions, promoting innovation, and reaping the advantages of AI, all while taking into account the specific concerns of the Brazilian context.

Notably, the Brazilian bill goes beyond mirroring the EU AI Act. It offers a novel framework that combines hard and soft law instruments, substantive and procedural rules, and overarching principles. A key differentiator is its proposal for a multi-tiered governance system. The Supervisory System for Artificial Intelligence empowers existing regulators while establishing a coordinating body, likely the data protection authority. This ensures safe AI development that fosters economic growth and innovation, but crucially, prioritizes fundamental rights as enshrined in the Brazilian Constitution. The Brazilian AI Bill, therefore, offers a valuable model for other nations seeking to navigate the complex landscape of AI regulation. Its emphasis on

63 Art. 56, *Bill No. 2338/2023*.

64 See Andres Guadamuz, 'A Scanner Darkly: Copyright Liability and Exceptions in Artificial Intelligence Inputs and Outputs' (2024) 73 GRUR International 111.

65 Art. 57, *Bill No. 2338/2023*.

balancing innovation, rights, and safety could serve as a blueprint for AI regulation in jurisdictions with similar legal and institutional context.

Digital Constitutionalism in the States-as-Information-Platforms Context: A New Programme, the Acknowledgement of 'Platform Rights'

Vagelis Papakonstantinou

Abstract: Constitutions (much more, constitutionalism) touch upon each and every aspect of human life, hence unavoidably a brief text about such broad, and central, topics as constitutions, the state, individuals and human rights either has to be laser-focused, and thus lack breadth, or attempt a helicopter view, and thus lack depth. This text, for better or worse, subscribes to the latter category. Specifically, a new approach to all of these topics will be attempted, based on the fundamental premise that states are, and always have been, information platforms for their citizens. It is under this viewpoint and within this context that the following analysis unfolds. Its overarching idea is the juxtaposition of the analogue and the digital worlds, in sections 1 and 2 respectively, in order to address the age-old question of natural rights (Do they exist? Are human rights natural or given to humans?) in the digital world – therefore, within a digital constitutionalism context. As it will be explained in section 3, certain "platform rights" are indeed natural to individuals on the information platforms that are their states.

A. Introduction

Constitutions (or rather, constitutionalism) touch upon each and every aspect of human life. Hence, any brief text about such broad and central topics as constitutions, the state, individuals and human rights either has to be laser-focused, and thus lack breadth, or needs to attempt a helicopter view, and thus lack depth. This text, for better or worse, falls into to the latter category. Specifically, it attempts to take a new approach to all these

topics, based on the fundamental premise that states are, and always have been, information platforms for their citizens.[1]

It is from this viewpoint and within this context that the following analysis unfolds. It juxtaposes the analogue and the digital worlds, in Sections B and C respectively, in order to address the age-old questions of natural rights (Do they exist? Are human rights natural or given to humans?) in the digital world—that is, within a digital constitutionalism context. As will be explained in Section D, certain 'platform rights' are indeed natural to the information platforms that are states.

B. The analogue world

Digital technologies have made a new perspective possible. The analogue world, the natural world as we know it, that we as humans live in and have lived in since we first appeared on the planet, can now be seen through a different lens, that of information processing. Old assumptions need to be reassessed and new ideas, among others, regarding the state and its definition or individuals and their rights, can now be attempted. Specifically, the state is an obvious point of departure for this analysis, with constitutionalism being intrinsically connected to it, as will be seen in Section B.III.

I. The state is, and always has been, an information platform for its citizens

States are, and always have been, nothing more than information platforms for their citizens. They are information-processing infrastructures, human fictions that have materialised in the analogue world. This definition applies as much today, when the analogue world is being challenged by the digital one, as in the depths of human history, when the first states emerged.

States are information platforms for their citizens in the sense that they (co-)create, store and disseminate information for them. How do they do this? The relevant mechanism is so common that it is easily overlooked. Immediately at birth every human is given a name. While it may be the

1 Within the context of a new political philosophy of information, see Vagelis Papakonstantinou, "States as Information Platforms: A Political Theory of Information," in *Data Protection and Privacy, Volume 16: Ideas That Drive Our Digital World*, ed. Hideyuki Matsumi et al. (London: Bloomsbury Publishing, 2024).

parents that do the name-giving, it is actually the state into which the human was born that makes this name possible. A name is useless without a state to guarantee it, tacitly, each time one human communicates with another. At the same time, meaning at birth, every human is provided with a citizenship: the state that guarantees the name also bestows its citizenship on that same human. The state is therefore an individualisation mechanism, the only one known to humans since they first appeared on the planet (or, at least, since they developed language). In essence, states turn humans into individuals, uniquely identifiable across space and time.

Once this has been done, whenever any two individuals communicate a third, silent, interlocutor is implied. This is the state, and it enables their communication. The state warrants that A is A and B is B, so as for A and B to be able to communicate. Unless this guarantee is given, there is no way for these two individuals to be certain that the other party is actually who it claims to be, and thus to communicate. It is the silent, ever-present third party, the state, that enables this, and thus makes any human contact, possible. Only in this way can humans live a meaningful life (at least, as we know it, separately from animals or God, neither of which have ever needed a state).

