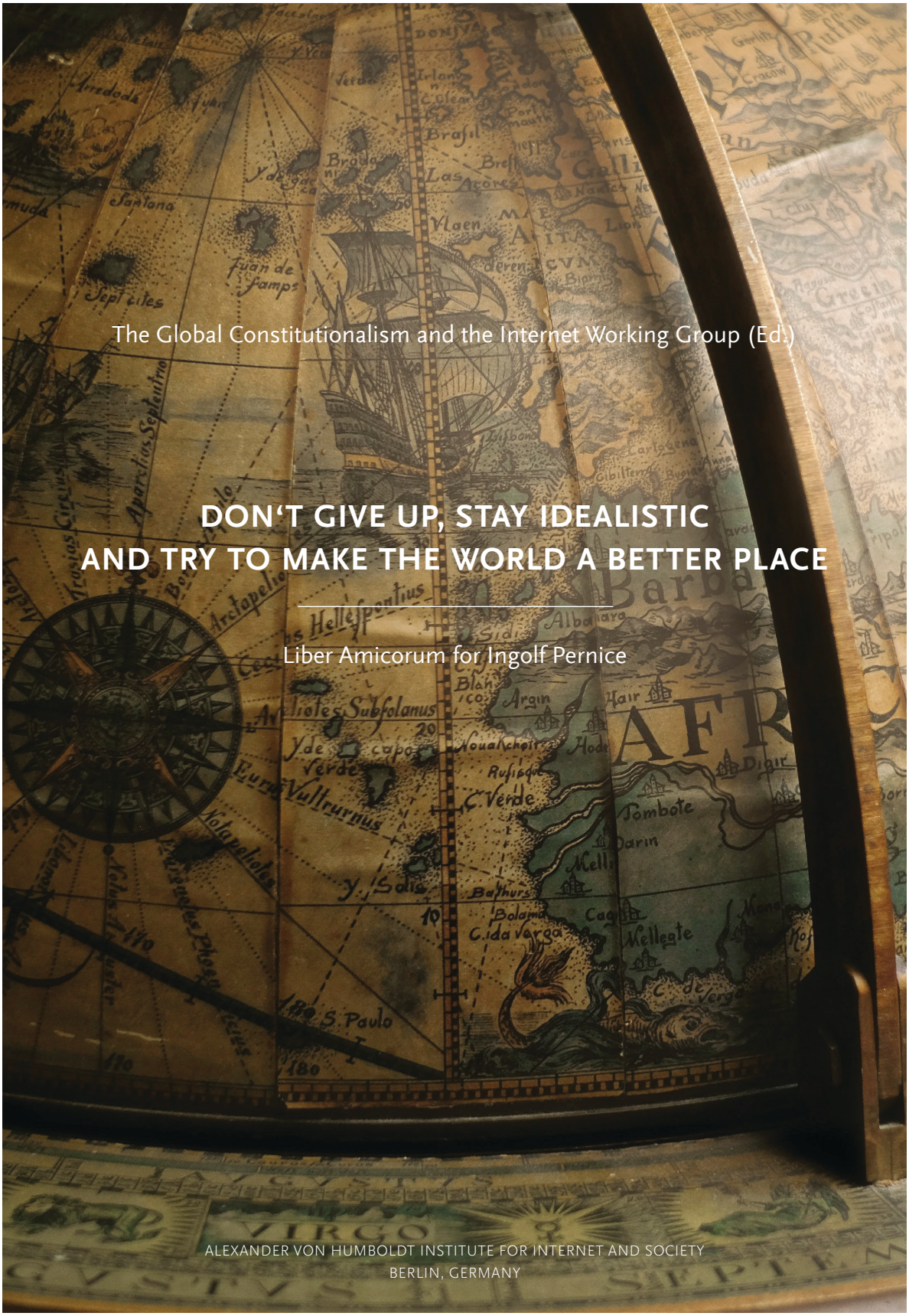

The Global Constitutionalism and the Internet Working Group (Ed.)

DON'T GIVE UP, STAY IDEALISTIC AND TRY TO MAKE THE WORLD A BETTER PLACE

Liber Amicorum for Ingolf Pernice

ALEXANDER VON HUMBOLDT INSTITUTE FOR INTERNET AND SOCIETY
BERLIN, GERMANY

The Alexander von Humboldt Institute for Internet and Society (HIIG) explores the dynamic relationship between the Internet and society, including the increasing penetration of digital infrastructures into various domains of everyday life. Its goal is to understand the interplay of social-cultural, legal, economic, and technical norms in the process of digitisation.

Alexander von Humboldt
INSTITUTE FOR INTERNET
AND SOCIETY

FOREWORD

This liber amicorum is dedicated to Ingolf Pernice, one of the founding directors of the Alexander von Humboldt Institute for Internet and Society (HIIG) in Berlin, Germany.

The HIIG wasn't Ingolf's only – or even his most important – waypoint in his career inside and outside academia, but maybe a comparatively challenging one and hopefully one of the most insightful. This waypoint was challenging because Ingolf stepped out of his academic comfort zone in more than one way. He stepped out of the sphere of legal scholarship at a renowned law faculty of a long-established university, the Humboldt-Universität zu Berlin, into an interdisciplinary brawl in an emerging academic field – internet research. He joined an academic institution that rather resembled a startup, a wholly different way of interacting, collaborating and innovating than within the halls of the academic ivory tower. However, he rose to the challenge formidably. Ingolf was integral to forming the diverse crowd of people with their different disciplinary backgrounds and academic histories into the institute that we know today. And this waypoint was insightful, because Ingolf never stopped questioning conventional assumptions, supposed truths and traditional solutions in his endeavour to better understand the increasing digitisation of society, from state bureaucracy to everyday life, and its implications for individuals and the society as a whole. In this endeavour, he went beyond the constraints of existing legal thinking, he ventured into the unknown, tried to put concepts borrowed from different disciplines to use and tested them for their ability to provide new insights into the law in the digital constellation, into the future of the law beyond the nation state and into the constitutionalisation processes on the global level.

Central to Ingolf's thinking was and is always and uncompromisingly the individual and the question of how he or she can evolve from an object of social regulation into its subject. How he or she can become the sovereign of a community in a self-determined and self-responsible manner, regardless of whether this community is a state, Europe or the world. He asks how fundamental rights and freedoms can overcome their artificial limitation to nation states. How we can create a global, democratically legitimised order that puts the individual at the centre, strengthens his or her rights and freedoms, and in which decisions can only claim legitimacy if they are clearly based on the demos of individuals and their decision-making.

Consequently, the central focus of his academic work in recent years has been to establish the human being as a point of reference and as an actor in international

law – as a bearer of fundamental rights, as a source of legitimacy for socially binding political decisions and as a co-decision maker. With his work, he aims to make use of positive as well as negative experiences in different forums – from local participatory budgeting to the global Internet Governance Forum – in order to strengthen the direct involvement of all stakeholders, especially citizens, in deliberation and decision-making. He has always paid particular attention to the question of how information and communication technologies can be used to strengthen the transparency of political action, accountability and participation – online and offline.

We brought together a small collection of friends, colleagues and disciples to contribute to this volume. They have worked with Ingolf, in projects under his lead or where he contributed or engaged in discussions at HIIG, or engaged with concepts that Ingolf helped shape. They were influenced by Ingolf's work or in scientific interchange with him. Either way, the contributions in this volume show the wide variety of fields and topics where Ingolf left his mark. They also convey that they are connected beyond Ingolf as a person as they deal with how the digital society can be shaped – as a global, sustainable, democratically legitimised, rights and freedoms-protecting order.

The editors

CONTENTS

Researching Global Constitutionalism and the Internet at HIIG: The Game is On

JÖRG POHLE, RÜDIGER SCHWARZ, ULRIKE HÖPPNER

The Global Constitutionalism and the Internet research group can look back on a long as well as an eventful, insightful and successful history. It originated as one of the four founding research departments of the Alexander von Humboldt Institute for Internet and Society (HIIG) in Berlin, Germany, when the institute was organised along thematic topics into departamental lines. Global Constitutionalism and the Internet was however the most innovative, cross-cutting one of these research units.

While the other three departments were largely organised along disciplinary boundaries, C-paX – as it was called internally – was much more diverse from the very beginning. Researchers came from many different disciplines, a wide variety of methodological approaches were pursued in the department's projects and the topics were not just interdisciplinary in nature but also approached in such a manner. In early 2013, shortly after its inception, the department could boast bringing together a Chilean lawyer with a German PhD in Political Science, a political scientist, a philosopher and media scholar as well as a computer scientist with a background in Law – without counting the student assistants. Ingolf Pernice, a renowned Public International and European Law scholar, who held a chair at the Law Faculty of Humboldt-Universität zu Berlin, headed and guided the department.

The department's research focused on three distinct, but overlapping research areas: (1) the internet-related and internet-driven constitutionalisation beyond the current regional and international institutional frameworks, (2) the public administration's progressive digitisation, and (3) the societal controversy on the implications of the increasing digitisation of all aspects of individual, social, political and economic life.The department's diversity was aptly reflected in it acronym, C-paX: "C" for constitutionalism, "pa" for public administration, and "X" as a mark for both the department's work on digital civil disobedience – and its own rather disobedient nature towards any premature conclusion or redemptive expectation concerning the internet, digital society and things alike.

RESEARCH FOCUS AND CONCEPTUAL BACKGROUND

The research department – and later the research group – focused on new legal and institutional approaches to transnational and global governance for a digital society. It embarked on the challenging journey of translating widely accepted constitutional

principles such as human dignity, fundamental rights and freedoms, democracy and participation, the separation of powers and the rule of law into specific institutional arrangements, for the digital realm.

The research group was seeking new approaches to the legal construction of processes and institutions in which human rights and democratic legitimation form the basis for a normative framework for various forms of governance. It did so recognizing the increasing need for effective regulation of the internet as a global infrastructure for communication and control, especially in the areas of the environment, security and trade, i.e. for regulation beyond the state.

An understanding of global constitutionalism as a normative framework which takes the individuals and their fundamental rights instead of states as its conceptual starting point – or better its normative core assumption – characterized the particular approach of the working group. Its starting question was always how generally accepted constitutional principles such as human dignity, freedom and equality rights, democracy and participation, the separation of powers and the rule of law as inviolable values could be thought of, conceptualized and implemented beyond the scope of the nation state on a global scale. Therefore its research specifically explored relations between people at the global level and governance structures such as legal frameworks or international institutions. The goal was to "translate" these principles into democratically legitimised decision-making processes within the different arena of decision making. Whether the internet can play any meaningful role in representing or better empowering the individual beyond the nation state is still an open question. In fact, the research group always took notions of a "digital city upon the hill" with a pinch of salt. At the same time the internet has changed the life of individuals as much as of societies around the globe in such fundamental ways that make it paramount to understand its potential as well as the risks associated with the use of modern information technologies. Hence, the research group investigated how technologies contribute to the formation of norms beyond the state and dealt with the question of how these processes can be reconstructed from the perspective of constitutionalist theories.[1] In doing so, the group addressed questions from the fields of privacy, surveillance and data protection, cyber security and civil disobedience, public administration and civic tech, e-democracy and digital identity that extend beyond their application cases from both a transdisciplinary and a legal point of view.[2]

In particular, the research group focused on three general areas of interest.

[1] Pernice, Ingolf (2016). Global Constitutionalism and the Internet: Taking People Seriously. In: Hofmann, Rainer, & Kadelbach, Stefan (eds.), *Law Beyond The State. Pasts and Futures*. Frankfurt/New York: Campus Verlag, pp. 151–205.

[2] Pernice, Ingolf (2017). E-Democracy, the Global Citizen, and Multilevel Constitutionalism. In: Prins, Corien, Cuijpers, Colette, Lindseth, Peter L., & Rosina, Mônica (eds.), *Digital Democracy in a Globalized World*. Cheltenham: Edward Elgar Publishing, pp. 27–52.

The first centred around the individual, exploring whether one can think of different orders taking the individual as their starting point, or what shifts might result when focusing on the individual in the governance of the internet or the reform of administration.

The second area of interest concerned the process dimension, i.e. how the new global orders that will shape life in the world are being negotiated globally, and how unity and diversity emerge in the different societal contexts and areas that are of interest for the research group.

The third area of interest was the very issue of "constitution": what does a constitution mean in the "digital constellation"? Is there a specific "digital constitution"? What are the principles that should guide or regulate the development of digital technologies in general and the internet in particular?

THE RESEARCH GROUP'S FOUNDING PROJECTS

The department started with three founding projects. First among them was the department's long-term lead project *Global Privacy Governance*, the other two being *Digital Public Administration*, later: *The Digital Administrative State*, and *Digital Civil Disobedience*.

GLOBAL PRIVACY GOVERNANCE

The interdisciplinary research project *Global Privacy Governance* was conceived against the backdrop of the European Union's endeavour to reform the European data protection regime, specifically the General Data Protection Regulation (GDPR) proposal published by the European Commission in early 2012 and the then-starting regulatory debate. The project's first major event was a two-day high-level conference on the German perspective on the European reform and the future of data protection in the 21st century in October 2012 as well as three preparatory workshops in August, co-organised with the German Federal Ministry of the Interior. However, from the very beginning the project was looking beyond the nation state or even the European Union. Its main aim was to achieve a comprehensive understanding of concepts, processes and expectations of global negotiations and the aspects of problem framing, regulation and enforcement linked with it, both from an empirical and a conceptual point of view. The Snowden revelations in June 2013, uncovering the mass surveillance conducted by the Five Eyes' intelligence services across the world – not to mention the support from many other nations, intelligence services as well as companies, including from Germany – certainly proved the necessity of choosing a global governance perspective and were also a major driver of the very global debate the project aimed to better understand.

Cybersecurity, privacy, surveillance and data protection debates have emerged as

a prominent focal point in the wake of new challenges arising from increased network connection, new data generation and collection, new analytical techniques, conflicting cultural values and the emergence of the internet as a critical infrastructure. This is no accident, as they touch on the core values of democracy, fundamental rights and the possibilities and limits of both technical infrastructure as well as regulatory attempts at different levels.[3] The *Global Privacy Governance* project therefore aimed at mapping the multitude of current, possible and desirable governing mechanisms available with the intention determining and conceptualising innovative instruments and processes of effective global regulation in this field.[4]

The very lengthy, and at times highly controversial, negotiation process of the GDPR's final text as well as its practical implementation were the project's main focus in the years after its commencement. The project paid particular attention to three issues. Firstly, it looked at the widespread and contentious lobbying by different stakeholders, especially from industry, in the legislative process, which culminated in a multi-stakeholder workshop and an interdisciplinary funding application. Secondly, it focused attention on the renewed effort to data protection by design, i.e. the translation of legal protection requirements into technical standards and organisational actions.[5] And thirdly, it considered the role of regulatory authorities in the governance of data protection, which was extensively explored in an international workshop in 2016 that brought together scholars and practitioners from data protection authorities and industry.

In December 2015, the *Global Privacy Governance* project initiated an interdisciplinary workshop series, "Privacy, Data Protection & Surveillance", hosted biannually at HIIG and, since 2018, annually at the *Institute for International Law of Peace and Armed Conflict* in Bochum. The workshop series has since become one of the premier events in this research field, focusing in particular on early-stage researchers, work in progress and a critical reflection on the premises of one's own research, theoretical school(s) and discipline(s).

On the international stage, the project joined forces with New York University's *Center on Law & Security* and Université Grenoble Alpes' *Centre d›Etudes sur la Sécurité Internationale et le Coopérations Européennes* to establish a "Transatlantic Technology and Security Working Group" as an open framework for promoting a continued di-

[3] Lewinski, Kai von (2014). *Die Matrix des Datenschutzes. Besichtigung und Ordnung eines Begriffsfeldes.* Tübingen: Mohr Siebeck; Pohle, Jörg (2018). *Datenschutz und Technikgestaltung: Geschichte und Theorie des Datenschutzes aus informatischer Sicht und Folgerungen für die Technikgestaltung.* Dissertation. Berlin: Humboldt-Universität zu Berlin. URL: https://edoc.hu-berlin.de/handle/18452/19886.

[4] Pernice, Ingolf (2013). Informationsgesellschaft und Politik: Vom Neuen Strukturwandel der Öffentlichkeit zur Global Privacy Governance. HIIG Discussion Paper Series No. 2013-02. URL: http://dx.doi.org/10.2139/ssrn.2222046.

[5] Pohle, Jörg (2015). Das Scheitern von Datenschutz by Design: Eine kurze Geschichte des Versagens. In: *FIfF-Kommunikation* 32(2), pp. 41–44.

alogue. The working group organised dedicated conferences and set out to develop common research projects in a field characterised by a controversial issue: the tension between cyber security and data protection. In late 2017, HIIG hosted the first of two conferences addressing this pressing challenge in the transatlantic relationship, "Privacy and Cyber Security on the Books and on the Ground". The conference brought together cyber security, data protection and governance experts, lawyers and representatives from security agencies, businesses and politics in order to analyse the problems in this field, gain a deeper understanding of different concepts, develop approaches and strategies for solutions, while ensuring a productive integration of the relatively independent discourses in the USA and Europe on this issue.[6] A year later, the project co-organised a second conference in New York, "Building Common Approaches for Cybersecurity and Privacy in a Globalized World", continuing the efforts of the first conference and focusing on developing solutions and strategies for the problems identified.[7]

DIGITAL PUBLIC ADMINISTRATION

The department's second founding project, *Digital Public Administration*, later: *The Digital Administrative State*, was started to examine the internet›s impact on public administration and on public institutions in general as well as on their modes of action (public governance). The main focus was not primarily on how digital technologies are rolled out or the form they take but instead on the fundamental repercussions and challenges these developments have for state institutions, their functional logics in general and for specific governance areas in particular, e.g. e-justice.

The project distinguished three impact categories: firstly, the internet as a precondition for providing public goods, especially in countries of the southern hemisphere; secondly, the internet as a challenge to the underlying organising principles of public administration and how it is conducted; and thirdly, the internet as an opportunity for efficiency and transparency in a digitalised public administration (as well as private business administration) depending on the security of and trust in the infrastructure and services.

With respect to the internet's function as a precondition for state institutions to provide collective goods, the project looked specifically at cases and countries located in the southern hemisphere, which are either emerging markets, as in the case of

[6] Pernice, Ingolf, & Pohle, Jörg (eds.) (2018). *Privacy and Cyber Security on the Books and on the Ground*. Berlin, Germany: Humboldt Institute for Internet and Society. URL: https://www.hiig.de/en/publication/privacy-and-cyber-security-on-the-books-and-on-the-ground/.

[7] Milch, Randal S., Benthall, Sebastian, & Potcovaru, Alexander (eds.) (2019). *Building Common Approaches for Cybersecurity and Privacy in a Globalized World*. New York: New York University, Center for Cybersecurity. URL: https://ssrn.com/abstract=3508933.

Chile[8] and Brazil[9], or newly emerging economies, as in the case of Kenya. In particular, it studied the effects of the internet on the ability of public institutions to provide goods and services in areas such as healthcare, education, combating corruption or guaranteeing access to information and justice.[10] The project revealed the significantly distinct and positive impacts information and communication technologies (ICTs) can have on the ability of public institutions in weak states to provide services and to be held accountable for their actions. However, it provided equally strong evidence that the provision of public goods by non-state actors enabled through ICT regularly failed to serve as a functional equivalent of – even weak – state institutions. Also, there was no evidence found that ICTs had any relevant impact on or potential for the economic growth in developing countries, often attributed to the areas of business process outsourcing (BPO) or internet-enabled services (IES).

In the research on the function of the internet as a challenge to the fundamental organising principles and logics of public administrations, the project addressed the repercussions of disruptive technologies such as big data or algorithmic decision-making. With the internet unleashing data-driven dynamics, significant changes within established systems of administration take place, the healthcare sector (e-health) or law enforcement agencies (predictive policing) being cases in point. In this context, the project also investigated the repercussions of these developments for constitutional principles, with a special focus on the effects on fundamental rights, citizens' participation in legitimate decision-making processes and the application of principles of proportionality to administrative processes in a digitally aware public administration.[11]

The internet also creates opportunities, especially for public – as well as private – administrations to become more efficient and transparent. The project addressed the conditions that must be fulfilled in order to exploit these opportunities. The most important of these conditions is the security of and trust in the infrastructure and services, both of which have to be actively created through a connection of legal, social, organizational and technical measures.[12]

[8] Saldías, Osvaldo, Letelier, Macarena, & Schaale, Claus (2014). *Chile, un hub digital para la región*. White Paper for the Chilean Ministry of Economics. URL: https://www.hiig.de/wp-content/uploads/2015/01/CHILE-UN-HUB-PARA-LA-REGION.pdf.

[9] Saldías, Osvaldo (2015). Coded for Export! The Contextual Dimension of the Brazilian Framework for Internet Law & Policy. In: *Direito Público* 12(61), pp. 189–207.

[10] Schwarz, Rüdiger (2015). Context Matters: The Role of ICTs for Supporting Democracy in the Southern Hemisphere. In: *PolitiKa* 1(2), pp. 106–111.

[11] Saldías, Osvaldo (2014). Unleashing the Potential of Smart Bureaucracies for our Intelligent Cities. In: *PolitiKa* (1). URL: http://www.fjmangabeira.org.br/edicoes-revista-politika/revista-politika-no-1.

[12] Pernice, Ingolf (2017). E-Government and E-Democracy: Overcoming Legitimacy Deficits in a Digital Europe. In: Papadopoulou, Lina, Pernice, Ingolf, & Weiler, Joseph H. H. (eds.), *Legitimacy Issues of the European Union In the Face of Crisis*. Baden-Baden: Nomos, pp. 287–316.

With new researchers joining the team in 2016, the project began to put a stronger focus on particular technologies within the broader field of digitisation. These technologies included methods and technologies originating from computer science research on AI, like artificial neural networks, support vector machines or expert systems. The project looked at how they are employed in public administration, what guidelines for their design and use already exist, and what trends are emerging. It specifically examined the intersection of law, technology, organisation and public policy, finding a lack of interdisciplinary research in this emerging field as well as a need for moderate regulation in order to exploit the technology's positive potential.[13] Special consideration was given to law as an instrument of design, particularly in combination with experimentation clauses that were enacted in conjunction with e-government laws within the last few years in Germany and in the Laender. These laws allow for experimenting with new forms of technology-based decision-making and decision-support systems in order to observe their implications both on the public administration itself and on their environments, such as their clientele and other affected parties. The aim of this experimentation is to provide insights and learnings for further legislation, especially if design and application are coupled with strong stakeholder participation.[14] Besides directly influencing the technology's design, e.g. through regulation or technical standards, governments can also exert a great deal of indirect influence, for example through the shaping of public procurement procedures and the setting of award criteria.[15]

DIGITAL CIVIL DISOBEDIENCE

The third founding project, *Digital Civil Disobedience*, has investigated a political phenomenon that has undergone a remarkable change in recent times: civil disobedience.[16] The research examined existing theories of civil disobedience and of its transformation in the digital era. It questioned the applicability of these theories on digital civil disobedience, with a particular focus on radical democratic theories that see civil disobedience not as a necessary evil, but as a potential cure for the structural deficits of law and government decisions. By analysing a variety of emerging practices of digital disobedience, from "electronic civil disobedience" in the mid-1990s, distrib-

[13] Djeffal, Christian (2018). Normative Leitlinien für Künstliche Intelligenz in Regierung und Verwaltung. In: Mohabbat Kar, Resa et al. (eds.), *(Un)berechenbar? Algorithmen und Automatisierung in Staat und Gesellschaft*. Berlin: Kompetenzzentrum öffentliche IT, pp. 493–515.

[14] Christian Djeffal (2018). *Künstliche Intelligenz in der öffentlichen Verwaltung*. Report for the German National E-Government Competence Center (NEGZ). URL: https://ssrn.com/abstract=3289109.

[15] Djeffal, Christian (2019) Künstliche Intelligenz. In: Klenk, Tanja et al. (eds.), *Handbuch Digitalisierung in Staat und Verwaltung*. Wiesbaden: Springer. URL: https://doi.org/10.1007/978-3-658-23669-4_3-1.

[16] Züger, Theresa (2013). Re-thinking civil disobedience. In: *Internet Policy Review* 2(4). URL: https://dx.doi.org/10.14763/2013.4.216.

uted denial of service (DDoS) actions, digital whistleblowing, website defacements and beyond, the project studied how these intentionally unlawful actions change and challenge established notions of this form of political action in the political sphere, in law as well as in research.[17] Its aim was to contribute a theoretical approach to the question of when and how civil disobedience using traditional or digital tactics can be seen as legitimate protest.[18]

NEW PROJECTS ALONG THE ROAD

Over the course of the following years, a number of new, often more focused projects have been started and successfully completed, or are still going on. First among those projects was HIIG's participation in the *Network of Excellence for the Law of Civil Security in Europe (KORSE)*, which has been funded by the German Federal Ministry of Education and Research. The second research project, *Orphan Works*, was conducted within dwerft, an interdisciplinary research consortium focusing on new IT-based film and television technologies, also funded by the German Federal Ministry of Education and Research. The still ongoing project on the *Public International Law of the Internet* focuses on the plethora of new legal questions in the field of international law that are raised by especially the principles and limits of intelligence activities in terms of mass surveillance. A special mention is due to a public, high-profile lecture series that C-paX organised on *The Internet as a Challenge for State, Law and Society*, held at Humboldt-Universität zu Berlin's Faculty of Law in summer 2015.

KORSE – NETWORK OF EXCELLENCE FOR THE LAW OF CIVIL SECURITY IN EUROPE

Between 2013 and 2016, four young researchers engaged in research on the theoretical and practical challenges for civil security in a united Europe. Focusing on cybercrime, government access to data and the protection of critical infrastructure as a point of reference, their work also shed light on the validity and protection of fundamental rights as well as the distribution of competences between the EU and its member states. Each individual project had a different approach to the wider problem and resulted in a separate book publication.

The first project started from the observation that IT security as a policy area is characterised by epistemic uncertainty. While clarity on what public authorities can know and may know is lacking, it is clear that, in order to regulate the field efficiently,

[17] Züger, Theresa, Milan, Stefania, & Tanczer, Leonie Maria (2016). Sand in the Information Society Machine: How Digital Technologies Change and Challenge the Paradigms of Civil Disobedience. In: *Fibreculture Journal: internet theory criticism research* 25. URL: https://dx.doi.org/10.15307/fcj.26.192.2015.

[18] Züger, Theresa (2017). *Reload Disobedience – Ziviler Ungehorsam im Zeitalter digitaler Medien*. Dissertation. Berlin: Humboldt-Universität zu Berlin. URL: https://edoc.hu-berlin.de/handle/18452/19321.

they should act only when they have sufficient information. Public authorities are faced with specific legal challenges, since IT infrastructures are mainly in the hands of private actors. Lacking direct access to these infrastructures as well as information concerning their current status, poses major challenges for public authorities' ability to govern in this field. Many private actors are reluctant to cooperate with public authorities, whether for fear of being exposed to bad publicity for their lack of proper security measures or because their business models are threatened by too much openness. Thus, the project explored public authorities' actual knowledge as well as what they need to know in order to fulfil their duties with regard to IT security.[19] It examined the contribution that the law can make by controlling information about internet security and threats, drawing on the legal foundations for the collection, sharing and publicising of information by the security authorities, which also seek to limit infringements on these private actors' fundamental rights.[20]

The second project dealt with the tension between opposing principles in European law. Its particular focus lay on the tension between fundamental rights in their aim to protect internet users from interference by state authorities (negative obligations) and their aim obliging these authorities to take action in order to protect the holders of these rights from violations committed by other private actors (positive obligations). With the European Court of Justice's ruling on data retention, in which the Court derived an independent fundamental right to security from Article 6 of the Charter of Fundamental Rights of the European Union (CFR), it continued and Europeanised a trend so far only observable on the Member States' level.[21] As sociological and political science research has shown, though, "security" is a fundamentally contested issue, which thus demands special consideration when being negotiated in the legal sphere. Thus, the research criticised the existing dogmatic fundamental rights concepts concerning the public goal of security in Union law from an interdisciplinary perspective and demonstrated their contradictions to the Union constitutional principles of democracy and separation of powers. On this basis, a fundamental rights-dogmatic alternative was developed and substantiated: Union law's security principle as a principle in the sense of Article 52 (5) CFR.[22]

The third project focused on the challenges substantive criminal law is facing

[19] Leisterer, Hannfried (2016). Das Informationsverwaltungsrecht als Beitrag zur Netz- und Informationssicherheit am Beispiel von IT-Sicherheitslücken. In: Kugelmann, Dieter (ed.), *Sicherheit. Polizeiwissenschaft und Sicherheitsforschung im Kontext*. Baden-Baden: Nomos, pp. 135–150.

[20] Leisterer, Hannfried (2018). *Internetsicherheit in Europa. Zur Gewährleistung der Netz- und Informationssicherheit durch Informationsverwaltungsrecht*. Tübingen: Mohr Siebeck.

[21] Leuschner, Sebastian (2016). EuGH und Vorratsdatenspeicherung: Erfindet Europa ein neues Unionsgrundrecht auf Sicherheit ? In: Schneider, Florian, & Wahl, Thomas (eds.), *Herausforderungen für das Recht der zivilen Sicherheit in Europa*. Baden-Baden: Nomos, pp. 17–46.

[22] Leuschner, Sebastian (2018). *Sicherheit als Grundsatz. Eine grundrechtsdogmatische Rekonstruktion im Unionsrecht am Beispiel der Cybersicherheit*. Tübingen: Mohr Siebeck.

with regards to computer and cybercrime. Member States conferred competences on the EU to harmonise national criminal laws with the Treaty of Lisbon for the first time. Since then, the EU has been permitted to adopt minimum rules for particularly serious crimes that have a cross-border dimension and that therefore demand cross-border regulation, which explicitly includes "computer crime". Against the backdrop of significant interpretive problems concerning "computer crime", the project shed light on the harmonisation of substantive criminal law in the European Union and the challenges arising in relation to the EU's harmonisation competences.[23] By taking a comprehensive look at the constitutional, European and criminal law foundations of the distribution of competences between the nation states and the European Union, the project developed a network-specific concept of "computer crime" for this purpose. The insights gained offer guidelines for future legislative acts as well as executive cooperation mechanisms that can also be used for other transnational areas of crime.[24]

The fourth project dealt with data protection issues in the context of criminal investigations that concern electronic data held by third parties, such as online service providers or intermediaries. Law enforcement agencies in Germany can collect physical objects as evidence, including from third parties, since 1877 when the respective provisions of the German Code of Criminal Procedure have been drafted originally. However, the vast amounts of data about their users at the disposal of these companies and the insights to be gained from this data on all aspects of the personal, social and professional life of suspects raise the question of the conditions for and the limits of the state's right to access to possible evidence.[25] The project tackled these questions from a human rights perspective, including the due protection of national and European fundamental rights. It shed light on the German Federal Constitutional Court's ruling deriving a right to the protection of confidentiality and integrity of information technology (IT) systems and proposed fundamental rights-dogmatic solutions for many of the difficult riddles in this field.

ORPHAN WORKS

The research project *Orphan Works* was, between 2014 and 2017, part of *dwerft*, an interdisciplinary research consortium focusing on new IT-based film and television

[23] Haase, Adrian (2015). Harmonizing substantive cybercrime law through European Union directive 2013/40/EU – From European legislation to international model law? In: *First International Conference on Anti-Cybercrime (ICACC)*, pp. 1–6.

[24] Haase, Adrian (2017). *Computerkriminalität im Europäischen Strafrecht*. Tübingen: Mohr Siebeck.

[25] Peters, Emma (2016). Strafrecht und Datenschutz im Internet. Zugriff der Strafverfolgungsbehörden auf die Cloud – Ermittlungen ohne Grenzen? In Kugelmann, Dieter (ed.), *Migration, Datenübermittlung und Cybersicherheit. Grundfragen und ausgewählte Handlungsfelder der Zusammenarbeit von Sicherheits- und Strafverfolgungsbehörden in der EU*. Baden-Baden: Nomos, pp. 167–172.

technologies. *Orphan Works* analysed the legal framework for the use of orphan cinematographic works, i.e. works whose rights holders are unidentifiable or untraceable, in comparative perspective, focusing on Europe and the US in particular. It found that the 2012 European directive on orphan works is not well suited for film works, and seeked to develop alternative approaches where possible, taking into consideration the role of fundamental rights and paying particular attention to the tensions between the protection of intellectual property rights and easier access to knowledge and culture worldwide.

On the basis of a taxonomy of different creative reuses (covering, for example, fan vids, remixes, mashups, documentaries, compilation films) developed in this project, exceptions toward copyright were found to come with significant insecurities for users even if leaving considerable room for creative reuses if underlying fundamental rights are adequately considered.[26] In terms of the preservation of orphan filmworks, the project's research suggests that the EU Orphan Works Directive and its implementation will probably not be sufficient to allow for the adequate archiving and preservation of orphan audiovisual works such as films or computer games. The project took a comprehensive look at remixes on hosting platforms, the colliding rights of users, rights holders and platform operators, as well as the complex interplay between contractual relations, the international nature of the parties and the use of automated filter systems. From these observations the project determined the extent to which legally permitted uses of remixes are effective and how making them accessible via platforms affects this area of law. In particular, the research shed light on the importance of artistic freedom for the interpretation of legal barriers in copyright law as well as in the take-down process.[27]

PUBLIC INTERNATIONAL LAW OF THE INTERNET

The research project *Public International Law of the Internet*, which is still ongoing, seeks to better understand new legal questions arising globally from the internet's rapid development in connection with the increasing digitisation of everyday life. In this endeavor, the project does not limit itself to considering the classic questions of public international law. Instead, the project references the contemporary global dimension by connecting questions of international and constitutional law with those of private law, especially of commercial law and competition law, security and criminal law. The research addresses which and whose laws are applicable to which aspects of everyday life and what this development means for nations' sovereignty.

[26] Maier, Henrike, & Jütte, Bernd Justin (2017). A human right to sample—will the CJEU dance to the BGH-beat? In: *Journal of Intellectual Property Law and Practice* 12(9), pp. 784–796.

[27] Maier, Henrike (2018). *Remixe auf Hosting-Plattformen. Eine urheberrechtliche Untersuchung filmischer Remixe zwischen grundrechtsrelevanten Schranken und Inhaltefiltern*. Tübingen: Mohr Siebeck.