This definition of states as being information platforms for their citizens applies as much today as in the distant past of human existence. States therefore formed naturally, automatically and immediately at the moment when two humans started to communicate. States are natural to humans. They are not artificial constructs; they are not the result of agreements (as most prominently claimed by Social Contract theory)[2] or of human rational thinking in the form of choosing among many alternatives.

Subsequently this individualisation information is enriched, depending on the state, the period in human history and, of course, the individual him or herself. Family life, property ownership, education, health and professional life are all pieces of information that are co-created and processed for individuals by the information platform that is their state. Individuals,

2 There is, of course, a vast bibliography on the Social Contract theory, that started, schematically, with the works of Hobbes, Locke and Rousseau and continues to this day, for example with the works of Rawls; indicatively, see Christopher W. Morris, ed., *The social contract theorists: Critical essays on Hobbes, Locke, and Rousseau* (Oxford: Rowman & Littlefield, 1999); David Boucher and Paul Kelly, eds., *The social contract from Hobbes to Rawls* (London and New York: Routledge, 1994 (2005)); Peter J. Steinberger, "Hobbes, Rousseau and the Modern Conception of the State," *The Journal of Politics* 70, no. 3 (2008).

to live a meaningful life, need their states to keep this information safely stored for the term of their lives and authoritatively transmittable to any third party they so choose. Should the state not be able to carry out these actions, or should this information be lost or tampered with or not be available to use for interaction with others, individuals will not only be unable to live a meaningful life but will also face a serious risk to their survival.

However, states are not only personal-information processing infrastructures—hence the use of the term 'platform' to define them. States make understanding the analogue world possible for their citizens. It is states that create language (i.e. the names of the things around them), metrics, money, and all the other human mechanisms and conventions that have been devised to help citizens to understand, and control, their analogue-world environment. Through their use, the information processing necessary for meaningful human life is possible. As such, each state is different to and distinguishable from other states: they are essentially platforms, in the literal or metaphorical meaning, on which people, or things, can stand. Using states as information platforms, individuals can process information pertaining to other individuals and things, share beliefs and ideas, and live under common rules (laws).

How do states accomplish all this? Basically, through control of any and all information processing that takes place on their platforms. States have access to, and therefore potential control over, any and all information they co-create with their citizens and which they safely store and authoritatively transmit for them. In the analogue world control is exercised through well-known means: in essence, any professional activity, any change in family life, any academic accreditation, any travel or relocation of citizens, as well as most of their health management, requires one type or another of state involvement. This applies as much today as thousands of years ago, when the first humans emerged—it is only the volume of information that differs, which varies depending on the moment in time and the location of the state concerned. Otherwise, the state has complete control, through its necessary involvement, of all information processing on its platform; that is, the state has never been questioned or challenged in the analogue world—until today.

II. Individuals, individualisation and individualism

If states are information platforms for their citizens, humans are information-processing entities ('informational beings') that can and will process information on their respective platforms (i.e. their states) whenever the opportunity arises. In fact, the analogue world can be viewed as a (closed, in the sense that the information on it is finite) system of information, whereby human life is the sum of our information processing.

What is unique, however, to humans is the need to augment their information processing. Humans have a constant need to process new information, and this augments their information processing both quantitatively and qualitatively. New information leads to the development of new processing tools, which in turn make further new information processing possible, in an endless virtuous cycle. From the time when our ancestors drew on the walls of caves and improved their food gathering skills to the Greco-Roman age, the Renaissance and the Industrial Revolution, humans have basically always been trying, and succeeding, to constantly increase their information processing abilities and to keep processing new information. In essence, human history (and culture) has been caused by (and is best viewed as) a continuous increase in the information processing carried out by humans.

However, humans process information individually—not collectively, as would be the case, for example, with units in a hive. It is each one of us separately who needs to increase his/her own information processing (one cannot hope to process all the information on the planet). It is not in human nature to be absorbed into a single all-encompassing entity, blindly and anonymously contributing to an overall processing increase, but to practice this individually—regardless of the fact that the sum of individual processing achieves the increase of humanity's overall processing capacity anyway. Human individualisation is only achievable through states. It is only through the individualisation mechanism seen above (through the granting of a name and citizenship) that humans become individuals, uniquely identifiable in space and time, and thus able to exponentially increase their individual information-processing capacity.

The above demonstrates how humans, separate from and different to any other animal (or, God), became individuals. This process of individualisation, which is natural to humans, ought not to be confused with individualism and individuality. These concepts reflect a specific political

philosophy that was developed in (Western) Antiquity[3] and which is very much alive today, underpinning modern life. Notwithstanding differences in approaches that can at times be significant, both notions build on a fundamental theoretical dichotomy: an individual is composed of a private and a public sphere, a private and a public self. The public self is external, and thus needs to remain flexible so as to conform and comply with societal, political or other circumstances. In contrast, the inner self is internal, private and personal and, to a larger or smaller extent, inalienable, and thus needs to be protected and safeguarded. Acknowledgement of these two selves, and the exact relationship between them, more or less delineates much of political philosophy (and religion) and is the cornerstone of modern thinking and politics.

Nevertheless, if seen from the point of view of the information platform that is the state, this dichotomy, basically, does not exist. This is because states, as seen in Section B.I, have access to and exercise control over any and all information processing taking place on their platforms. The state is, in fact, omnipresent. To the state there is no private and public sphere of individuals—there is only the information processing of humans and the things that exist on its platform. The state is the necessary party to all information processing carried out by its citizens, be the information external or internal (the latter being processed as soon as it materialises in the analogue world). Or, in other words, the state knows all and can control everything anyway. It cannot *not* do so, being an indispensable part of the information creation and processing of each and every individual living on the platform.