From these observations it seeks to answer the question if there is something that could be called "digital sovereignty" – and what that would mean. The project sheds light on the challenges for safeguarding human and fundamental rights against the actions of nation states and private actors. This is of particular importance considering the ongoing global search for responses to the challenges of cybercrime, cyberwar and cyber attacks by individuals, groups and states, responses that could create or amplify risks for fundamental rights.[28] Thus, the project investigates existing and innovative regulatory approaches and processes for the emergence of global standards or global law and explores how such solutions could be drawn up.[29]

The principles and limits of intelligence activities in terms of mass surveillance are a special focus of the research. Effective regulation and democratic control exist only sporadically and, indeed, almost absent at the international level. The possibility of analysing large amounts of data means that individuals are affected more by intelligence agencies' activities than in the era of classic public international law. Hence, the project underscores the necessity of redefining the relationship between legitimate security interests and the effective protection of human rights.[30]

THE INTERNET AS A CHALLENGE FOR STATE, LAW AND SOCIETY

In summer 2015, C-paX organised a weekly public, high-profile lecture series held at Humboldt-Universität zu Berlin's Faculty of Law. The series gave an introduction to the operating principles of the internet and shed light on different topics around social and legal challenges of digitisation, especially the internet, and the 'digital society'. Selected speakers, among them academics, politicians, public officials, civil society representatives as well as a former judge, illuminated different aspects of the internet's challenges for law and society from their respective perspectives. The lecture series met with keen interest and was very well attended, with valuable contributions from a diverse audience that sparked fruitful debates among the participants.

NEW PERSPECTIVES AND GETTING CLOSER TO TECHNOLOGY

Since 2016, the research group has moved from a rather general perspective on digitisation and the internet towards taking a closer look at particular technologies, such as IoT, anonymisation and e-voting. The *IoT and eGovernment* project ran from 2016

[28] Pernice, Ingolf (2016). Global Constitutionalism and the Internet: Taking People Seriously. In: Hofmann, Rainer & Kadelbach, Stefan (eds.), *Law Beyond The State. Pasts and Futures.* Frankfurt: Campus, pp. 151–205.

[29] Pernice, Ingolf (2015). Das Völkerrecht des Netzes. Konstitutionelle Elemente eines globalen Rechtsrahmens für das Internet. In: Biaggini, Giovanni et al. (eds), *Polis und Kosmopolis: Festschrift für Daniel Thürer.* Zurich / St. Gallen: DIKE / Nomos, pp. 575–588.

[30] Pernice, Ingolf (2018). Risk Management in the Digital Constellation – A Constitutional Perspective (part I). In: *IDP. Revista de Internet, Derecho y Política* (26), pp. 83–94.; Pernice, Ingolf (2018). Risk Management in the Digital Constellation – A Constitutional Perspective (part II). In: *IDP. Revista de Internet, Derecho y Política* (27), pp. 79–95.

to 2017 as a *Digital Public Administration* spin-off in order to focus more closely on the government's use of Internet of Things applications. The *Goodcoin* project, which was conducted from 2016 to 2019 in collaboration with Humboldt-Universität zu Berlin and a startup and has been funded by the German Federal Ministry of Education and Research, seeked to develop a privacy-friendly bonus point and customer loyalty system. The third project, *DECiDe – Digital Identity, European Citizenship and the Future of Democracy*, conducted in cooperation with Procivis AG (Switzerland) and the Random Sample Working Group has developed a technical prototype that combines digital identities and random sample voting, and examined the opportunities and risks for democratic decision-making in Europe. *DECiDe* has received financial support from Advocate Europe, an idea challenge realised by MitOst and Liquid Democracy, funded by Stiftung Mercator, as well as demokratie.io.

IOT AND EGOVERNMENT

The *Digital Public Administration* spin-off project *IoT and eGovernment* funded by Cisco Systems, examined how governments and public administrations can make use of IoT applications to facilitate public services, and what role regulation plays. In early 2017, scholars and practitioners from a wide range of disciplines came together for an international conference on "IoT & Trust" to look at how trust and distrust may and do influence the adoption and use of IoT solutions in public administration and private businesses as well as what role standardisation, collaboration and regulation may play in turning distrust into trust.[31] The project investigated further whether and how the Internet of Things and its application may change public administration's policy objectives, instruments and services and what their constitutional limits are,[32] how IoT technologies' adoption by public administrations can be influenced,[33] and how administration can influence both the design and the adoption of IoT technologies.[34]

GOODCOIN – ROBUST PRIVACY FOR LOYALTY PROGRAMMES AND PAYMENT SYSTEMS

The research project *Goodcoin* had two goals. The main goal was practical and consisted in developing a privacy-friendly bonus point and customer loyalty system. In

[31] Pernice, Ingolf, Schildhauer, Thomas, Tech Robin, & Djeffal, Christian (eds.) (2017). *IOT & TRUST – Researchers Conference Booklet*. Berlin, Germany: Humboldt Institute for Internet and Society. URL: https://www.hiig.de/en/publication/iot-trust-researchers-conference-booklet/.

[32] Hölzel, Julian (2017). Vom E-Government zum Smart Government. In: *Deutsches Verwaltungsblatt (DVBl)* 132(16), pp. 1015–1018.

[33] Djeffal, Christian (2017). Das Internet der Dinge und die öffentliche Verwaltung: Auf dem Weg zum Smart Government? In: *Deutsches Verwaltungsblatt (DVBl)* 132(13), pp.808–816.

[34] Djeffal, Christian (2017). Leitlinien der Verwaltungsnovation und das Internet der Dinge. In: Klafki, Anika et al. (eds.), *Digitalisierung und Recht*. Hamburg: Bucerius Law School Press, pp. 81–117.

collaboration with Humboldt-Universität zu Berlin and a startup, the project engaged computer engineers and lawyers to closely work together to ensure a privacy-preserving design of the technology and legal compliance already during its development. *Goodcoin* aimed at reconciling the frequently conflicting interests of consumers, who want informational self-determination, and retailers, who want to offer their customers a more personalised selection of products. The system developed enables anonymous shopping, based on innovative encryption and anonymisation procedures,[35] and at the same time leverages detailed statistical evaluations of the transactions within the system, helping retailers to better tailor their products. In the project, legal compliance was understood much broader than just covering applicable data protection law, and included the EU Payment Service Directive II (PSD II) as well as requirements formulated by regulatory authorities such as the BaFin (German Federal Financial Supervisory Authority).

The theoretical goal, which was mainly pursued at HIIG in close cooperation with other members of the C-paX research group, was to gain a deeper understanding of the relationship between legal and technical concepts in this field, in particular regarding the concepts of anonymity and anonymisation.[36] While the project's research found some overlaps between the underlying assumptions and the goals pursued. The differences between legal and technical concepts of identity, anonymity and anonymisation pose special challenges to the law's acceptance of technical implementations as a solution to the particular problems that law aims to address when it conceptualises anonymisation as a legal means for "escaping the data protection law".[37] Attempting to anonymise personal data thus requires prior assessment of the specific implications it has for fundamental rights and freedoms.[38]

DECIDE – DIGITAL IDENTITY, EUROPEAN CITIZENSHIP AND THE FUTURE OF DEMOCRACY

For a variety of reasons there is an increasing dissatisfaction of a growing number of citizens with their governmental organisations. The *DECiDe* project looked into new forms of political participation – beyond elections and formal referendums – and the potential of digital technologies for overcoming shortcomings of current governance

[35] Brack, Samuel, Dietzel, Stefan, Scheuermann, Björn (2017). ANONUS: Anonymous Bonus Point System with Fraud Detection. In: *2017 IEEE 42nd Conference on Local Computer Networks (LCN)*, pp. 356–364.

[36] Hölzel, Julian (2018). Anonymisierungstechniken und das Datenschutzrecht. In: *Datenschutz und Datensicherheit*, 42(8), pp. 502–509.

[37] Hölzel, Julian (2019). Differential Privacy and the GDPR. In: *European Data Protection Law Review* 5(2), pp. 184–196.

[38] Pohle, Jörg, & Hölzel, Julian (2020). *Anonymisierung aus Sicht des Datenschutzes und des Datenschutzrechts.* Opinion on the German Federal Commissioner for data Protection and Freedom of Information's public consultation on "Anonymisation under the GDPR with special consideration of the telecommunications sector".

models and strengthening the interaction between elected officials and their grassroots constituencies.[39] The project explored how digital identities would facilitate new forms of online as well as offline co-determination, spanning from decision-making in associations and civil society groups to e-polling and e-voting on national, European and global levels. The random sample voting tool (RSV) developed by David Chaum if combined with a sortition-based scheme as an alternative to calling to the vote the entire relevant population, could provide a digital identity-based e-voting system, which may provide for many and diverse polls and referendums without overstraining the people. It could even allow each group of selected representatives to convene in citizens› assemblies, deliberate options with their pros and cons, and decide on the motions in question. The project developed and tested a digital voting system, and examined its conformance with constitutional law including, in particular, the principle of electoral transparency and control as developed by the case law of the German Federal Constitutional Court.[40]

CONCLUSION AND FUTURE WORK

The sheer diversity of the projects undertaken and the issues addressed is remarkable. And it is no accident. The research on *Global Constitutionalism and the Internet* at HIIG was always meant to reach far beyond the confines of legal debates. This is why all projects involved more than just legal perspectives – and some hardly any. And this is why the events were always geared towards a diverse audience. No disciplinary context was out of the reach of cooperation and much time was spent translating between disciplines, engaging diverse researchers in complex debates about disciplinary differences and differing concepts and ideas. Many misunderstandings cleared up through constant interaction laid the basis for not just recognising that digital times need interdisciplinary research but actually doing it. And this is why the success of the research done is not adequately measured just by projects completed, conferences held and publications finished. The real achievement goes beyond that. Many people›s mindsets on the limits of interdisciplinary dialogue and common research projects were challenged. And even where no formal project was realized, our work pushed the limits of what was imaginable in interdisciplinarity – in and beyond the HIIG, in departments, universities and the funding agencies of academic research. It is that challenge to the system, that crowns the many achievements laid out here.

[39] Pernice, Ingolf (2016). *E-Government and E-Democracy: Overcoming Legitimacy Deficits in a Digital Europe*. HIIG Discussion Paper Series, 2016-01. URL: https://ssrn.com/abstract=2723231.

[40] Pernice, Ingolf (2019). *Digitale Abstimmung, Zufallsauswahl und das Verfassungsrecht: Zur Überbrückung der Kluft zwischen Regierung und Regierten*. HIIG Discussion Paper Series, 2019-01. URL: https://ssrn.com/abstract=3456579.

It comes as no surprise, then, that it was a former HIIG Fellow at the Global Constitutionalism and the Internet research group who set up an international Digital Constitutionalism Working Group in 2018 to continue to advance the research activities in this field. Since its inception, the working group meets online twice a quarter in order to discuss recent developments in the fields of constitutional theory and constitutionalism, constitutionalisation processes in the internet, from private ordering in social networks, controversies around intermediaries' content regulation and free speech, to internet governance.

The working group has come a long way and there is still a long way to go. We do not yet know what our future research will bring, but we can assure you with a wink:

we shall contemplate on the beaches,
we shall think on the landing grounds,
we shall conceptualize in the fields and in the streets,
we shall brainstorm in the hills;
we shall never surrender to simple-mindedness.

Constitutionalism in the Digital Age

EDOARDO CELESTE[1]

Abstract: This paper aims to introduce the notion of digital constitutionalism and, in particular, to define its relationship with contemporary constitutionalism. Constitutionalism is a historical concept, whose main values and principles have constantly evolved, and are still evolving today. Digital constitutionalism embodies the idea of projecting the values of contemporary constitutionalism in the context of the digital society. This paper assesses the transformative character of digital constitutionalism. It concludes that digital constitutionalism does not subvert the DNA of contemporary constitutionalism, but rather aims to perpetuate its core values in a form that better addresses the peculiarities of the digital society. Digital constitutionalism is not engendering a constitutional revolution, but represents a necessary evolution of contemporary constitutionalism in the context of the digital age.
Keywords: Digital revolution, constitutionalism, constitutionalisation, digital constitutionalism.

> *As the Internet is becoming the most important infrastructure for worldwide communication, constitutionalising its governance is required in order to ensure its security and resilience as well as the protection of the individual rights of all people involved, including the freedoms of information and expression, of sciences and education, intellectual property rights and the protection of data and privacy as elementary aspects of human dignity.*
>
> – Ingolf Pernice[2]

1. A NEW CONSTITUTIONAL MOMENT

A series of ongoing transformations in contemporary society are challenging existing constitutional law apparatuses. The changes prompted by the digital revolution in relation to ourselves, our relationships with other individuals and, ultimately, in the

[1] Lecturer in Law, Dublin City University; Irish Research Council Scholar, University College Dublin; former Fellow, Humboldt Institute for Internet and Society (HIIG) of Berlin. The paper represents a revised version of Chapter 5 of my PhD thesis 'Digital Constitutionalism: The Internet Bills of Rights'. This work has been funded by the Irish Research Council and the Sutherland School of Law, University College Dublin. The main ideas at the basis of this paper have been elaborated during my stay at the HIIG. I am greatly indebted to the members of the HIIG research group 'Global Constitutionalism' for the many stimulating discussions on this topic.

[2] Ingolf Pernice, 'Global Constitutionalism and the Internet. Taking People Seriously.' in Stefan Kadelbach and Rainer Hofmann (eds), *Law Beyond the State: Pasts and Futures* (Campus Verlag 2016), also available at <https://ssrn.com/abstract=2576697>, 48.

society at large ferment under a vault of constitutional norms that have been shaped for 'analogue' communities. However, the constitutional ecosystem does not lie inert. Existing constitutional settings are being modified or integrated in a way that better addresses the transformations of the digital age. We are witnessing a new constitutional moment: a complex process of constitutionalisation is currently under way.

A multiplicity of normative counteractions is emerging to address the constitutional challenges of the digital revolution. They attempt to reaffirm our core fundamental rights in the digital context and to rebalance new asymmetries of power. The increased power of states that, through the use of digital technology, have gained even more control over the lives of their citizens. But also, the power of the new 'silicon giants',[3] potent multinational companies that, by managing digital products and services, *de facto* influence the way in which we enjoy our fundamental rights. A paradigmatic example is the progressive development of data protection law. An area of law that has profound constitutional implications, as it is designed to limit the power of public and private actors to control our digital body, and in parallel aims to strengthen a series of positive rights of the individuals, such as their capability to freely develop their personality in the online world.

However, interestingly, this complex process of constitutionalisation of the digital society is not concerted centrally: there is no single constitutional framer. As in a vast construction site there are several contracting companies working at the same time, so, in a globalised environment, constitutionalisation simultaneously occurs at different societal levels. Not only in the institutional perimeter of nation-states, but also beyond: on the international plane, in the private fiefs of multinational technology companies, within the civil society. The sense of this Gordian knot of multilevel normative responses can be deciphered only if these emerging constitutional fragments are interpreted as complementary tesserae of a single mosaic. Each one surfacing with a precise mission within the constitutional ecosystem, each one compensating the shortcomings of the others in order to realise a common aim: translating the core principles of contemporary constitutionalism in the context of the digital society. Or, in other words: achieving a 'digital constitutionalism'.

The purpose of this paper is to introduce the notion of digital constitutionalism and, in particular, to define its relationship with contemporary constitutionalism. Indeed, is digital constitutionalism a new form of constitutionalism? By adapting its core values to face the mutated context of the digital society, is the constitutional ecosystem radically changing its core tenets? Does digital constitutionalism represent a constitutional revolution, or is it rather a physiological evolution of constitutionalism in the digital age?

[3] Stefano Rodotà, 'Una Costituzione per Internet?' [2010] Politica del diritto 337.

This paper will proceed in four parts. Considering the great level of ambiguity and inconsistency within the scholarship, section 2 will preliminary clarify the distinction between the notion of constitutionalism and the often interchangeably used concept of constitutionalisation. Section 3 will explain that constitutionalism is a historical concept, whose main values and principles have constantly evolved, and are still evolving today. Section 4 will then introduce the concept of digital constitutionalism and will analyse the idea of projecting the values of contemporary constitutionalism in the digital age. Lastly, section 5 will assess the transformative character of digital constitutionalism. The paper will conclude that digital constitutionalism does not represent a Copernican revolution, but a necessary evolution of contemporary constitutionalism in the context of the digital age.

2. CONSTITUTIONALISM VS CONSTITUTIONALISATION

Constitutionalisation and constitutionalism are not two interchangeable concepts. Unfortunately, the scholarship sometimes uses these two terms as synonyms.[4] Several authors attempted to systematically define the meanings of the trio constitution-constitutionalism-constitutionalisation.[5] Yet, it seems that a certain nebulosity on the matter still persists.[6] Undoubtedly, the absence of a common definition of the notion of constitution does not help.[7] Moreover, the application of these terms in the fields of international law and legal sociology has amplified their degree of semantic flexibility and further nuanced the boundaries of their expressive contours.[8]

[4] Rossana Deplano, 'Fragmentation and Constitutionalisation of International Law: A Theoretical Inquiry' [2013] European journal of legal studies.

[5] See Paul Craig, 'Constitutions, Constitutionalism, and the European Union' (2001) 7 European Law Journal 125; Anne Peters, 'Compensatory Constitutionalism: The Function and Potential of Fundamental International Norms and Structures' (2006) 19 Leiden Journal of International Law 579; Karolina Milewicz, 'Emerging Patterns of Global Constitutionalisation: Towards a Conceptual Framework' (2009) 16 Indiana Journal of Global Legal Studies 413.