Consequently, individualism and individuality are little other than the externally imposed exercise of restraint by the state. Or to be clearer, they are political theories under which the state, although having access to and potential control over all information and information processing on its platform, accepts restrictions on its own processing.[4] The state is told which information to pretend to ignore, to abstain from further processing or to continue processing but only at a minimal level. However, seen in this way, the artificiality of this assumption becomes obvious: any such restrictions

3 Broadly, since the time of Plato and Aristotle; before them, even within democratic Ancient Greek city-states, unity of the citizen with his/her city was the norm, an idea not far removed from that of contemporary theocratic and absolutist political systems.

4 That is, the processing carried out by the government, which controls the state, and not the state itself, it (the state) being merely a (passive) information platform, a processing infrastructure.

imposed by a political system are not natural to the information platform that is the state, but are introduced ('posited') by a specific political philosophy. How this affects human rights and constitutionalism in the broader sense will be seen in the subsequent section.

III. Human rights, constitutions and constitutionalism

If states are information platforms for their citizens and individuals wish to constantly process new information, some rules for this processing are necessary. How these rules are established (whether by nature, revealed by God or agreed in written law), how elaborate or otherwise they are, and how permissive or restrictive they are for some or all individuals, are all questions that are crucial and have preoccupied humanity since its appearance on the planet. However, the content of these rules should, for a moment, be put aside in order to pay attention to the fact of the existence of the rules per se. There is no information processing going on the platform that is the state that is not subject to rules. Rules for processing, in other words, are natural on the information platform that is the state. These rules regulate all information processing on the platform, meaning that they specify whether a particular form of processing is allowed to take place, by whom and under which conditions.

Having established the existence of rules, we can now turn our focus to their emergence. How are these rules created? Notwithstanding their exact form each time (meaning whether they are written or perceived), these rules are either invented by humans, for whatever reason, or are inherent on the platform that is the state. The former, meaning the invented rules, can take (and have taken, throughout human history) any direction: they can be more or less equal for all citizens, more or less fair, more or less liberal, and so on. They can be stated in writing, as in laws, or perceived, as in the case of customs. They can be as elaborate and detailed as they are in modern states, or as basic as the Code of Hammurabi.

Not all rules are invented, however: a few are inherent on the information platform that is the state. For example, because all humans receive a name and a citizenship at birth, all humans are born equal with regard to their state. Also, because all humans are born equal in their state, all are born free from the control of other humans in their state. In addition, because states need to keep the information on their citizens safely stored

and protected for the term of their lives (humans being informational beings), security of the person is inherent on the information platform that is the state. In other words, these rules are natural in states-as-information-platforms, they are the 'platform(-born) rights' given to all individualised humans, notwithstanding whether any given state at any given time in human history has acknowledged them. Such platform rights, although they are born naturally of the platform that is the state (and remembering that the state is itself natural to humans), ought not be confused with 'natural rights' within the positive and natural human rights dichotomy. Natural rights, 'that may be appealed to whether or not embodied in the law of any community'[5] are the result of one or another type of human reasoning ('practical reasonableness' in Finnis's words)[6] that nevertheless cannot be taken for granted over the long and extremely varied haul of human history and culture.

In modern states acknowledgement of the rules applicable to information processing on the platform is made formally and in writing through the legal system, at the top of which stands the constitution.[7] Although the role and content of modern constitutions remains contested,[8] acknowledgement in their text of the rights afforded to their citizens is an integral part common to all. Importantly, however, as noted above, platform rights are not necessarily acknowledged in constitutions—a state may well ignore them within its political system, as has frequently been the case throughout human history. It is therefore up to constitution-drafting, or, constitutionalism, to deal with them or not, as the case may be.

Constitutionalism and constitutions have triumphed in the modern world, there being practically no state today that does not have a constitution, but their triumph cannot hide their temporality. Constitutions are a relatively recent phenomenon in human history, being only a few hundred years old. As such, constitutionalism remains a contested term. Specifically, it is still unclear whether the term is connected to all constitution-drafting[9]

5 See John Finnis, *Natural law and natural rights* (Oxford: Oxford University Press, 2011), 199.

6 Finnis, *Natural law and natural rights*, 100ff.

7 See Hans Kelsen, *General Theory of Law and State* (New Brunswick (USA) and London (UK): Transaction Publishers, 1945 (2006)), 115.

8 See, for example, Nicholas William Barber, *The constitutional state* (Oxford: Oxford University Press, 2010), 75ff.

9 See, for example, Barber, *The constitutional state*, xiii.

or only to constitutions that limit the power of the state.[10] The latter form of constitutionalism is ultimately connected to the existence of a democratic and liberal state, one that includes among its foundational values democracy, the protection of human rights and the upholding of the rule of law.[11] If this is the case, however, then constitutionalism in the analogue world is basically the implementation of liberal and democratic political theory in state practice—complete with the artificial assumptions seen above (in Sections B.I and B.II) of individuals' public and private selves, or the existence of a social contract to justify state formation. This being the triumphant, dominant model in the analogue world today, it is perhaps of little practical use to contest it and showcase its limitations through a political philosophy of information—after all, it may well be that the digital world, and digital constitutionalism, will do this anyway.