[6] See Deplano (n 4); Peer Zumbansen, 'Comparative, Global and Transnational Constitutionalism: The Emergence of a Transnational Legal-Pluralist Order' (2012) 1 Global Constitutionalism 16; Anne Peters and Klaus Armingeon, 'Introduction: Global Constitutionalism from an Interdisciplinary Perspective' (2009) 16 Indiana Journal of Global Legal Studies 385; Aoife O'Donoghue, *Constitutionalism in Global Constitutionalisation* (Cambridge University Press 2014).

[7] See Herbert John Spiro, 'Constitution', *Encyclopedia Britannica* (2018) <https://www.britannica.com/topic/constitution-politics-and-law> accessed 23 October 2018; Roger A Shiner, 'Constitutions' in Enrico Pattaro (ed), *A Treatise of Legal Philosophy and General Jurisprudence*, vols 3 'Legal Institutions and Sources of Law' (Springer 2005); Dieter Grimm, *Constitutionalism: Past, Present, and Future* (Oxford University Press 2016); Giovanni Sartori, 'Constitutionalism: A Preliminary Discussion' (1962) 56 The American Political Science Review 853.

[8] See Federico Fabbrini, 'The Constitutionalization of International Law: A Comparative Federal Perspective' (2013) 6 European journal of legal studies 7; Jan Klabbers, Anne Peters and Geir Ulfstein, *The Constitutionalization of International Law* (Oxford University Press 2009); Christoph B Graber, 'Bottom-up Constitutionalism: The Case of Net Neutrality' (2016) 7 Transnational Legal Theory 524; Chris Thornhill, *A Sociology of Constitutions: Constitutions and State Legitimacy in Historical-Sociological Perspective* (Cambridge University Press 2013); Gunther Teubner, *Constitutional Fragments: Societal Constitutionalism and Globalization* (Oxford University Press 2012).

However, it is possible to present a basic distinction between the two concepts, on which the scholarship seems to generally agree.

The concept of constitutionalisation denotes a process.[9] The suffix –isation characterises a procedure, an operation; it implies the idea of advancement, progression, and evolution. It may have occurred in the past, be still ongoing, or be advocated in a normative sense for the future. Conversely, constitutionalism is a 'theory',[10] a 'movement of thought',[11] a 'conceptual framework',[12] a 'set of values',[13] an 'ideology'.[14] Again, an analysis of the term itself can be of help. The suffix –ism does not imply the idea of process; it denotes a more static concept.[15] An ism is a 'a distinctive practice, system, or philosophy, typically a political ideology or an artistic movement'.[16] Neglecting for a moment the question of what the actual principles of constitutionalism – the aims of this ideology – are, one could argue that, lato sensu, constitutional-isation is the process of implementation of constitutional-ism. Constitutionalisation would put into effect the values of constitutionalism or, regarded the other way around, constitutionalism would provide the principles that permeate, guide, inform constitutionalisation.[17]

3. THE VALUES OF CONSTITUTIONALISM

Constitutionalism evolves. This concept does not denote a process, as we have seen, but this does not contradict the fact that its underlying values, ideals, principles have changed over time. The notion of constitutionalism emerged at the beginning of the nineteenth century as a response to absolute monarchy and popular despotism.[18] It

[9] See Girardeau A Spann, 'Constitutionalization' [2004] Saint Louis University Law Journal 709; Milewicz (n 4); Garrett Wallace Brown, 'The Constitutionalization of What?' (2012) 1 Global Constitutionalism 201; Aoife O'Donoghue, 'Alfred Verdross and the Contemporary Constitutionalization Debate' (2012) 32 Oxford Journal of Legal Studies 799; Antje Wiener and others, 'Global Constitutionalism: Human Rights, Democracy and the Rule of Law' (2012) 1 Global Constitutionalism 1.

[10] Jeremy Waldron, 'Constitutionalism: A Skeptical View' [2010] Philip A. Hart Memorial Lecture <https://scholarship.law.georgetown.edu/hartlecture/4>; see also Pernice (n 2) 7, according to whom constitutionalism is a form of 'theoretical thinking'.

[11] Marco Bani, 'Crowdsourcing Democracy: The Case of Icelandic Social Constitutionalism' (Social Science Research Network 2012) SSRN Scholarly Paper ID 2128531 <https://papers.ssrn.com/abstract=2128531> accessed 15 August 2019.

[12] Zumbansen (n 6).

[13] O'Donoghue (n 6).

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

[15] See Waldron (n 10); Milewicz (n 5).

[16] *Oxford Dictionary of English* (Third Edition, Oxford University Press 2010).

[17] Celeste, 'Digital Constitutionalism' (n 14).

[18] András Sajó and Renáta Uitz, *The Constitution of Freedom: An Introduction to Legal Constitutionalism* (Oxford University Press 2017) ch 1; Harold J Berman, *Law and Revolution. The Formation of the Western Legal Tradition* (Harvard University Press 1983); Graber (n 8).

advocated the adoption of a constitution, a written legal text establishing the fundamental law of a country, and, at the same time, its primacy over the discretion of rulers.[19] The power of the government should be legitimated by the constitution, an expression of popular sovereignty, and should be bound by the constitution, which represents its ultimate limit.[20] No actor in society should detain at the same time the legislative, executive and judiciary power.[21] No ruler should be *ab-solutus*, unrestricted from the control of other institutional organs whose power derives from the constitution. At the outset, constitutionalism was an ideology, a movement of thought that claimed the values of the rule of law and the separation of power.

This normative vision of society championed by the original constitutionalism was subsequently enriched with other ideals. Democracy definitively supplanted other forms of government and established itself as a foundational value.[22] Besides a negative, limitative approach, claiming the restriction of the power of rulers by law and the institution of a system of checks and balances, constitutionalism also developed a positive aspect, pivoting around individual empowerment.[23] In this way, the ultimate mission of constitutionalism, the limitation of power, was re-oriented towards the protection of fundamental rights and, ultimately, the safeguarding of human dignity.[24]

Looking back before the nineteenth century, one could identify forms of constitutionalism within other ages. One could talk of a Greek or Roman constitutionalism, for instance.[25] However, this intellectual exercise is only possible analogically and by extension. Gerhard Casper rightly observed that

> constitutionalism does not refer simply to having a constitution, but to having a particular kind of constitution.[26]

When one thinks of constitutionalism, one generally implies the values underlying contemporary constitutionalism, the ideology that progressively developed from the big revolutions of the end of the eighteenth century. Constitutionalism is today syn-

[19] See Milewicz (n 5); Sajó and Uitz (n 18) chs 1 and 8; Berman (n 18); Peters (n 5).

[20] See Waldron (n 10); András Sajó, *Limiting Government: An Introduction to Constitutionalism* (Central European University Press 1999); Wil Waluchow, 'Constitutionalism' in Edward N Zalta (ed), *The Stanford Encyclopedia of Philosophy* (Spring 2018, Metaphysics Research Lab, Stanford University 2018) <https://plato.stanford.edu/archives/spr2018/entries/constitutionalism/> accessed 16 August 2019; Peters (n 5).

[21] See Richard Bellamy, 'Constitutionalism', *Encyclopædia Britannica* (2019) <https://www.britannica.com/topic/constitutionalism> accessed 16 August 2019.

[22] See Sajó and Uitz (n 18) ch 3; Nicholas W Barber, *The Principles of Constitutionalism* (Oxford University Press 2018) ch 6; see also Pernice (n 2).

[23] See Barber (n 22) ch 1; Waldron (n 10).

[24] See Sajó and Uitz (n 18) chs 1 and 10; Milewicz (n 5); Pernice (n 2).

[25] See Charles Howard McIlwain, *Constitutionalism: Ancient and Modern* (Amagi, originally published by Cornell University Press, 1947, 2007).

[26] Gerhard Casper, 'Constitutionalism' in Leonard W Levy; Karst L Kenneth and Dennis J Mahoney (eds.), *Encyclopedia of the American Constitution* (1986th edition, Macmillan) 474.

onymous with the values of democracy, the rule of law and the separation of powers. Constitutionalism is associated with the idea of the protection of all fundamental rights that have been gradually recognised over the past few centuries, be they civil, political, socio-economic or cultural.[27] However, what today no longer holds true is the necessary connection of the idea of constitutionalism with the nation state.

The values of constitutionalism historically ripened in the context of the state.[28] However, over the past few decades, in a society that has become increasingly more global, the centrality of the state has faded due to the emergence of other dominant actors in the transnational context.[29] The scholarship has therefore started to transplant the constitutional conceptual machinery beyond the state, including the concept of constitutionalism.[30] The myth of the compulsory link between constitutionalism and the state is debunked.[31] As Hamann and Ruiz Fabri state, today 'it appears that any polity can be endowed with or can acquire constitutional features'.[32] Consequently, the constitutional ecosystem becomes plural, composite and fragmented.[33] If the values of constitutionalism remain the same in their essence, their articulation in specific contexts, within and beyond the state, necessarily becomes 'polymorphic'.[34]

4. DIGITAL CONSTITUTIONALISM

Contemporary constitutionalism was not extracted from the rock of history as a monolithic marble block. Constitutionalism developed more like an onion. Its inner fundamental values progressively shaped further external layers: principles budding to face the emerging complexities of the society. In the words of Chris Thornhill:

> Constitutional norms are constructed as layers within the evolving inclusionary structure of the political system; new constitutional norms are articulated, progressively, as society's political system is exposed to challenges and demands, which it cannot absorb, and as it requires additional normative complexity to sustain its functions of

[27] See Sajó and Uitz (n 18) chs 1 and 10.

[28] See Grimm (n 7).

[29] See Petra Dobner and Martin Loughlin (eds), *The Twilight of Constitutionalism?* (Oxford University Press 2010).

[30] See Grimm (n 7) chs VII and VIII.

[31] See Ulrich K Preuss, 'Disconnecting Constitutions from Statehood: Is Global Constitutionalism a Viable Concept?' in Petra Dobner and Martin Loughlin (eds), *The Twilight of Constitutionalism?* (Oxford University Press 2010).

[32] A Hamann and H Ruiz Fabri, 'Transnational Networks and Constitutionalism' (2008) 6 International Journal of Constitutional Law 481, 503.

[33] Neil Walker, 'The Idea of Constitutional Pluralism' (2002) 65 The Modern Law Review 317; Teubner (n 8); see also Paul Blokker, 'Modern Constitutionalism and the Challenges of Complex Pluralism' in Gerard Delanty and Stephen P Turner (eds), *Routledge International Handbook of Contemporary Social and Political Theory* (Routledge 2011) <https://papers.ssrn.com/abstract=1719258> accessed 22 August 2018.

[34] See Walker (n 33).

> inclusion. The key to understanding constitutions, in consequence, is to examine constitutional norms as a historically constructed, adaptive apparatus, which is closely correlated with distinct *inclusionary pressures* in society.[35]

Today, analogue constitutional principles cannot anymore solve all the challenges of the digital society. The external shape of constitutionalism necessarily changes again. New constitutional layers are progressively added to those already in existence. Novel principles emerge to articulate the fundamental values of constitutionalism in light of the problematic issues of contemporary society.[36] The scale of transformation prompted by the advent of the digital revolution is such that one can neatly distinguish the multiplicity of new normative layers embracing or even incorporating older ones. A fresh sprout within the constitutionalist theory: what one could call 'digital constitutionalism'.

Digital constitutionalism is 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.[37] At first sight, however, such a descriptor could appear as misleading.[38] The adjective 'digital' does not directly qualify the substantive 'constitutionalism'. It is not akin to expressions such as 'democratic constitutionalism' or 'liberal constitutionalism' in which, respectively, democracy and liberalism characterise a newly acquired orientation of the theory of constitutionalism.[39] 'Digital' is rather an adverbial conveying the idea that one is referring to that strand of the constitutional theory that seeks to articulate principles for the digital society.[40] Similarly, the scholarship has talked of 'global' or 'international' constitutionalism.[41]

The notion of 'digital constitutionalism', and, more broadly, the idea of project-

[35] Thornhill (n 8) 9,

[36] Cf. Osvaldo Saldías, 'Patterns of Legalization in the Internet: Do We Need a Constitutional Theory for Internet Law?' (Social Science Research Network 2012) SSRN Scholarly Paper ID 1942161 paras 5–6 <https://papers.ssrn.com/abstract=1942161> accessed 19 August 2019.

[37] First formulated in this sense in 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; subsequently revised and amplified in Celeste, 'Digital Constitutionalism' (n 14). In this last paper, at 88, I defined 'digital constitutionalism' as 'the ideology which aims to establish and to ensure the existence of a normative framework for the protection of fundamental rights and the balancing of powers in the digital environment'.

[38] See Edoardo Celeste, 'What Is Digital Constitutionalism?' (*HIIG Science Blog*, 31 July 2018) <https://www.hiig.de/en/what-is-digital-constitutionalism/> accessed 31 August 2018.

[39] See Blokker (n 33); Michael W Dowdle and Michael Wilkinson (eds), *Constitutionalism beyond Liberalism* (Cambridge University Press 2016).

[40] In these terms, Celeste, 'What Is Digital Constitutionalism?' (n 38); Celeste, 'Digital Constitutionalism' (n 14).

[41] See, ex multis, Jan Klabbers, 'Constitutionalism Lite' (2004) 1 International Organizations Law Review 31; Ronald MacDonald and Douglas Johnston (eds), T*owards World Constitutionalism: Issues in the Legal Ordering of the World Community* (Brill 2005); Peters (n 5); CEJ Schwöbel, 'Situating the Debate on Global Constitutionalism' (2010) 8 International Journal of Constitutional Law 611.

ing constitutionalism in the context of the digital environment, is not new. However, the scholarship employed this concept in an inconsistent way.[42] Fitzgerald talked of 'informational constitutionalism' to denote state law, in particular in the fields of intellectual property, competition, contracts and privacy, aiming to limit the power of tech companies to self-regulate.[43] For Berman, 'constitutive constitutionalism' advocates for an expansion of the reach of US constitutional law to encompass those private actors.[44] In Suzor, 'digital constitutionalism' is a project seeking to articulate a set of limits on private powers that affect how individuals can enjoy their rights in the digital world. The values of state constitutional law would inform the adoption of ordinary statutes imposing a series of minimal guarantees that tech companies should respect in self-regulating their products and services.[45] Karavas praised a form of digital constitutionalism without the state, or, at least, with its intervention kept to a minimum. The communities of cyberspace should be able to self-constitutionalise themselves in a bottom-up and incremental way. State judges should play only a maieutic role, socratically teaching what the basic rules in creating valid constitutional norms are.[46] Redeker, Gill and Gasser, lastly, employed the notion of digital constitutionalism to connect the emergence of a series of non-binding declarations of Internet rights which aim to set limits on both public and private power in the digital context.[47]

At first sight, all of these interpretations of digital constitutionalism appear different. However, they are not incompatible as, if comprehensively regarded, they reveal themselves as multiple facets of a broader unitary picture.[48] They all deal with the issue of the limitation of power of dominant actors and, when considered together, they recognise the existence of a plurality of normative instruments translating constitutional values in the digital society, both emerging in the state context, such as constitutional and ordinary law, and beyond, as in the case of private companies'

[42] For a comprehensive and detailed analysis of the literature on the topic, see Celeste, 'Digital Constitutionalism' (n 14).

[43] See Brian Fitzgerald, 'Software as Discourse? A Constitutionalism for Information Society' (1999) 24 Alternative Law Journal 144.

[44] 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.

[45] See Nicolas Suzor, 'Digital Constitutionalism and the Role of the Rule of Law in the Governance of Virtual Communities' (phd, Queensland University of Technology 2010) <https://eprints.qut.edu.au/37636/> accessed 30 August 2018; Nicolas Suzor, 'The Role of the Rule of Law in Virtual Communities' (2010) 25 Berkeley Technology Law Journal 1817.

[46] See 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).

[47] 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; for a critical analysis, see Celeste, 'Digital Constitutionalism' (n 14).

[48] See Celeste, 'Digital Constitutionalism' (n 14) para 4.

self-regulation. Ultimately, these various readings provide plausibility for the wider vision that sees digital constitutionalism as the theoretical strand of contemporary constitutionalism that is adapting core constitutional values to the needs of the digital society. Digital constitutionalism advocates the perpetuation of foundational principles, such as the rule of law, the separation of powers, democracy and the protection of human rights, in the mutated scenario of the digital society. It triggers a complex process of constitutionalisation of the virtual environment, which occurs through a multiplicity of constitutional counteractions, both within and beyond the state. Century-old values are translated in normative principles that can speak to the new social reality. Digital constitutionalism reiterates that digital technology does not create any secluded world where individuals are not entitled to their quintessential guarantees.

5. A NEW CONSTITUTIONALISM?

Digital constitutionalism represents the conceptual lymph of the current constitutional moment. It normatively advocates a reconfiguration of the constitutional framework. Analogue norms are no longer able to address the full range of complexities of the virtual environment. A series of normative counteractions are emerging to implement the principles of a constitutionalism rethought for the digital age. The current constitutional moment, too, has a 'transformative impact'.[49] Core constitutional values are generalised and subsequently re-specified in light of the characteristics of the contemporary society.[50] Constitutionalism is translated in a language that speaks to the actors of the virtual environment. In this way, old principles become more easily applicable in new societal contexts. Further corollaries, and even novel norms emerge to express foundational constitutional values in the digital society.