C. The digital world

The digital world is something new and unprecedented for humanity, a transformational and revolutionary development that can only be compared with the invention of writing. All the assumptions that humans have been living with for the thousands of years of their recorded history in the analogue world, all of our beliefs and ideas need to be reassessed in view of the entirely new reality that has reached us, broadly speaking, at the turn of the twenty-first century. This is not simply a matter of an Information Revolution following the Industrial Revolution, it is not simply the development of new tools that will enable humanity to reach its imaginable objectives. It is the creation of an entirely new world, an entirely different reality that humans never imagined was available—and are still struggling to come to terms with.

As such, the emergence of the digital world can be viewed as the fourth of the milestone moments in humanity's development so far. The first one is only conceptual, it occurred when humans started talking to each other

10 See, for example, Richard S Kay, "American constitutionalism," in *Constitutionalism: Philosophical Foundations*, ed. Alexander Larry, Cambridge Studies in Philosophy and Law (Cambridge: Cambridge University Press, 1998), 16; Scott Gordon, *Controlling the state: Constitutionalism from ancient Athens to today* (Cambridge, Massachusetts: Harvard University Press, 1999), 5; Dieter Grimm, *Constitutionalism: Past, Present, and Future* (Oxford: Oxford University Press, 2016), 61.

11 See Edoardo Celeste, "Digital constitutionalism: A new systematic theorisation," *International Review of Law, Computers & Technology* 33, no. 1 (2019): 12.

using language and acquired self-consciousness; the second occurred when humans developed agriculture, some 10,000 years ago; the third occurred when writing was invented, some 5,000 years ago. We can, schematically, place the fourth one, the emergence of the digital world, around the year 2000.

I. A world without states

Completely in contrast with the analogue world that is,[12] and always has been, state-organised, there are no states in the digital world. The digital world was created from scratch by private, public and semi-public actors who did not care to transpose into the digital world the state organisation already known to them from the analogue world. On the contrary, there was a time, during the early years of the Internet, when the new digital world was imagined specifically as being a non-state one.[13] States, too, kept away from the development of the digital world, and even today focus on the regulation of large actors in the field (gatekeepers)[14] the protection of specific state organisations (critical infrastructures)[15] and the use of the digital world for the improvement of services to their citizens (e-government), rather than, so far at least, as a space for the exercise of state authority and power.

This completely overturns the analogue-world model known to humanity until now. Not only have humans always been connected to states, states being natural to them, but states have also always exercised control over information processing on their platforms—something that is no longer possible in the digital world. As seen in Section B.I, in the analogue world states control any and all information processing taking place on their

12 See, for example, Morris' "We live in a world of states" Christopher W Morris, *An essay on the modern state* (Cambridge University Press, 2002).

13 See, for example, John Perry Barlow, "A Declaration of the Independence of Cyberspace," *Duke Law & Technology Review* 18 (1996 (2019)).

14 See, for example, EU's DMA (Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act)).

15 See, for example, EU's NIS2 Directive (Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)).

platforms, being the necessary, implied, third party in all information processing regarding their citizens' professional and family lives, academic and vocational achievements, travel and so on. However, this is no longer the case in the digital world. Today an individual may reside physically in a state but study and work in the digital world, without the individual's state participation in or even awareness of the relevant information flows.

This fundamental change can be clearly illustrated through reference to Leviathan, the modern state's iconic concretisation in Hobbes's monumental book.[16] On its well-known frontispiece, the state is depicted as a giant completely dominating the scene. The citizens composing the giant have their backs to the viewer, facing Leviathan itself, because they can see (and process information) only through it. This is no longer the case: today citizens can look outwards, to the digital world, without Leviathan even being aware of it—much less dominating it too.

As such, this development is unprecedented in humanity's history. If a parallel had to be found with anything even remotely similar in the past, it could perhaps be the period of the existence of company-states, the workaround that Western states used in the seventeenth century to colonise Asia and the Americas. Because colonisation required efforts that greatly surpassed states' (processing) capacity at the time, the task was outsourced to private companies—but control of the colonies was immediately recovered by the relevant state as soon as its capacity had increased sufficiently.[17] It could therefore be the case that ours is an intermediate period during which states are allowing private parties to 'colonise' a new world, the digital world, about which for the moment they (the states) know and can do very little—with the relevant powers over this world to be recovered as soon as this situation changes. Whatever the case may be, the fact remains that for the first time ever individuals are able to live (even part of) their lives outside the gaze and control of their state.

16 Thomas Hobbes, *Leviathan*, ed. Christopher Brooke (London: Penguin, 1651 (2017)).

17 On the topic of company-states see, indicatively, Philip J Stern, *The company-state: corporate sovereignty and the early modern foundations of the British empire in India* (Oxford: Oxford University Press, 2011); Andrew Phillips and Jason Campbell Sharman, *Outsourcing empire: How company-states made the modern world* (Princeton and Oxford: Princeton University Press, 2020).