This process of constitutionalisation is still ongoing; yet, it is legitimate to ask: are we facing an evolution or a *r*-evolution of contemporary constitutionalism? Is reshaping constitutionalism for the digital age merely a way to enhance its fitness vis-à-vis the mutated conditions of the social reality? Or does it imply a more radical change of paradigm?

The extended scope of digital constitutionalism in comparison with its analogue version could be mentioned as apparent evidence of the revolutionary nature of the current constitutional moment. Constitutionalism is no longer anchored to the nation state. In the digital age, it promotes ways to limit the power of all dominant

[49] JHH Weiler, *The Constitution of Europe: 'Do the New Clothes Have An Emperor?' And Other Essays on European Integration* (Cambridge University Press 1999) 4.

[50] The idea of a process of generalisation and re-specification of constitutional principles was first advanced in Gunther Teubner, 'Societal Constitutionalism; Alternatives to State-Centred Constitutional Theory?' in Christian Joerges, Inger-Johanne Sand and Gunther Teubner (eds), *Transnational Governance and Constitutionalism. International Studies in the Theory of Private Law* (Hart 2004); see also Teubner (n 8); Celeste, 'Digital Constitutionalism' (n 14).

actors, be they public or private.[51] Overlooking the capability of non-state actors to affect individual rights would be anachronistic, and would ultimately fail to safeguard human dignity, which can be equally violated by public and private hands.[52]
According to Suzor, the present circumstances would necessarily require 'a new constitutionalism'.[53] One is tempted to evoke the advent of a new form of constitutionalism because constitutional moments generally represent the apex of a transformative process. Adaptations and transformations have always been integral components of the vital cycle of constitutionalism. However, today, constitutional counteractions emerge in response to a digital revolution that is violently shaking the existing constitutional architecture. Existing constitutional norms, which were shaped for an analogue society, are under unprecedented stress. One therefore envisages the need for immediate, drastic transformations. Digital constitutionalism would represent an appeal to urgently take a remedial action: a last minute, normative SOS.[54]

If the digital revolution is regarded as a looming and inexorable cataclysm, the extent of the constitutional change is dramatized too. The constitutional ecosystem has still to fully realise the severity of the storm that it has started to navigate. It has waited until the last minute to understand the necessity to react against the challenges of the digital revolution, and now one has the impression that the normative transformations needed will represent a Copernican revolution.

Certainly, the emergence of constitutional counteractions is not evidence that supports the vision of a constitutional ecosystem that is riding the digital revolution on the crest of the wave – this is true. However, from an objective standpoint, the current constitutional moment does not represent a radical upheaval.[55] We are not facing a change of paradigm that is indelibly transforming the shape of our constitutional identity. We are not witnessing a transition from democracy to technocracy, for example.[56] Digital constitutionalism does not advocate a *tabula rasa* of our core constitutional values. On the contrary, it is deeply rooted in these foundational principles.

Digital constitutionalism champions their translation in the context of the dig-

[51] See Fitzgerald (n 43).

[52] Celeste, 'Digital Constitutionalism' (n 14) paras 3.5 and 4.2; see also Redeker, Gill and Gasser (n 47); cf. 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> accessed 30 August 2018, where a conception of digital constitutionalism still anchored to the idea of limitation of power of public actors is present.

[53] Nicolas Suzor, *Lawless. The Secret Rules That Govern Our Digital Lives* (Cambridge University Press 2019) 9, original emphasis.

[54] See Teubner (n 8) 82.

[55] See Celeste, 'Digital Constitutionalism' (n 14) para 2.

[56] See Emilio Castorina, 'Scienza, tecnica e diritto costituzionale' [2015] Rivista AIC <http://www.rivistaaic.it/la-scienza-costituzionalistica-nelle-transizioni-istituzionali-e-sociali.html>.

ital society. Innovation, of course, occurs – it suffices to think to the fact that digital constitutionalism seeks to limit the power of private actors too. The societal context unavoidably imposes similar changes. However, this does not subvert the original constitutional paradigm founded on the values of democracy, the rule of law, the separation of powers, and the protection of human rights. Digital constitutionalism perpetuates these constitutional principles in a mutated social reality: in the digital society, the DNA of contemporary constitutionalism is ultimately preserved.

Harnessing Artificial Intelligence the European Way

CHRISTIAN DJEFFAL

Ingolf Pernice is generally acknowledged as a great European and a master of European law. In the last 10 years, he has also become an expert on law and digital technologies, especially on questions of the internet. While some might consider this as something of a change or switch in a long and successful career, one might also think that Europe and technology actually are interlinked. In the latter view, Ingolf Pernice was just a forerunner and an early adopter of the increased importance of digitization for Europe and European law. In fact, the European project has always been about technologies and to be more precise, about the value-sensitive design and use of technologies. Two of the three communities forming the basis of European law had a direct relation to technology. The European Community for Coal and Steel was a supranational authority regulating industrial production and the use of coal and steel. The European Atomic Energy Community (EuroAtom) is still in existence today. It is an international organization with a broad scope of competences regarding nuclear energy production, distribution and sale. Yet, even the European Economic Community has engaged in many activities that shaped innovation, development, use, and sale of technology in Europe. In that view, the recent activities of the EU concerning digital technologies are rather an extension of activities than something genuinely new. The theme of integration through law has become a well-known concept in European Studies. Maybe, the process of European integration has always been about integration in the face of technological change. One of the latest developments in that regard are the developments regarding artificial intelligence. There have been many developments recently and 10 April 2018 might go down as one of the most important dates in recent history. On that date, the Declaration on Cooperation in Artificial Intelligence[1] was signed (European Commission, 2018).

During the European Union's second Digital Day in Brussels, this informal agreement was signed by 25 states including the United Kingdom and Norway. The signatories of the declaration believe that the development of AI will have a great impact on their future. AI applications are already ubiquitous in daily life. Think about the assistant on your mobile phone and ever smarter robots (BostonDynamics, 2017). The discussions about lethal autonomous weapons systems remind us that AI can also be a question of life and death. In the context of the rising importance of AI

[1] http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=50951.

and the increased willingness to influence its development (Gasser & Almeida, 2017) also on the highest political levels (Thompson, 2018), the Declaration represents a new and unique approach.

At first sight, this document seems to be quite unspectacular: on no more than three pages, it lists three general areas of cooperation – AI research, its economic impacts and social issues – and 14 more specific measures. What is special is the declaration's specific integrative approach. Unlike discussions about AI on the international plane, the declaration aims to integrate countries, research and development and policy areas.

The declaration is a collaboration of EU member states including the United Kingdom which is about to leave the Union, and Norway, which is not a member. They agree to form a "comprehensive and integrated European approach on AI".

In the current strategic debate about AI on the international plane, one usually finds positions that emphasize competition rather than integration. The Russian president Vladimir Putin famously stated at the Russian Children on Knowledge day that "whoever becomes the leader in this sphere will rule the world and it would not be desirable that this monopoly be concentrated in someone's hands" (Russia Insight, 2017). China has published its strategy to become the leading nation by 2030 (Mozur, 2017). The UK's Prime Minister Theresa May stated at the World Economic Forum that she was "establishing the UK as a world leader in Artificial Intelligence" (May, 2018).

To some these views of states bear some resemblance to the arms race of the cold war when states struggled for technological superiority (Stavridis, 2016; Straub, 2018a, 2018b). Yet, the Declaration resembles more the community of coal and steel than a nuclear arms race. The first Digital Day in 2017 marked the 60th anniversary of the Treaties of Rome, which were built on the European Coal and Steel Community. Speeches held at the event often referred to digital technology as having the potential for integrative effects like coal and steel for Europe after the second world war (European Commission, 2017). European countries combined their coal and steel industries and created a supranational authority with own competences to govern this area. This was a key factor to establish mutual trust between states. While the empowerment of states through AI is often compared to nuclear technology, coal and steel might prove to be a better metaphor: Coal is used to produce steel like data is used for the training in many AI technologies. Like AI, steel can be the basis of artefacts having many purposes. Steel can be turned into swords and ploughshares. AI can be the basis for nursing robots and automated lethal weapon systems. So, it might be better not only to share the knowledge about AI technologies, but to work together in exploring, designing and using them.

The second area of integration is the integration of research. This has economic

and scientific aspects. The signatory states agree to establish new digital innovation hubs, but also to reinforce existing research centers on AI and support their pan-European dimension. Therefore, the research should be organised in a decentralised and interconnected way which might one day even include states outside Europe. One of those institutions could be the envisaged French-German centre for AI, which is also part of the German coalition agreement between the governing parties. Contrast this with the more centralist plans of the Chinese government to spend 2.1 billion US $ to build a technology park covering 54.87 hectares in China's capital Beijing (Yamei, 2018). In a more centralist structure, collaboration is of course possible (Burchardt, 2018). In an integrated rather than federalist structure, it is a necessity. Research, development and innovation funding is also part of the declaration. In his speech at the Sorbonne, the French President Emmanuel Macron went as far as calling for a European agency for disruptive innovation (Macron, 2017). The only technology he mentioned in that context was artificial intelligence. Yet, an integrative approach does also deal with knowledge distribution: The AI resulting from this research has to be made available to different parts of society such as public administration and companies with less AI capabilities.

The third level of integration relates to policy areas. According to the theory of functional integration, integration of one policy area spills over into the next. Economic collaboration could be a first step for states to work together in other areas. The first three areas mentioned in the declaration can be compared to the three big areas of European integration: The Community of Coal and Steel integrated resources and technology, this spilled over to the European Economic Community integrating the several national markets in Europe. The third step was an increasing political and social integration resulting in the European Union.

What is special about the declaration is that it has an integrative view on technology, economy and society. AI technologies are not to be viewed separately from other areas but as a whole. This integrated view does not give precedence to innovation, economic benefits, governance, design or accountability. It tries to deal with all aspects at the same time. Such an integrated approach is mindful of the embeddedness of technology in society. The focus of development of important and relevant technologies must be on their impacts from the start of the design process. It is a process of constant learning. The level of integration envisaged in the declaration is, however, nuanced: the countries agreed to exchange views on ethical and legal frameworks. That leaves some leeway for each respective country. They, however, also agreed that humans must remain in the centre of development, deployment and decision making of AI. These two aspects mirror the idea of unity in diversity in Europe. Convergent ethical and legal frameworks and human-centricity could become

part of the nucleus of a particular European stance towards the future of AI, which could turn out to be an important part of our future.

At the moment, there are many initiatives aiming to guide the development of AI in a sustainable and ethically responsible way. What makes the declaration special is that it represents also an idea how to get there. It is a translation and adaption of the European idea of integration. Whether 10 April 2018 will become a date mentioned in future history books – or their functional digital equivalents – is hard to predict. It is my hope that looking back, we will have forgotten Zuckerberg's tie and remember this day as part of a series of events that helped to ensure a responsible and sustainable development of AI for the common good.

This text is an extended version of Djeffal, Christian: *Harnessing Artificial Intelligence the European Way*, VerfBlog, 2018/4/25, https://verfassungsblog.de/harnessing-artificial-intelligence-the-european-way/, DOI: 10.17176/20180425-075748.

REFERENCES:

BostonDynamics. (2017). What's new, Atlas? Retrieved from https://www.youtube.com/watch?v=fRj34o4hN4I.

Burchardt, D. A. (2018). Pekinger Vize-Bürgermeister besucht DFKI Berlin: Kooperationsvertrag verstärkt Zusammenarbeit. *idw - Informationsdienst Wissenschaft*. Retrieved from https://idw-online.de/de/news693049.

European Commission. (2017). Digital Day. Retrieved from https://ec.europa.eu/digital-single-market/en/digital-day.

European Commission. (2018). EU Member States sign up to cooperate on Artificial Intelligence. Retrieved from https://ec.europa.eu/digital-single-market/en/news/eu-member-states-sign-cooperate-artificial-intelligence.

Gasser, U., & Almeida, V. A. (2017). A layered model for AI governance. *IEEE Internet Computing, 21*(6), 58-62. doi:10.1109/mic.2017.4180835.

Macron, E. (2017). Sorbonne Speech of Emmanuel Macron—Full text/English Version. *Ouest France*. Retrieved from http://international.blogs.ouest-france.fr/archive/2017/09/29/macron-sorbonne-verbatim-europe-18583.html.

May, T. (2018). PM's speech at Davos 2018: 25 January. Retrieved from https://www.gov.uk/government/speeches/pms-speech-at-davos-2018-25-january.

Mozur, P. (2017). Beijing Wants AI to be Made in China by 2030. *New York Times*. Retrieved from https://www.nytimes.com/2017/07/20/business/china-artificial-intelligence.html.

Russia Insight. (2017). Whoever leads in AI will rule the world!- Putin to Russian children on Knowledge Day. Retrieved from https://www.youtube.com/watch?v=2kggRND8c7Q.

Stavridis, J. (2016). Are we entering a new Cold War. *Foreign Policy*. Retrieved from https://foreignpolicy.com/2016/02/17/are-we-entering-a-new-cold-war-russia-europe/.

Straub, J. (2018a). Artificial intelligence is the weapon of the next Cold War. *The Conversation*. Retrieved from https://theconversation.com/artificial-intelligence-is-the-weapon-of-the-next-cold-war-86086.

Straub, J. (2018b). The Weapon of the Next Cold War: Artificial Intelligence. *The Wire*. Retrieved from https://thewire.in/external-affairs/weapon-next-cold-war-artificial-intelligence.

Thompson, N. (2018). Emmanuel Macron Talks to Wired About France's AI Strategy. *Wired*. Retrieved from https://www.wired.com/story/emmanuel-macron-talks-to-wired-about-frances-ai-strategy/.

Yamei. (2018). Beijing to build technology park for developing artificial intelligence. *Xinhuanet*. Retrieved from http://www.xinhuanet.com/english/2018-01/03/c_136869144.htm.

Digitalisierung, Öffentlichkeit, Demokratie – drei Thesen

JEANETTE HOFMANN

THESE 1: DIE DEMOKRATIE IST EINE MEDIATISIERTE HERRSCHAFTSFORM

Dass die Demokratie eine mediatisierte Herrschaftsform ist, klingt nach einer trivialen Beobachtung, wenn man bedenkt, dass alle menschliche Wahrnehmung, Kommunikation und Handlung medial vermittelt ist. Sei es durch den menschlichen Körper und seine Sinne, sei es durch gesellschaftliche Institutionen und Technologien, die gesellschaftliches Handeln vielfach erst möglich machen, Medien vollbringen, was Sybille Krämer (1998: 559) als „Distanzleistungen" bezeichnet hat. In diesem Sinne verweist die erste These nicht auf einen bestimmten Typ der Demokratie, etwa auf die digitale Demokratie, von der inzwischen öfter die Rede ist, sondern sie akzentuiert eine spezifische Beobachtungsperspektive, nämlich auf die Rolle, die Medien für die Realisierung von Demokratie spielen. Die repräsentative Demokratie, so der Gedanke, der der ersten These zugrunde liegt, ist ohne einen spezifischen Typ von Verbreitungsmedien gar nicht vorstellbar: Es muss Verbreitungsmedien wie die Schrift und den Buchdruck geben, um politische Verständigung über größere regionale Distanzen zu realisieren. Eine solche medienorientierte Perspektive auf die Demokratie ist zumindest in der Politikwissenschaft bislang unterentwickelt. Es gibt keine systematische Forschung über den Zusammenhang von Medien und demokratischer Selbstbestimmung.

Dem amerikanischen Politikwissenschaftler Benedict Anderson (1983) verdanken wir die Einsicht, dass die Entstehung nationaler Gemeinschaften, „imagined communities" in seiner Terminologie, und somit auch des Nationalstaats das Aufkommen des „Printkapitalismus" zur Voraussetzung hat. Verbreitungsmedien wie die Tageszeitung ermöglichen erst, dass alle Bürger zur gleichen Zeit die gleichen politischen Nachrichten studieren – in dem Bewusstsein, dass viele andere Menschen dies auch tun. Gleichzeitigkeit und Vernetzung, so Anderson, bilden wichtige Elemente in der Herausbildung nationaler Gemeinschaften. Aber auch in einem ganz materiellen Sinne ist eine öffentliche Sphäre über größere räumliche Distanzen auf Kommunikationsmedien angewiesen. Ohne eine öffentliche Sphäre kann es wiederum keine zeitnahe Verbreitung politischer Nachrichten, keinen politischen Diskurs und folglich auch keinen nationalen Demos geben. Repräsentative Demokratie und Kommunikationsmedien können daher als sich wechselseitig konstituierende Einheit verstanden werden: Massenmedien schaffen die Voraussetzung für die territorialstaatliche Demokratie; umgekehrt prägt das moderne Demokratieverständnis

mit seinen Anforderungen an Inklusivität und Transparenz politischer Prozesse die Formate und Publikationsrhythmen der Kommunikationsmedien.

Es gibt jedoch noch einen zweiten, auf die Eigenschaften von Medien selbst verweisenden Grund, warum der Zusammenhang zwischen Medien und Demokratie nicht trivial ist. Medien ermöglichen nicht nur bestimmte Kommunikations- oder Koordinationsformen, sondern sie schließen ebenso viele andere, zumindest prinzipiell mögliche Varianten aus. Medien sind mit anderen Worten performativ; sie übertragen Kommunikationsinhalte nicht bloß, sondern sie wirken auf die Art und Weise der Kommunikation und ihre Inhalte unmittelbar ein: „the medium ist the message" (McCluhan 1964).