II. A world without individuals

The analogue-world notion of an individual safe is not safe in the digital world either. In effect, no current idea or concept of individuals or individuality remains unchallenged. The first to be attacked is the notion of individuality, specifically human uniqueness. In the analogue world the only conscious actors are humans. Information is, of course, also processed by other animals (all life being information processing), but actions that significantly affect the natural world are carried out exclusively by humans—including the organisations created and run by them. This is no longer the case in the digital world. In it, actions (information processing) may also be carried out by artificial informational beings (e.g. software agents) that may have been created by humans but from some point on act on their own. A robot automatically indexing webpages or a computer virus (not to mention artificial intelligence software) may have been created by humans to carry out a preset range of activities, but the fact remains that even within these strictly defined boundaries these informational beings process information and act on their own initiative. In other words, in the digital world humans are not the only beings processing information. Whether their distinctive characteristic, of constantly increasing their information processing, retains its validity in a world containing artificial informational beings (similarly to the situation of animals versus humans in the analogue world) remains to be seen.

The second notion to be challenged is individual unity, and thus accountability. In the analogue world a human becomes an individual through the authority of his or her state and this individual is who he or she remains for the rest of his or her life. Although an individual may change his or her natural or psychological traits or even name and citizenship, a trail will always lead, and refer to uniquely, to that single initial identity. Generally speaking, only actors and other small circles of individuals (e.g. priests) are likely to change their identity, but usually for very specific purposes and in situations that are only applicable to a specific circle of people. This is no longer the case in the digital world, where anonymity is (for the moment, at least) not only possible for everybody but having multiple identities is encouraged. This change, other than its psychological and societal repercussions, which we are still trying to come to terms with, also affects traditional and fundamental legal notions such as accountability. For example, at what point are digital identities bound to an individual? Is

crime, and its damages, assessable in the digital world similarly to how it is assessed in the analogue world?

What is more, the traditional dichotomy of an individual's private and personal life is also challenged in the digital world. As seen in Section B.II, in the analogue world, philosophy and religion have for centuries worked on the assumption that an individual has an inner, personal and private self and an external, social one, each of them living different lives and following different rules. However, this distinction was made possible by (if not developed because of) externalities: a number of external circumstances that alluded to and signalled a private life, for example, a home, closed doors, reading in silence, meditation and so on. In other words, because humans behave externally in a specific way (i.e. they 'hide' in their homes, close the doors to their rooms, read in silence (at least once books became widely available), find refuge in temples etc.), it was possible to create and apply a theory on the above dichotomy. However, in the digital world these externalities no longer exist—or, to put it better, new and unprecedented externalities that replace them are being released every day. In addition, the notions of both 'public' and 'private' are being irretrievably eroded in the digital world. As regards the 'private', the externalities that created commonly accepted boundaries in the analogue world are now long gone: in practice each individual is given control over what is considered private (information) but is left to decide him or herself whether, when and how to share (i.e. to give consent)[18] or not, thus blurring the common understanding of the term. Finally, what was considered 'public' in the analogue world, meaning in most cases information shared among a closed circle of people and a short life expectancy for the information concerned (printed on paper, at best), has now been transformed into global access for (digitised) perpetuity.

III. A world without finite information

Even more important than the erosion of the traditional notions of the state and individuals, however, is the transformation of information processing itself in the digital world. Specifically, in the analogue world information

18 It should not be forgotten that (data) privacy laws did not emerge until the 1970s and only then due the advent of information technology, even though they regulate an issue that has troubled humans since they first appeared on earth.

is finite, whereas in the digital world it is infinite. In the analogue world, the natural world around us, there is a limited number of things (be they artefacts or natural resources) that humans can process information about. In other words, there is a finite number of cars, houses, tables and chairs, televisions, but also plots of land, fruit, minerals and so on, on the planet. In essence, the analogue world is a closed system of information with a fixed, preset number of processing operations possible (with exactly how many being dependent on the moment in time and the specific state in question).

This is a fundamental, basic understanding in contemporary philosophy, religion and human existence. Within a closed system of information, the processing of one human is detrimental to, reductive of, the processing of another. Because humans need to augment their information processing, they will process information on the things around them whenever possible, exercising control over them as part of this processing. Control means to be able to allow or prohibit processing of that same thing by others (property rights). In other words, if there is a fixed number of houses or plots of land or cars to be had on the planet, if one individual amasses them all (i.e. controls them by having property rights over them), there will be none left for anyone else. It is this understanding, this inherent scarcity of resources in the analogue world that implicitly underlies any political philosophy (for example, the 'state of nature', where resource conflict is perpetual),[19] ethics (the meaning of justice, fairness, the *summum bonum*), morality, religion, economics and so on.

This fundamental understanding is overturned in the digital world, where information is infinite. New information in the digital world can be created in perpetuity by any human.[20] Digitised versions of analogue-

19 Most prominently found on the basis of Hobbes's theory (see, for example, Gregory S Kavka, "Hobbes's War of all against all," in *The Social Contract Theorists: Critical Essays on Hobbes, Locke, and Rousseau*, ed. Christopher W. Morris (Lanham Boulder New York Oxford: Rowman & Littlefield, 1999).), the topic of an, imagined, state of nature however being central (and, mostly, problematic) among all social contract theorists.