In der Medienwissenschaft wie auch der Systemtheorie beruft man sich auf die Unterscheidung zwischen Medium und Form, um die Selektivität von Medien zu erfassen. Medien wie die Sprache schaffen Möglichkeitsräume, aus denen spezifische Formen wie Wörter, Sätze, aber auch die Schrift hervorgehen. In der Systemtheorie spricht man in diesem Kontext von losen und festen Kopplungen (Luhmann 1997). Andere Kopplungen wären jeweils möglich gewesen, aber diese sind uns für gewöhnlich nicht präsent, denn die Form steht immer im Vordergrund, während das Medium als Möglichkeitsraum unsichtbar und in seinen Grenzen unbestimmbar bleibt. Ein bekanntes Beispiel für dieses Verhältnis aus Medium und Form ist Berthold Brechts sogenannte Radiotheorie, die in den frühen Tagen des Internets wieder an Popularität gewann. Seine Theorie lief auf eine Neukonfiguration des Rundfunks hinaus, die den „Distributionsapparat" in einen „Kommunikationsapparat" des öffentlichen Lebens transformiert – realisiert als ein „ungeheures Kanalsystem", das den vereinzelten Zuhörer zu einem Sprechenden macht, der sich mit anderen Sprechenden darüber in Beziehung setzen kann (Brecht 1992: 129). Brechts Theorie erkundete das Medium Rundfunk und kritisiert seine restriktive Form, die One-to-many-Kommunikation. Medien sind also performativ in dem Sinne, dass sie Neues wie nationale Öffentlichkeiten und „Zuschauerdemokratien" schaffen, aber vermittels ihrer Formen zugleich ausschließend wirken, indem sie andere mögliche Kommunikations- und Beteiligungsformen unwahrscheinlich machen.

THESE 2: DIGITALISIERUNG, ÖFFENTLICHKEIT UND DEMOKRATIE ENTWICKELN SICH KOEVOLUTIONÄR – INTERDEPENDENZ STATT KAUSALBEZIEHUNG

Spätestens seit dem britischen Brexit-Referendum und der Wahl von Trump bei den letzten US-Wahlen ist die Beziehung zwischen Demokratie und Digitalisierung erneut auf die politische Tagesordnung gerückt. Im Unterschied zu den 2000er Jahren, als das Internet als Ressource für die Demokratie wahrgenommen wurde (Stichwort „Arabischer Frühling"), stehen derzeit die Bedrohungen digitaler Technologien

für die Demokratie im Vordergrund. Das Erstarken populistischer Parteien und Bewegungen, aber auch neue Formen der Wähleransprache und Manipulation wie Micro-Targeting oder Social Bots werden als Belege dafür angeführt, dass die Digitalisierung mittlerweile zur Gefahr für die Demokratie geworden ist. Demokratie und Digitalisierung werden hierbei als zwei voneinander unabhängige Entitäten wahrgenommen und in eine kausale Beziehung zueinander gesetzt. Demnach stellt die digitale Technik eine unabhängige Kraft dar, die auf das demokratische Gemeinwesen und seine Institutionen einwirkt und diese stärkt, schwächt oder gar unterläuft. Diese Sichtweise schreibt der Digitalisierung nicht nur ein bemerkenswertes Maß Autonomie zu, sie verkennt auch die enorme Kontingenz oder Entwicklungsoffenheit, die dieser innewohnt.

Benedict Anderson hat die Formierung nationaler Gemeinschaften denn auch nicht der Ausbreitung der Drucktechnik zugeschrieben, sondern auf die Entstehung des „print capitalism" verwiesen. Diesen kann man sich als Konstellation vorstellen, in der sich verschiedene gesellschaftliche, technische, kulturelle und wirtschaftliche Entwicklungen gebündelt haben. Dazu gehört die Drucktechnik, aber ebenso die Säkularisierung, die ein Interesse an neuen Typen von Druckerzeugnissen wie Literatur und Zeitungen weckt, das Verlegerkapital, das die Gründung von Zeitschriften ermöglicht und nicht zuletzt die Alphabetisierung und Herausbildung von überregionalen Sprachgemeinschaften, die unabdingbar für die Entwicklung nennenswerter Absatzmärkte für Druckerzeugnisse waren.

Bezogen auf die Frage nach dem Verhältnis von Demokratie und Digitalisierung ist Andersons Printkapitalismus relevant, weil er der Drucktechnik zwar eine essentielle, aber keine exklusive Rolle zuschreibt. Ohne die anhaltende Säkularisierung etwa hätte sich die Drucktechnik sicherlich in einer anderen Form ausdifferenziert. Diese Feststellung lässt sich dahingehend verallgemeinern, dass Technologien ihr spezifisches Funktionsspektrum bzw. ihre Form jeweils als Bestandteil größerer gesellschaftlicher Zusammenhänge ausprägen, also die Signatur der gesellschaftlichen und politischen Umstände tragen, in der sie zur Geltung kommen. Ihre Entwicklung ist deshalb nicht beliebig, so gibt es natürlich erhebliche Unterschiede zwischen analogen und digitalen Kommunikationsmedien; aber aus diesen materiellen Unterschieden allein lassen sich die Entwicklungspfade und Nutzungsweisen des Internets nicht erklären.

Wie im Falle der Drucktechnik ist auch in Bezug auf das Internet nach der Gesellschaftsformation zu fragen, die aus dem Möglichkeitsraum, den die digitale Technik aufspannt, bestimmten technischen Formen den Weg ebnet. Die Durchsetzung des Internets und seiner Dienste, die uns heute so selbstverständlich erscheinen, war und ist jedenfalls bis heute kein Selbstläufer. David Clark (2016), einer der Architekten des Internets, hat dessen Geschichte als eine Abfolge von „forks in the

road“ beschrieben; Weggabelungen also, die andere Entwicklungspfade digitaler Netze möglich und zeitweilig sogar wahrscheinlich gemacht haben. Rückblickend betrachtet erweist sich die Durchsetzung des Internets als eine eher unwahrscheinliche Entwicklung. Bis in die 1990er Jahre konkurrierte es gegen eine alternative Netzarchitektur, die sich, weil sie von den nationalen Postbehörden über die Internationale Fernmeldeunion (ITU) initiiert worden war, auf die politische Unterstützung der staatlichen Administrationen stützen konnte. Dass sich das Internet, das zunächst kaum mehr als eine experimentelle Entwicklungsumgebung darstellte, gegen diese Konkurrenz durchsetzen konnte, kann nicht auf technische Überlegenheit zurückgeführt werden, sondern verdankt sich einer gesellschaftlichen Konstellation, die wirtschaftliche, politische und kulturelle Liberalisierungstendenzen vereinte.

Eine große Rolle spielte die in den OECD-Ländern vorangetriebene Privatisierung der Telekommunikation in den 1990er Jahren. Die Realisierung eines territorialen, zentral verwalteten Datennetzes mit eigens darauf ausgerichteten Kommunikationsdiensten konnte nun nicht länger hoheitlich verordnet werden, sondern sah sich mit einem Gegenentwurf konfrontiert, der auf nicht-proprietäre Standards sowie eine dezentral und grenzüberschreitend angelegte Netzarchitektur setzte. Innovationen wie das WorldWideWeb, das dem Internet schließlich international zum Durchbruch verhalf, wären in dem staatlich geplanten Datennetz technisch ausgeschlossen gewesen. Die weitere Entwicklung der digitalen Anwendungen und ihrer Nutzung reflektierte dann in zunehmendem Maße auch die kulturelle und politische Liberalisierung, die im Nachgang der 1960er Jahre zum Mainstream avancierte. Das Fehlen einer hierarchischen Kontrolle und effektiven Veto-Instanz hat zu einer Vielzahl innovativer Anwendungen geführt, die dem Anspruch auf Individualisierung, wirtschaftlicher und politischer Freiheit zumindest in der wesentlichen Welt einen willkommenen Resonanzboden bietet.

Einer Formulierung von Andreas Reckwitz (2008) folgend, könnte man sagen, dass sich das Internet zu einem „Übungsfeld für neue Subjektformen“ entwickelt hat. Im Umfeld der sozialen Netzwerke etwa experimentierten die jungen Generationen heute mit den kulturellen, wirtschaftlichen und politischen Freiheiten, die ihre Eltern und Großeltern in der zweiten Hälfte des 20. Jahrhunderts erkämpft haben und treiben auf diese Weise den digitalen Wandel weiter voran. Das Internet, so meine These, ist ein Kind der Spätmoderne. Seine Entwicklung reflektiert das Zusammentreffen kultureller, wirtschaftlicher und politischer Liberalisierungsprozesse, die sich gewissermaßen in die Technik einschreiben. Entsprechend sollte der Strukturwandel, den wir gegenwärtig beobachten, nicht als primär technikgetrieben verstanden werden, sondern als Ausdruck einer gesellschaftlichen Orientierung, die wirtschaftliche und kulturelle Freiheit prämiert und deren Beschränkung durch kollektive Normen unter erhöhten Rechtfertigungsdruck stellt.

THESE 3: DIE DIGITALISIERUNG BEWIRKT EINE STEIGERUNG VON KONTINGENZ, DIE DIE ENTSCHEIDBARKEIT UND FRAGILITÄT DEMOKRATISCHER INSTITUTIONEN SICHTBAR MACHT

Ein Effekt des digitalen Strukturwandels ist, dass er uns Merkmale der mediatisierten Demokratie vor Augen führt, die wir, solange sie intakt waren, als selbstverständlich wahrgenommen haben. Durch den Rückspiegel können wir Stabilitätsmechanismen der Demokratie identifizieren, die den politischen Apparat und die Massenmedien ermöglichend und zugleich begrenzend miteinander verbunden haben. Die Systemtheorie würde hier von festen Kopplungen sprechen, die den Massenmedien ihre spezielle Form verleihen.

Bis zur Jahrtausendwende hatten die Massenmedien in westlichen Demokratien eine nahezu unangefochtene Monopolstellung in der öffentlichen Sphäre inne. Sie entschieden über die Relevanz und Irrelevanz von Akteuren, Ideen und Programmen, und prägten damit die medial erfahrbare politische Wirklichkeit. Das Zusammenspiel von Politik und Medien wurde zusätzlich durch eine kapitalintensive Medientechnologie befestigt, die das Publizieren von Nachrichten und Weltdeutungen auf wenige Organisationen und Autorinnen und Autoren beschränkte. Medienbetriebe besaßen oder kontrollierten zumindest ihre Ausspielkanäle. Diese Kontrolle erleichterte die Durchsetzung journalistischer Normen und zementierte die strikte Trennung zwischen wenigen professionellen Produzenten und einem großen konsumierenden Publikum. Sie begrenzte auch, mit Bourdieu (1996) gesprochen, den öffentlichen Raum des Sag- und Denkbaren.

Man kann nun einwenden, dass die mächtige Rolle der Medien als Gatekeeper vielfach kritisiert worden ist, nicht zuletzt aufgrund der intellektuellen und gesellschaftlichen Nähe zwischen politischen und journalistischen Eliten. Und doch erschließt sich erst im Rückblick, wie stark die Kopplung von analogen Medientechnologien, Konventionen der Berichterstattung und Kontrolle der Kommunikationskanäle unser Verständnis von demokratischer Öffentlichkeit und politischer Partizipation geprägt hat. Dazu gehört vor allem auch die von der deliberativen Demokratietheorie entwickelte Vorstellung eines nationalen öffentlichen Raums als geteiltem politischen Bezugsrahmen, an dem alle Bürger zumindest als Rezipienten teilhaben (Habermas 1992).

Die Digitalisierung zerstört diese enge Verbindung zwischen Politik und Medien nicht, aber sie eröffnet neue Kommunikationsmöglichkeiten und schafft damit ein Übungsfeld für Akteure und Ausdrucksformen, die im öffentlichen Diskurs bislang nicht repräsentiert waren. Die sozialen Netzwerke haben die Menschen faktisch mit einem Lautsprecher ausgestattet und der Unterscheidung zwischen Informationsproduzenten und -empfängern ihre materielle Grundlage entzogen. Im Prinzip können nun alle Menschen öffentlich kommunizieren. Soziale Netzwerke

wie YouTube und Facebook haben ihr Geschäftsmodell ursprünglich speziell auf diese nutzergenerierten Inhalte ausgerichtet. Eine neue Generation von Sprecherinnen und Sprechern sowie Politikerinnen und Politikern hat die öffentliche Bühne betreten, die sich nicht länger an die alten Regeln der öffentlichen Rede gebunden fühlen. In der Folge hat sich der Raum des Sagbaren erheblich erweitert.

Die digitalen Publikationsplattformen haben dem Bürgerrecht auf Meinungsfreiheit gewissermaßen Flügel verliehen. Zu den ersten politischen Kräften, die das erkannten und für sich effektiv zu nutzen wussten, gehörte nicht zufällig die neue Rechte, die von den Massenmedien weitgehend marginalisiert worden war. Sie eignet sich das Internet als Propagandamaschine an und experimentiert mit politischen Interventionsformen, die Aufmerksamkeit, die neue knappe Ressource, binden. Gleichzeitig erodiert der alte informelle Konsens über die Grenzen dessen, was öffentlich gesagt und getan werden darf. Die neue Haltelinie rückt näher an das Strafrecht heran, das mit dem jüngst geschaffenen Netzwerkdurchsetzungsgesetz für diese Aufgabe gerüstet werden soll.

Unterdessen entwickeln sich die digitalen Plattformen zu den neuen Gatekeepern des öffentlichen Raums. In dem Maße, in dem sie sich als Infrastruktur für den politischen Diskurs etablieren, ändern sich auch die entsprechenden Selektionskriterien und -mechanismen. Journalistisch ermittelte politische Relevanz konkurriert nun mit allem was Klicks erzeugt und der algorithmischen Prüfung noch tolerabel erscheint. Als neue Intermediäre empfehlen sich die Plattformen für die Gesellschaft, für Parteien und Abgeordneten wie auch die politische Berichterstattung. Selbst aktive Wahlkampfunterstützung bieten Facebook, Google und Co. an – mit Werbeeinnahmen für Wahlkampfanzeigen als Gegenleistung. So umfassend und subtil ist die Durchdringung der sozialen Netzwerke mittlerweile, dass den alten Massenmedien derzeit wenig anderes übrigbleibt, als sich ihren Regeln und Aufmerksamkeitslogiken zu beugen.

Die Plattformisierung der Öffentlichkeit zeigt exemplarisch, dass sich die mediatisierte Demokratie im Umbruch befindet. Die eingespielten Beziehungen zwischen Massenmedien und politischem Betrieb verlieren ihre Selbstverständlichkeit; und das digitale Medium hat einen neuen Möglichkeitsraum geschaffen, dessen Tiefe wir zwar nicht vermessen, aber doch praktisch erproben können. Diese Entwicklung beschränkt sich keineswegs auf die öffentliche Sphäre, sondern berührt auch andere Dimensionen der repräsentativen Demokratie. Aus Sicht der digitalen Avantgarde US-amerikanischer Provenienz ist die repräsentative Demokratie längst obsolet. Demokratie, so stellt Jamie Bartlett (2018) nüchtern fest, ist eine „‚general purpose' technology […] that somehow stopped evolving". In dichter Folge lassen sich Experimente beobachten, die bestehende Strukturen und Verfahren der repräsentativen Demokratie zur Disposition stellen. Dazu gehören neue Beteiligungsmechanis-

men, Willensbildungs- und Transparenztechniken, die am Dogma der elektoralen Demokratie rütteln. NGOs wie „liquid democracy“ oder die Entwickler der App „Democracy“ („Wahl war gestern. Demokratie ist immer“) arbeiten darauf hin, die Arbeitsteilung zwischen Repräsentanten und Repräsentierten, zwischen politischen Entscheidern und betroffenen Bürgerinnen und Bürgern, aber auch das Zeitregime der Demokratie neu zu justieren. Auch politische Parteien experimentieren angesichts ihrer schwindenden Mitgliederbasis mit neuen Organisationsformen, die sie stärker in die Nähe von Bewegungen und Schwärmen rücken (Chadwick und Stromer-Galley 2016; Dormal 2018). Selbst wenn die Demonstration technischer Machbarkeit in einigen Fällen überzeugender sein mag, als die politische Sinnhaftigkeit, ist diesen Initiativen doch gemeinsam, dass sie das Verhältnis von neuen medialen Möglichkeiten und den Ausschlusseffekten, das heißt den unrealisiert gebliebenen Optionen tradierter politischer Institutionen problematisieren. Die Entscheidbarkeit und Gestaltbarkeit demokratischer Strukturen und Verfahren rückt darüber wieder ins Bewusstsein; und dies eben nicht allein als Folge des technischen Wandels, sondern all der Herausforderungen, die sich das demokratische System selbst geschaffen hat.

LITERATUR

Anderson, Benedict (1983). Imagined Communities: Reflections on the Origin and Spread of Nationalism. London: Verso.

Bartlett, Jamie (2018). The People Vs Tech. How the internet is killing democracy (and how we save it). London: Ebury Press.

Brecht, Berthold (1967/1992). Der Rundfunk als Kommunikationsapparat. In: Bertolt Brecht: Gesammelte Werke in 20 Bänden. Band 18. Frankfurt am Main: Suhrkamp, S. 127–134.

Bourdieu, Pierre (1996) The rules of art: Genesis and structure of the literary field. Stanford, CA: Stanford University Press.

Chadwick, Andrew, und Jennifer Stromer-Galley (2016). „Digital Media, Power, and Democracy in Parties and Election Campaigns: Party Decline or Party Renewal?“, The International Journal of Press/Politics 21(3), S. 283–93.

Clark, David D. (2016). „The Contingent Internet“, Daedalus 145(1), S. 9–17.

Dormal, Michel (2018). Der Formwandel der Demokratie und die rechtspopulistische Regression. In: Yves Bizeul, Ludmila Lutz-Auras und Jan Rohgalf (Hrsg): Offene oder geschlossene Kollektivität. Wiesbaden: Springer, S. 87–106.

Habermas, Jürgen (1992). Faktizität und Geltung. Frankfurt: am Main Suhrkamp.

Krämer, Sybille (1998). Form als Vollzug oder: Was gewinnen wir mit Niklas Luhmanns Unterscheidung von Medium und Form? Zuerst erschienen in: Rechtshistorisches Journal 17, S. 558–573.

Luhmann, Niklas (199). Die Gesellschaft der Gesellschaft. Frankfurt am Main: Suhrkamp.

McLuhan, Marshall (1964). Understanding Media. The Extensions of Man. New York: McGraw-Hill.

Reckwitz, Andreas (2008). Medientransformation und Subjekttransformation, in Unscharfe Grenzen. Perspektiven der Kultursoziologie. Bielefeld: transcript Verlag.

Anmerkungen zur Systemrelativität des Personenbezuges im Datenschutzrecht

JULIAN HÖLZEL

Auch mehr als 40 Jahre nach dem Aufkommen des sog. Personenbezugs als zentraler Kategorie des zunächst bundesdeutschen, inzwischen europäischen Datenschutzrechts sind die Fundamente dieses Begriffes kaum geklärt. Die Diskussion orientiert sich in guter Tradition an über die Dekaden aufgeschichteter Kasuistik, ohne dass bislang eine überzeugende theoretische Beschreibung dieses Rechtsbegriffes angefertigt werden konnte. Nach der hier vertretenen Auffassung liegt die Ursache dafür in dem Versuch einer objektivistischen Fassung des Begriffes, der ohne Reflexion auf den jeweiligen Interpretationshorizont der Rechtsanwenderinnen auskommen soll. Dies soll Anlass sein, einen konsequent anwendungsrelativen Begriff zu skizzieren.

DER KONTEXT DER UNTERSCHEIDUNG

Die Unterscheidung zwischen personenbezogenen und nicht-personenbezogenen Daten taucht aus Rechtsanwendungsperspektive in zwei unterschiedlichen Kontexten auf: zum einen als Kriterium der Verarbeiterin, die EDV-Prozesse auf deren datenschutzrechtliche Relevanz hin beobachtet, sowie als Kriterium der Datenschutz-Aufsichtsbehörden, deren Aufgabe es ist, die verarbeitenden Organisationen daraufhin zu beobachten, ob diese sich entsprechend den ihnen durch das Datenschutzrecht auferlegten Pflichten verhalten[1], um schließlich bei einer etwaigen Differenz zwischen den rechtlichen Anforderungen und tatsächlichem Verhalten durch geeignete Maßnahmen[2] auf eine Differenzverringerung hinzuarbeiten.

Im Hinblick auf unser Thema bedeutet das insbesondere, dass die Aufsichtsbehörden die Verarbeiterinnen bei der Anwendung der Unterscheidung zwischen personenbezogenen und nicht-personenbezogenen Daten auf ihre eigenen Verarbeitungsprozesse hin beobachten. Diese Feststellung ist trivial, aber von großer Tragweite, denn sie bedingt, dass die Interpretation der Merkmale des Tatbestandes der personenbezogenen Daten immer vor dem Hintergrund einer Verarbeiterin erfolgt:

[1] Eine entsprechende Beobachterinnen-Position nehmen die Mitbewerberinnen der Verarbeiterin und entsprechende Verbände ein, insoweit diese aktivlegitimiert nach den lauterkeitsrechtlichen Vorschriften sind. Im Detail ist noch Vieles umstritten, siehe z.B. Ohly, GRUR 2019, S. 686ff. Für unsere weiteren Betrachtung ist diese Frage ohne Belang und wird daher im Folgenden ausgeklammert.

[2] Dabei hat sich das Datenschutzrecht längst von einem klassischen Sanktionen- hin zu einem Aufsichtsrecht entwickelt, das eine Vielzahl von unterschiedlichen Maßnahmeformen kennt, siehe nur Artikel 57, 58 der DS-GVO.

Personenbezogene Daten sind nur personenbezogene Daten relativ zu einer Verarbeiterin[3]. Die Personenbezogenheit von Daten ist nicht – wie es der Sprachgebrauch in Form des „Personenbezuges" nahelegen mag – eine diesen intrinsische Eigenschaft, sondern sie bezeichnet eine bestimmte Beziehung, die eine Verarbeiterin aufgrund ihrer Interpretation des Datums zwischen diesem und einer Person herstellt[4]. Es handelt sich daher vielmehr um eine Eigenschaft, die die Beziehung zwischen Verarbeiterin und Datum kennzeichnet. Damit rückt bei der Beurteilung, ob eine Verarbeiterin personenbezogene Daten verarbeitet, die Frage nach den Kriterien in den Mittelpunkt, nach welchen eine solche Relation zwischen dieser und einem Datum gerechtfertigter Weise angenommen werden kann. Ausgeschlossen ist damit auch, diese Annahme für bestimmte Darstellungsformate von Daten pauschal ohne Rücksicht auf die Verarbeiterin zu treffen. Eine IP-Adresse ist nicht schlechterdings personenbezogen, genausowenig wie für sog. „synthetische Daten" oder „aggregierte Daten" ein Personenbezug ohne Weiteres abzulehnen ist.

Die kanonische Analyse der Artikel-29-Gruppe[5], die vielfach zur Auslegung herangezogen wird, zerlegt den Begriff in vier Elemente, mit denen sich der Interpretationsvorschlag an dem Wortlaut der inzwischen außer Kraft getretenen Datenschutz-Richtlinie orientiert. Gleichwohl weist die Gruppe darauf hin, dass sich die „Begriffsbausteine" wechselseitig beeinflussten, die Trennung daher im Wesentlichen ihrem analytischen Ansatz geschuldet sei. Ohne dies methodisch zu reflektieren oder auch nur explizit zu machen, geht diese Analyse von einer Art objektivistischem Beurteilungshorizont aus, bei der der Verwendungskontext fast vollständig[6] außer Betracht bleibt. In Anlehnung an die Trennung dieser vier Elemente[7] wollen wir vor dem Hintergrund unseres vorangestellten Interpretationshorizontes der Verarbeitungsrelativität des Personenbezugs begriffliche Umdispositionen vor-

[3] Damit ist zugleich angezeigt, dass wir die seit gut 40 Jahren in der datenschutzrechtlichen Diskussion verankerte Unterscheidung zwischen dem sog. „relativen" und „absoluten" Personenbezug nicht mitvollziehen. Denn selbst der Begriff des sog. „absoluten Personenbezugs" imaginiert auch nur Mittel und Fähigkeiten irgendeiner Akteurin, um von dort aus den Personenbezug zu bestimmen, aber eben doch auch nur relativ zu eben diesem. Der Unterschied besteht lediglich in dem, was einer konkreten Verarbeiterin, deren Eigenschaft als Verantwortliche in Rede steht, als Mittel und Fähigkeiten noch eben zugerechnet wird.

[4] Oder, unterstellt bestimmt Fähigkeiten und Mittel, durch die Verarbeiterin herstellbar, im überkommenen Datenschutzrechtsdiskurs „Personenbeziehbarkeit" genannt. Dies ist aber nicht viel mehr als eine Modalisierung der Personenbezogenheit.

[5] Artikel-29-Datenschutzgruppe, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten" (im Folgenden WP136).

[6] Diese Perspektive scheint nur sehr kurz bei Ausdefinition des dritten Elementes „über" auf, wenn dieses trotz Fehlens eines (objektivistischen) Inhaltselementes mit Rücksicht auf den Verarbeitungszweck oder gar nur aufgrund der Beeinflussung des Verarbeitungsergebnisses festgestellt werden soll. Die sich sofort anschließende Frage wäre natürlich, in welches Verhältnis die überkommene Dogmatik Verarbeitungszweck und sachlichen Anwendungsbereich stellt.

[7] Die Artikel-29-Datenschutzgruppe benennt als diese: „alle Informationen", „über", „identifizierte/identifizierbare", „natürliche Person".

schlagen. Das betrifft insbesondere die Voraussetzungen, die für eine Verarbeiterin vorliegen müssen, um eine entsprechende Beurteilung der einzelnen Elemente für die Relation zwischen dieser und Datum zu plausibilisieren.

„ALLE INFORMATIONEN"

Zu Beginn einer näheren Begriffsbestimmung dieses Elementes wird häufig darauf hingewiesen, es sei nicht etwa der „mathematische" Informationsbegriff zugrundezulegen, sondern vielmehr ein „geisteswisseschaftlicher", der nämlich auch die „Bedeutung" der „Information" abzubilden im Stande sei[8]. Informationen im Sinne des Datenschutzrechtes seien daher alle sinnhaften Aussagen über natürliche Personen[9]. Damit wird freilich übersehen, dass auch die Sinnhaftigkeit von Nachrichten ihrerseits nur vor dem Hintergrund aller möglichen Sinnangebote, mithin vor einem Selektionshorizont festgestellt werden kann. Dies aber ist auch der Kern der mathematischen Informationstheorie, der es um die genaue Reproduktion einer Nachricht geht, für die die Annahme gilt, dass bereits diese aus einem Repertoire möglicher Nachrichten ausgewählt wurde. Die Reproduktion der Nachricht erfolgt dann vor dieser a priori gegebenen Menge möglicher Nachrichten an anderer Stelle. Der entscheidende Umstand ist der der Wahrscheinlichkeit, welche die Erwartungsunsicherheit der Empfängerin vor Empfang der Nachricht konstituiert. Information ist dann ein Maß, welches anzeigt, dass und „wieviel"[10] dieser Unsicherheit beseitigt wurde.

Für die Zwecke dieses Beitrages muss von der traditionellen Bestimmung nicht vollständig abgerückt werden. Der Vergleich mit den Grundannahmen der „mathematischen" Informationstheorie macht aber deutlich, dass die Rede von Informationen darauf angewiesen ist, entsprechend offene Erwartungsstrukturen und damit Möglichkeitshorizonte anzugeben, deren Reduktion dann als Information bezeichnet werden kann. In dieser Hinsicht zwingt uns das Element „alle Informationen" be-

[8] Der Nachweis der Ungeeignetheit erfolgt regelmäßig über ein Zitat aus der Einleitung des Artikels von Shannon, in der dieser das ingenieurwissenschaftliche Problem technisch vermittelter Kommunikation behandelt. Dort heißt es auf S. 379: „Frequently the messages have meaning; that is they refer to or are correlated according to some system with certain physical or conceptual entities. These semantic aspects of communication are irrelevant to the engineering problem." (Shannon, A Mathematical Theory of Communication, The Bell System Technical Journal, July 1948, S. 379ff.).

[9] WP136, S. 7.

[10] Dieser Umstand ist aus technischer Sicht entscheidend, denn davon abhängig sind dann die Eigenschaften der zu konstruierenden Kommunikationskanäle. Eine genaue Messung der Beseitigung von Unsicherheit erfordert dann freilich auch eine genaue Quantifizierung der Unsicherheit, mithin eine genaue Angabe der erwartbaren Nachrichten. Zu einer Reflexion der Bedingungen einer solchen Möglichkeit in diesem Band Pohle, On Measuring Fundamental Rights Protection – Can and Should Data Protection Law Learn From Environmental Law?.

reits auf dieser Ebene, „personenbezogene Daten“ als systemrelativ[11] zu begreifen[12], denn andernfalls wären wir außerstande, eine entsprechende Erwartungsstruktur anzugeben. Offen bleibt allerdings ein die Menge der möglichen Systemrelationen limitierenden Merkmales. Diese Funktion liegt in einem anderen Definitionselement.

„IDENTIFIZIERTHEIT/IDENTIFIZIERBARKEIT“

Durch dieses Merkmal legt das Datenschutzrecht fest, welches Wissen und welche Fähigkeiten einer Verarbeiterin zurechenbar hinsichtlich der Frage ist, ob für diese eine konkrete Möglichkeit der Identifikation des in Rede stehenden Datums mit der Verarbeiterin bereits bekannten Angaben besteht, die diese auf eine realweltliche Entität[13] bezieht. Die Formulierung in Erwägungsgrund 26 der Verordnung macht dabei klar, dass es nicht nur auf aktuelles Wissen und Fähigkeiten der Verarbeiterin ankommt, sondern auch auf solches, das in der Person anderer Verarbeiterinnen vorliegt, für welche aber für die in Rede stehende Verarbeiterin eine angebbare Zugriffschance besteht. Zwar spricht der Wortlaut von Erwägungsgrund 26 von beliebigen „anderen Person[en]“, die dabei zu berücksichtigen sind, ohne diesen Kreis ausdrücklich einzuschränken. Aus rechtsstaatlicher Sicht dürfte dabei nur auf solche Personen abzustellen sein, zwischen denen und der Verarbeiterin eine reale Kommunikationschance besteht. Andernfalls wäre für die Verarbeiterin in ihrer Selbstbeobachtung nicht feststellbar, ob sie unter den Anwendungsbereich des Datenschutzrechtes fallen – ultra posse nemo obligatur.

Die juristische Diskussion der letzten Dekaden zum Problem des Personenbezuges war ganz maßgeblich von der praktischen Unsicherheit hinsichtlich der jeweils im konkreten Fall unterstellbaren Fähigkeiten und Mittel der Verarbeiterinnen begleitet, aus welchen diesen wenigstens die Möglichkeit der Identifikation der von in den Daten liegenden sinnhaften Aussagen betroffenen Personen zugesprochen werden konnte. Die Debatte unterschlägt dabei noch immer, dass jede Identifikation eine für diese Operation konstituierte Identität voraussetzt[14], und kann daher keine abstrakten Kriterien vorweisen, nach denen sie diese für die Identifikation erfor-

[11] Ohne freilich bereits eine spezifische Systemreferenz angeben zu müssen. Darin liegt dann die Funktion eines anderen Defintionselementes.

[12] So bereits Steinmüller, Stellenwert der EDV in der öffentlichen Verwaltung und Prinzipien des Datenschutzrechts, ÖVD 1972, S. 460; sowie Steinmüller/Ermer/Schimmel, Datenschutz bei riskanten Systemen, Berlin-Heidelberg 1978, S. 84.

[13] Konzeptuell kommen damit beliebige Einheiten in Betracht, die von der Verarbeiterin als solche zugrunde gelegt werden. Datenschutzrechtlich relevant sind freilich nur natürliche Personen, wie sich aus einem weiteren Merkmal ergibt. Zum Hintergrund dieser Annahmen aus dem Bereich der Datenmodellierung siehe Hölzel, European Data Protection Law Review 2019, S. 189; ders., DuD 2018, S. 504.

[14] Dazu aus sprachanalytischer Perspektive Tugendhat, Traditional and Analytical Philosophy, Cambridge 1982, S. 310ff., mit der Unterscheidung zwischen ursprünglicher Spezifikation und davon abhängiger Identifikation, sowie Kripke, Naming and Necessity, Cambridge 1980, S. 107, der die Herstellung der ursprünglichen Identität als „Taufe“ bezeichnet. Beide weisen darauf hin, dass es sich um eine unhintergehbare Voraussetzung handelt.

derliche Identität als hinreichend konstituiert ansieht. Eindrücklich sichtbar wird das insbesondere im parallel geführten technischen Anonymisierungsdiskurs, der durchgehend unter der Prämisse einer im Zusatzwissen der Verarbeiterin bereits hinreichend etablierten Identität geführt wird[15] und damit die Operation der Identifikation als Vorgang der „record linkage" über einen Ähnlichkeitsvergleich der Attributwerte eines angegriffenen Datensatzes bestimmen kann. Die Herstellung dieser ursprünglichen Identität wird damit als notwendige Voraussetzung begriffen, die im Wesentlichen im pragmatischen Belieben des Datenbankherstellers liegt[16]. Auch an dieser Stelle zeigt sich die notwendige Systemrelativität des Personenbezuges, denn jede Identifikation setzt eine ursprüngliche Identitätsherstellung voraus, die technisch durch eine bestimmte Kombination von Attributwerten innerhalb eines Attributschemas verwirklicht wird. Der Wortlaut des Datenschutzrechts in Artikel 4 Nr. 1 der Verordnung sieht an dieser Stelle nur eine beispielhafte Aufzählung von „insbesondere" in Betracht kommenden „Kennungen" vor, wie etwa Namen oder Kennnummern. Damit wird deutlich, dass das Datenschutzrecht von einem funktionalen Identitätsbegriff ausgeht, es also keineswegs auf Kategorien wie die des bürgerlichen Namens ankommt, sondern nur auf die Schaffung der Voraussetzung einer Beobachtungsverknüpfung in Form von sinnhaften Aussagen über eine designierte Entität.