20 It is, of course, understood that the digital world is created by computers, which exist in the analogue world and therefore their number is finite, and thus possibly controllable (as is also true of the energy they need to operate). However, even ignoring the fact that computer ownership is widely dispersed (with, effectively, most humans on the planet owning more than one), the digital world is in fact created by their combined processing power, and, for the moment at least, it is difficult to imagine that this will become extinct.

world information can similarly be created and processed infinitely.[21] In other words, in the analogue world if someone eats all the fruit on the planet there will be no other fruit for anybody to eat; in the digital world, if someone excludes others from processing specific information, those affected can create other information to process for themselves. Even with the suitability of this particular information, the special experience offered by it or any other attempt at uniqueness (and, thus, scarcity) taken into consideration, the fact remains that possibilities for information processing for humans are infinitely greater in the digital than in the analogue world. This is a life-changing worldview that overturns development for humans and as noted in the introduction to this section, marks the fourth of the milestone moments in humanity's development so far.

D. A concluding proposal: a new programme for digital constitutionalism, the acknowledgement of platform rights

It needs to be decided whether the intention of constitutionalism, triumphant today in the analogue world, is about constitution-drafting in general or specifically about limiting the power of the state. Even if it is the latter, however, it still remains to be decided whether constitutionalism specifically focuses on human rights and values or whether it encompasses all the management functions of state power as well (for example, the separation of powers, the organisation of government etc.). Although in principle the term 'constitutionalism' would be expected to cover all the chapters found in modern constitutions, this is apparently not necessarily the case. For example, the European Declaration on Digital Rights and Principles has been celebrated as a milestone in (digital) constitutionalism,[22] even though it focuses exclusively on human rights and values.

---

21 Intellectual property rights notwithstanding, because, first, they apply only to a very small subset of the overall digitised information and, second, because they gradually expire anyway.

22 See Cristina Cocito and Paul De Hert, "The transformative nature of the EU Declaration on Digital Rights and Principles: Replacing the old paradigm (normative equivalency of rights)," *Computer Law & Security Review* 50 (2023); Giovanni De Gregorio, "The Declaration on European Digital Rights and Principles: A first analysis from digital constitutionalism," *The Digital Constitutionalist*, 2022, https://digi-con.org/the-declaration-on-european-digital-rights-and-principles-a-first-analysis-from-digital-constitutionalism/.

Digital constitutionalism, therefore, is unavoidably burdened by this vagueness. This, however, is not its only problem. Professing the 'digital' denomination, it promises to bring traditional constitutionalism into the digital world. While the confirmation that fundamental human values such as 'human dignity, freedom, equality and solidarity'[23] still apply in the digital world is undoubtedly of the highest importance, in order to retain the constitutional context, the basic terms of reference of constitutions need to continue to apply. However, as seen above, this is no longer the case. In the digital world the traditional notion of the state is eroded; the same is true of the traditional notion of an individual. More significantly, however, the basic analogue-world understanding of the scarcity of resources is reversed in the digital world. Under these circumstances, how can constitutionalism be adapted for the digital world, if the foundations upon which it is built are profoundly shaken?

In view of this possibly being a transitory, interim stage (the digital world having a life of only a few decades) before the state reaffirms its authority in the digital world and individuals also digitally reclaim their unique individuality in space and time, digital constitutionalism may do well to focus only on those aspects of constitutionalism that are most pressing—with human rights and values coming first to mind—during the construction of the digital world. The European Declaration, therefore, is a good example in this regard. Nevertheless, which values and which human rights should be transposed from the analogue to the digital world? The entire list of analogue-world fundamental rights? All human values applicable in liberal and democratic states? Even if such a (political) decision was reached, are all such rights suitable for simple transposition from the analogue to the digital world?

This does not seem to be the case. Not all analogue-world fundamental human rights and values are transposable as such to the digital world—simply adding the term 'digital' in front of them does not necessarily work. The basic right to security is a good example in this regard. Security of the person is a well-known and defined right in the analogue world, because, after living for thousands of years on the planet, humans know well when and how they can be threatened, what the risk is, and how best to deal with it—and what damage violence causes if it occurs. None of these

23 See par. 1 of the Preamble of the European Declaration on Digital Rights and Freedoms.

assumptions applies in the digital world. There humans may not even be aware that they are being threatened; even if they do know, most of the time they may not be able to assess the threat or the damage might not appear until long after a threat has been realised. This being the case, how could the right to security simply be transposed as a right to (cyber)security?[24]

This could therefore be an objective of a new programme for digital constitutionalism: to focus, for an interim period, only on human rights and values, as part of traditional constitutionalism, in order to identify similarities and differences in the analogue and the digital worlds and to assist in transposing traditional human rights and values into the digital realm, identifying which among them are suitable for transposition (and under which conditions) and which are not. In this context, platform rights, that is, the rights inherent on the information platform that is the state, are obvious candidates for this (re)assessment exercise. Because they are derived from an information-processing environment, these rights are most suitable for transposition to the digital world, which is itself an information-processing system. Because they are natural to humans, these rights have to be transposed into the digital world too, because humans, as informational beings, are active there. And, because states also continue to provide an indispensable and irreplaceable individualisation mechanism to humans in the digital world (ultimately, for the moment at least, all human activity in the digital world has to materialise in the analogue world in order to benefit the humans concerned), it is state power that will guarantee their application, in spite of state control being severely challenged.

A transitory, interim period in the advent of monumental change necessitates short-term, principle-driven decisions. With the digital world not having fully settled, nor showing any signs of doing so any time soon, legal rights and principles have to focus on the bigger picture, making use of whatever new perspectives and reassessments of the past have already been made possible. It may well be the case that the state will soon claim its power and authority in the digital world, as in the analogue one, asserting itself as soon as it becomes possible, as was the case in the period of company-state colonisation. Until that time, however, digital constitutionalism has a critical and paramount mission: to provide in the digital world an

24 See also Vagelis Papakonstantinou, "Cybersecurity as praxis and as a state: The EU law path towards acknowledgement of a new right to cybersecurity?," *Computer Law & Security Review* 44 (2022).

as-appropriate confirmation of the fundamental human rights and values that have been developed over the centuries in the analogue world.

List of Authors

Prof. Dr. iur. Dipl.-Soz. Marion Albers

Marion Albers is Professor of Public Law, Information and Communication Law, Health Law and Legal Theory at the University of Hamburg. She has been part-time lecturer at Seoul National University for the course „Comparative Constitutional Law" and Principal Investigator in the German/Brazilian DAAD/CAPES PROBRAL-Research Project „Internet regulation and und Internet rights". She is Managing Director of the Cyber Law Clinic at the Faculty of Law at the University of Hamburg, Fellow at the Institute for Advanced Study Berlin, and Member of the German Council for Scientific Information Infrastructures. Her main areas of research are Fundamental Rights, Information and Internet Law, Data Protection, Biolaw, Police Law and Law of Intelligence Services.

Prof. Dr. João Bachur

João Bachur is guest researcher at the Max Planck Institute for Legal History and Legal Theory in Frankfurt am Main, Germany. He is also Professor for Social and Legal Theory at the Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa - IDP (Brazilian Institute for Education, Development and Research), in Brasília, Brazil. He was previously guest researcher at the Institute of Philosophy at the Berlin Free University as Alexander von Humboldt-Fellow.

Prof. Dr. Rodrigo Brandão

Rodrigo Brandão is Professor of Constitutional Law at the State University of Rio de Janeiro. He holds a Doctorate and master's degree in Public Law from UERJ, serves as a Prosecutor for the Municipality of Rio de Janeiro, and practices Law as an attorney.

Dr. Ricardo Campos, LL.M.

Ricardo Campos has been Lecturer (since 2021) at the law faculty of Goethe University Frankfurt am Main. He holds a PhD in Law from the Goethe University Frankfurt am Main. He took part in the Commission of Legal Experts responsible to advise the Brazilian Senate in the reform of the Civil Code. He is also Director of the Legal Grounds Institute (Sao Paulo).

Prof. Dr. Edoardo Celeste

Edoardo Celeste is Associate Professor of Law, Technology and Innovation and Chair of the Erasmus Mundus master´s Program in Law, Data and AI (EMILDAI) at the School of Law and Government of Dublin City University, Ireland. He is the author of Digital Constitutionalism: The Role of Internet Bills of Rights (Routledge 2022).

Prof. Dr. Victor Oliveira Fernandes

Victor Oliveira Fernandes is Professor of Economic Law at the Brazilian Institute of Teaching, Development, and Research (IDP). He holds a Ph.D. in Law from the University of São Paulo (USP).

Dr. Giulia Gentile, LL.M.

Giulia Gentile is Lecturer in Law at Essex Law School and co-PI for the EU Horizon 2021-2027 collaborative project 'EXPRESS2'. Her research focuses on the promotion of human rights in the digital society and EU constitutional law. She is particularly interested in the use of AI in the legal profession and in justice systems. She joined Essex Law School in 2023, having previously worked as Fellow at LSE Law School, Teaching Fellow and Postdoctoral Researcher at Maastricht University. She holds a PhD and an LL.M. from King's College London, where she also worked as Visiting Lecturer in Law.

Dr. Clara Iglesias Keller

Clara Iglesias Keller is research lead in Technology, Power and Domination at the Weizenbaum Institute and the WZB Berlin Social Sciences Center and a Guest Professor at the Brazilian Institute for Education, Development and Research (IDP). She holds a doctorate and a master's degree in Public Law from the Rio de Janeiro State University and an LL.M. in Information Technology and Media Regulation from the London School of Economics and Political Science. Her research agenda is focused on the relationship between technologies and democratic institutions, including platform governance, artificial intelligence regulation and democratic legitimacy in digital spheres.

Dr. Beatriz Kira

Beatriz Kira is a Lecturer in Law at the University of Sussex and a Research Fellow in Law & Regulation at UCL's Digital Speech Lab. Trained as a lawyer and as a social scientist, she has a PhD in Economic Law from the University of São Paulo (USP) and an MSc in Social Sciences of the Internet from the University of Oxford. She has previously held postdoctoral positions at UCL and at the Blavatnik School of Government, University of Oxford.

Prof. Dr. Alessandro Mantelero

Alessandro Mantelero is Associate Professor of Private Law and Law & Technology at Polytechnic University of Turin and EU Jean Monnet Chair in Mediterranean Digital Societies & Law. He is also Associate Editor of of the journal Computer Law & Security Review and member of the editorial board of European Data Protection Law Review.

Prof. Dr. Claudia Lima Marques

Claudia Lima Marques is full Professor in Private International Law (Federal University of Rio Grande do Sul, UFRGS, Porto Alegre, Brazil), President of the International Association of Consumer Law – IACL (Bruxels) and Chair of the Committee of International Protection of Consumers of the International Law Association (London).She is also Director of the Center for European and Germany Studies, CDEA-DAAD, Porto Alegre and Brasilcon and holds a Doctor iuris utriusque (Ruprecht-Karls Universität Heidelberg), Legum Magister (Eberhard-Karls Universität Tübingen), Diplom in European Integration (Universität des Saarlandes) and SDJ (UFRGS). She was former President of ASADIP-Asociación Americana de Derecho Internacional Privado (Asunción) and BRASILCON (Brazilian Institut for Consumer Law and Policy, Brasilia) and is a Professor at the Doctorate Program at UFRGS (Porto Alegre) and at UNINOVE (São Paulo).

Prof. Dr. Gilmar Mendes

Gilmar Mendes is Professor of Constitutional Law at the Brazilian Institute of Teaching, Development, and Research (IDP). He is a Supreme Court Justice in Brazil and holds a Ph.D. in Constitutional Law from the University of Münster (Westfälische Wilhelms Universität Münster).

Prof. Dr. Laura Schertel Mendes

Laura Schertel Mendes is Professor of Law at the University of Brasilia (UnB) and at the Brazilian Institute for Development, Education and Research (IDP). She holds a Ph.D. from Humboldt University, Berlin, Germany and was a postdoctoral researcher at the Goethe University Frankfurt am Main (Capes/Alexander von Humboldt Fellowship 2022/2023). She is President of the Digital Law Commission of the Brazilian Bar Association and Director of the Centre for Law, Internet and Society (CEDIS/IDP). She was the Rapporteur of the Commission of Legal Experts, in charge of advising the Brazilian Senate on the regulation of artificial intelligence in Brazil in 2022. She is a member of the Board of Editors of the Journal of AI Law and Regulation (AIRe).

Prof. Dr. Fabiano Menke

Fabio Menke is Associate Professor for Civil Law - Faculty of Law Federal University of Rio Grande do Sul – UFRGS, Professor at the Postgraduate School Faculty of Law – UFRGS and holds a Ph.D. from the University of Kassel, Germany (Scholarship CAPES/DAAD).

Prof. Dr. Vagelis Papakonstantinou

Vagelis Papakonstantinou is Professor on Personal Data Protection Law at the Faculty of Law & Criminology of the Free University of Brussels (VUB, Vrije Universiteit Brussel), focusing also on Cybersecurity, Intellectual Property, and the broader topic of technology regulation. He is the director of VUB's Cyber and Data Security Lab (CDSL), as well as a core member of VUB's Research Group on Law Science Technology & Society (LSTS) and the Brussels Privacy Hub.

Prof. Dr. Jane Reis Gonçalves Pereira

Jane Reis Gonçalves Pereira is Associate Professor of Constitutional Law at the Law School of the Rio de Janeiro State University (UERJ), a Federal Judge and a member of the Brazil Chapter of the International Society of Public Law (ICON-S). She holds a Ph.D. in Public Law from UERJ and a master's degree in Constitutional Law and Theory of the State from Pontifícia Universidade Católica do Rio de Janeiro (PUC-Rio).

Prof. Dr. Alexander Peukert

Alexander Peukert is Professor of Civil, Commercial and Information Law at the Faculty of Law of Goethe University Frankfurt am Main. From 2009 to 2019, he was principal investigator of the Cluster of Excellence "The Formation of Normative Orders". His main research interest is in Intellectual Property and Unfair Competition Law.

Prof. Dr. Gabrielle Bezerra Sales Sarlet

Gabrielle Bezerra Sales Sarlet is lawyer and legal consultant, with a bachelor's and master´s degree in law from the Federal University of Ceará (UFC), a Ph.D. in Law from the University of Augsburg (UNIA - Germany), post-doctoral research in Law from the University of Hamburg (Germany) and the Pontifical Catholic University of Rio Grande do Sul (PUCRS). She is specialized in neuroscience and behavioral sciences at the Pontifical Catholic University of Rio Grande do Sul (PUCRS). She is also Professor in the undergraduate, master´s, and doctoral programs (PPGD) at the Pontifical Catholic University of Rio Grande do Sul (PUCRS).

Prof. Dr. Ingo Sarlet

Ingo Sarlet is a lawyer and legal consultant. He holds a Ph.D. degree in Law from the University of Munich, where post-doctoral studies were also conducted. He is a professor and coordinator of the master's and PhD in Law program (PPGD), as well as professor in the master's and Ph.D. in the Criminal Sciences program (PPGCRIM) at the School of Law of the Pontifical Catholic University of Rio Grande do Sul (PUCRS). Sarlet is a retired Judge of the Tribunal de Justiça of Rio Grande do Sul (State Court of Justice) and a former Judge at the Regional Electoral Court of Rio Grande do Sul.

Prof. Dr. Indra Spiecker gen. Döhmann, LL.M.

Indra Spiecker genannt Döhmann holds the Chair of Public Law, Law of Digitality and Legal Theory and heads the Institute of Digitization at the University of Cologne. She also coordinates the LL.M. Digitalization and the Special Program on Digitalization thereof. Prior, she held the Chair in Public Law, Information Law, Environmental Law and Legal Theory at Goethe University Frankfurt a.M., where she was also director of the Data Protection Research Institute and where she is still associated with the Center for Critical Computational Studies (C3S). She is director in Athene, Europe's largest IT-Competence Center, as well as in KASTEL, KIT's Institute of Institute of Information Security and Dependability.