Ein Beispiel dafür wäre etwa das sogenannte datr-Cookie, welches bei einem Besuch der Facebook-Webseite auf dem Rechner gespeichert wird, von dem der Zugriff mittels des Browsers stattfindet. Es handelt sich um eine Textdatei, die wenige Einträge wie etwa das Erzeugungs- und Ablaufdatum, eine eindeutige Buchstabenkette und Datum und Zeit des letzten Zugriffs enthält. Das Cookie besitzt einen Gültigkeitszeitraum von zwei Jahren und kann von Facebook etwa auch dann abgerufen werden, wenn sogenannte „Social Plugins" auf Drittseiten eingebunden und diese abgerufen werden. Es ist Facebook damit relativ einfach möglich, eine Surfhistorie anzufertigen[17]. Auf dieser Grundlage kann dann etwa spezifische Werbung über das Facebook-Werbenetzwerk ausgespielt werden. Diese Spezifizierung der ausgespielten Inhalte erfolgt anhand der von Facebook generierten Erwartungshorizonte hinsichtlich zukünftigen Surfhaltens; die Informativität der über das Cookie verknüpften Beobachtungen, die als strukturierte Daten vorliegen, besteht dann darin, diese Erwartungswerte in die eine oder andere Richtung zu beeinflussen.

[15] Nur selten so explizit wie bei Willenborg/Waal, Elements of Statistical Disclosure Control, New York 2001, S. 41: „A requirement of a target unit is that it be identfiable, that is that it has an associated identity.".

[16] Dazu und näher zu den technischen Hintergründen insgesamt Hölzel, DuD 2018, S. 502ff.

[17] So korrekt das OLG Düsseldorf im Vorlagebeschluss vom 19.01.2017, I-20 U 40/16. Der EuGH hat in der darauffolgenden Entscheidung vom 29.07.2019, C-40/17 – Fashion iD diese Prämisse übernommen, ohne diese selbst zu überprüfen.

„ÜBER“

Der traditionelle Ansatz qualifiziert über dieses Element den Aussagegehalt des Datums im Hinblick auf die zumindest identifizierbare Person. Innerhalb dieses Ansatzes werden drei mögliche Dimensionen unterschieden, nach denen dieser besondere Aussagegehalt beurteilt werden kann: nach Inhalt, nach Zweck und nach dem Ergebnis. Das Inhaltselement sei dann anzunehmen, wenn „Informationen über eine bestimmte Person gegeben werden“[18], das Zweckelement dann, wenn das Datum mit dem Zweck verwendet werden wird, eine Person einer aufgrunddessen differenzierten Behandlung zu unterziehen und das Ergebniselement schließlich dann, wenn sich die Verwendung des Datums auf Rechte und Interessen der Person auswirken könnte.

Das Verhältnis dieser durch den Wortlaut der Verordnung nicht induzierten Differenzierung in drei Unterelemente bleibte dabei über die Feststellung, es handele sich um alternative, nicht um kumulative Kriterien, unklar. So bleibt etwa offen, wie z.B. im Rahmen des Zweckelementes einer Person eine bestimmte Behandlung angediehen werden kann, ohne zugleich an einer ihr zugesprochenen Eigenschaft anzuknüpfen, die in Form einer Aussage über diese Person dargestellt werden kann. Die Einführung eines Inhaltselementes in der Bestimmung der Artikel-29-Gruppe ist auch logisch zirkulär insofern, als dieses immer dann bejaht werden soll, wenn „Informationen über eine bestimmte Person gegeben werden“. Genau diese Frage ist aber noch zu beantworten, sodass es sich bei diesem Element im Wesentlichen um eine tautologische Wiedergabe der Ausgangsfrage handelt. Deutlich wird dabei der objektivistische Interpretationshorizont, der der Analyse der Artikel-29-Gruppe zugrunde liegt, nach der versucht wird, das Kriterium des Personenbezuges ohne Rekurs auf ein kognitives System zu bestimmen. Erreicht wird damit freilich nur eine Verdunkelung der dann zugrundegelegten Interpretationskriterien, in der die Bestimmung dann gleichsam in der „Natur des Datums“ liegt[19].

Mit dem Zweck- und dem Ergebniselement ist hingegen einem systemrelativen Ansatz bereits der Weg geebnet, indem die Interpretation auf dem Datum selbst externe Bedingungen zurückgreift. Beide Elemente können dann auf die jeweiligen Entscheidungsprogramme der Verarbeiterinnen, in denen an Personenmodellen angeknüpft wird, zurückgeführt werden, indem das Zweckelement den Horizont der intendierten Folgen, das Ergebniselement den Horizont der nichtintendierten Nebenfolgen als Interpretationskriterien absteckt. Präzisierend sei für das Ergebnise-

[18] WP136, S. 11.

[19] Dabei dürften insbesondere aus Perspektive der Rechtsanwendung unabweisbare praktische Bedürfnisse eine Rolle spielen, um die in der Praxis kaum einmal erfüllbaren Anforderungen einer systemrelativen Beurteilung auf ein handhabbares Maß zu reduzieren. Die dann aber eigentlich sofort offenkundige Frage nach der prinzipiellen Geeignetheit eines so gestalteten Regulierungsmodells wird aber kaum einmal gestellt.

lement lediglich angefügt, dass es sich um für die Verarbeiterin reflektierbare Nebenfolgen handeln muss, sodass es sich bei der ex-post-Feststellung, ein bestimmtes Datum habe als Ursache einer differenzierten Behandlung gewirkt, für sich genommen nicht ausreicht, solange dieser Umstand für die Verarbeiterin nicht erkennbar war[20]. Festzuhalten ist, dass das Element „über" den Kreis der von der Verarbeitung in datenschutzrechtlich relevanter Weise Betroffenen konkretisiert. Daten beziehen sich damit dann auf identifizierbare Personen, wenn diese nach den Entscheidungsprogrammen der Verarbeiterinnen die Ursache[21] einer differenzierten Behandlung dieser Person darstellen.

FAZIT

Die vorstehenden Ausführungen sollten verdeutlichen, dass im Rahmen eines systemrelativen Ansatzes der Auslegung des Personenbezuges die kognitiv-normativen Strukturen – Erwartungen an Personen sowie Entscheidungsprogramme – der Verarbeiterinnen in den Mittelpunkt rücken. Es handelt sich um einen im Sinne der Schutzgüter des Datenschutzrechts[22] – die Grundrechte und Grundfreiheiten natürlicher Personen als Betroffene automatisierter Datenverarbeitungen – längst überfälligen Schritt[23], denn die Interpretationslinie der letzten 40 Jahre konnte die Unsicherheiten der praktischen Anwendung nicht überwinden. Aus rechtspolitischer Perspektive wäre schließlich die Konsequenz zu ziehen, das sachliche Anwendungskriterium „personenbezogene Daten" durch ein entsprechend explizit entscheidungsorientiertes Konzept zu ersetzen[24].

[20] Als Instrument für die Etablierung eines konkreten Erkennbarkeitsmaßstabes dürfte sich z.B. die Datenschutz-Folgeabschätzung in Artikel 35 der DS-GVO eignen.

[21] Das betrifft, wie eben ausgeführt zukünftige Ursachen, die anhand der Reflexion von intendierten Folgen und Nebenfolgen der Entscheidungsprogramme bezeichnet werden können, sowie vergangene Ursachen nur dann, wenn deren Ursächlichkeit für die Verarbeiterin bei Anwendung geeigneter Reflexionsmittel erkennbar waren.

[22] Des aktuell geltenden Datenschutzrechts, wohlgemerkt, und nicht der innerhalb der Datenschutzrechtstheorie beschreibbaren Schutzgüter.

[23] So auch Jörg Pohle, Personal Data Not Found, DANA – Datenschutz Nachrichten 1/2016, S. 14ff.; ders., Datenschutz und Technikgestaltung, Berlin 2018, insbes. S. 251ff.; Moritz Karg, Die Rechtsfigur des personenbezogenen Datums – Ein Anachronismus des Datenschutzes?, ZD 2012, S. 255ff.

[24] So ebenfalls die Forderungen von Pohle, ibid., der an personenbezogenen Entscheidungen anknüpfen will, und Karg, ibid., der von personenbezogenen Verfahren spricht.

Taking Ingolf Pernice Seriously[1]

MATTHIAS C. KETTEMANN

I have known Ingolf Pernice through his writings long before I met him, unforgivably late in my career, but still in time to influence my thinking, in Frankfurt in 2014. On the occasion of the 100th anniversary of its foundation, the University of Frankfurt was inviting key scholars during the year to look back, to assess the present, to give perspectives for the future. Nobody who ever met Ingolf would doubt that he leaned firmly towards the last. In light of the eminent role of Frankfurt for the development of public law beyond the state, the Faculty of Law and the Cluster of Excellence "The Formation of Normative Orders", where I was working on my *Habilitation*, had convened, in June 2014, a workshop analyzing the past, present and future of international and European law.

The three speakers selected who spoke about the future challenges of the international legal order were Martti Koskenniemi, preeminent *renaissance* publicist and theorist of international law (who spoke on the potential of international law to realize our goals, our utopias), Joseph H.H. Weiler, one of the most influential experts on European law, especially from outside of Europe (who looked at Europe's future through Europe's values) and, of course, Ingolf Pernice himself, who presented his approach to allow for the participation of all persons actually affected by global decision-making in the decision-making processes themselves at the example of Internet Governance. Where Koskenniemi extolled us to take international law seriously and Joseph H.H. Weiler showed that we needed to take Europe and its values seriously, Ingolf focused on the legal *monad:* the individual, and in a Dworkinian formulation demanded we take "people seriously".[2]

TAKING PEOPLE SERIOUSLY IN CONSTITUTIONALIZING THE INTERNET

Ingolf Pernice is a ground-breaking scholar, well versed in taking concepts and flipping them on their head, to much intellectual and practical gain. Taking *people* seriously in an age of powerful companies; a *constitution* for the most ungoverned socio-political arena; the internet. He has helped us tremendously in understanding the

[1] With a friendly nod to Ingolf Pernice, Global Constitutionalism and the Internet: Taking People Seriously, in Rainer Hofmann and Stefan Kadelbach (eds.), Law Beyond the State (Frankfurt am Main: Campus, 2016), 151-206 (also pusblished as Ingolf Pernice, Global Constitutionalism and the Internet. Taking People Seriously. HIIG Discussion Paper Series (2015/01), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2576697.

[2] Ibid.

normative dynamics of the internet. Where John Perry Barlow declared the independence of cyberspace,[3] Ingolf de facto declared independent thinking on cyberspace his (or rather one of his) chosen domain(s). He did so in an exemplary fashion in his Frankfurt presentation, which gave insight into his and his team's work at the HIIG and Humboldt University, Berlin. In his paper he showed how different approaches to, and concepts of, global constitutionalism can be useful to develop a "constitutional frame of governance" for the internet and, importantly, through the internet: "It is the Internet that seems to allow the information and transparency, communication and discourse, participation of and control by (global) citizens necessary for organizing legitimacy."[4] While his study is a must-read for any scholar interested in the dynamics of online rule-making, I found his seven elements or stages of a norm-setting process for the emergence of "globally binding rules" most interesting. This is indeed a key question to which few have found any remotely satisfactory answer: How can we develop – in light of the overlapping spheres of authority, the new normative vocabularies and the ever richer field of normative actors – binding rules that are legitimate – and legitimated. Ingolf saw seven steps to lead to norms that are "validated and revisited in a manner giving people a voice and so taking people seriously":[5] a common knowledge basis, a public sphere, an institutional framework, a multistakeholder-based method, validation, a fair dispute settlement apparatus and the openness of norms (through processes of monitoring and revisiting).[6]

By now I have moved academically and physically to Hamburg, where global constitutionalism – a topic of Ingolf Pernice's that predates his engagement with the internet – has very strong roots. But it is his writing that sums up best why constitutionalist approaches to the internet can be useful. Global constitutionalism and the Internet, for Ingolf, are related and mutually reinforcing:

> "the Internet is an important tool for developing a system of democratically legitimate regulation at the global level, giving people a voice, and so favours global constitutionalism, both for the space of communication and participation in politics it offers, and for the models of multi-stakeholder processes it has developed."

But constitutionalism also 'gives':

> "As the Internet is becoming the most important infrastructure for worldwide communication, constitutionalising its governance is required in order to ensure its security and resilience as well as the pro-

[3] John Perry Barlow, A Declaration of the Independence of Cyberspace, EFF (8 February 1996), https://www.eff.org/cyberspace-independence.

[4] Pernice (2015).

[5] Ibid.

[6] Ibid., 33-45.

> tection of the individual rights of all people involved, including the freedoms of information and expression, of sciences and education, intellectual property rights and the protection of data and privacy as elementary aspects of human dignity."[7]

For Ingolf Pernice, thus, global constitutionalism can be harnessed to ensure that the rights of people are realized in Internet rule-making. Over the last years, I have pursued a similar project in which I developed a theory of order of the internet: the normative order of the internet. I see it as being one way to formalize the frame in which Ingolf's global constitutionalist approaches can influence internet-related norm-development.

THE NORMATIVE ORDER OF THE INTERNET[8]

When speaking of the concept of 'normative order', I refer to the approach by Forst and Günther, who see norms less in terms of legality grounded in *formality* and more in terms of *functionality*. Norms, to them, are "practical reasons to act [containing] the claim of being binding upon the addressee."[9] These claims are narrativized and contextualized, habituated in practices, contained in customs (implicit, instituted normativity) and conventions *as social contracts* (implicit again) or conventions *as treaties* (explicit constituted normativity). The claims of being binding are thus *not legal* in that they are premised upon a legal procedure to ensure compliance, but nevertheless exercise, through their claim to be binding, a certain compliance pull.

But norms in the context of my study are *legal* in the sense that they shape and frame the *legal* space (*Rechts*raum), contribute to ensuring *legal* peace (*Rechts*frieden), provide for a *law* of collision (Kollisions*recht*) between applicable regimes and are treated by and large *as legal* norms or at least *legality* heuristics which ease decisionary burdens.

Taken together, the norms constituting the normative order of the internet (those *normatively* relevant for the internet and digitality in a *materially* relevant way) form a multi-layered legal order. This does not mean that they are centrally *ordered* or *hierarchically* layered. A normative order is a "complex of norms and values with which the fundamental structure of a society (or the structure of international, supranational or transnational relationships) is legitimated, in particular the exercise of

[7] Pernice (2015), 48.

[8] Cf. Matthias C. Kettemann, Deontology of the Digital: The Normative Order of the Internet, in Matthias C. Kettemann (ed.), Normative Ordnungen. Neue Perspektiven / Normative Orders. New Perspectives (Frankfurt/Main: Campus, 2020).

[9] Rainer Forst and Klaus Günther, Die Herausbildung normativer Ordnungen. Zur Idee eines interdisziplinären Forschungsprogramms, in Rainer Forst and Klaus Günther (eds.), Die Herausbildung normativer Ordnungen. Interdisziplinäre Perspektiven (Frankfurt/New York: Campus, 2011), 11-30 (16).

political authority and the distribution of basic goods."[10] These are key *legal* functions. At the same time, the normative order of the internet is more than a purely legal order as it relies on norms and processes that cannot easily be conceptualized in the language, logic and legitimacy structures of traditional legal systems.

The order extends to regulating and legitimating (or providing the normative tools for contestation of) the exercise of private or public authority and the distribution of basic goods in relation to the use and development of the internet by multiple actors, including internet access and access to internet content. It enshrines a *rule of norms*, the set of norms and normative expectations that shape the use and development of the internet, which lead to a *rule of law*.

The measure of *legality* of the normative order cannot be the "political constitution" (of states), against which it would fall short (but so does the international *legal* order). Rather the normative yardstick must be the normative order of the internet's *Eigenverfassung*,[11] as instituted by practices, and auto- and hetero-constituted. Norms from the third category (transnational regulatory arrangements, internet standards ...) may not be *legal norms* in traditional national or international legal approaches (they are the *tertium*), but they can be considered to have some or most of the qualities of legal norms (*Rechtsnormqualität*) if they meet internal, regime-specific transnationalized and objective human rights-based checks and balances as to their production, content and application.[12]

The normative order of the internet encompasses norm-generative processes and includes, through its processes, normatively relevant action by all actors. These actors develop normative expectations which are debated, contested and realized on the basis of shared principles within the order.

The concept of the normative order of the internet is thus an empirical-conceptual and a normative construct: it provides legitimacy (and justification) narratives and functions as an elastic normative space, with principles and processes for solving public policy conflicts connected to safeguarding the internet's integrity and protecting states and societies, natural and legal persons, from dangers related to internet use and misuse. The order integrates norms materially and normatively connected to the use and development of the internet at three different levels (regional, national, in-

[10] Forst and Günther (2011), 15: "Unter 'normativer Ordnung' verstehen wir den Komplex von Normen und Werten, mit denen die Grundstruktur einer Gesellschaft (beziehungsweise die Struktur inter- bzw. supra- oder transnationaler Verhältnisse) legitimiert wird, namentlich die Ausübung politischer Autorität und die Verteilung von elementaren Lebens- und Grundgütern" (translation by the author).

[11] Gunther Teubner, Globale Zivilverfassungen: Alternativen zur staatszentrierten Verfassungstheorie, 63 ZaöRV (2003), 1-28 (22).

[12] Thomas Vesting: Die Medien des Rechts: Computernetzwerke (Weilerswist: Velbrück Wissenschaft, 2015), 144.

ternational), of two types (privately and publicly authored), and of different character (from ius cogens to technical standards). As a legal order it operates through the form of law and analogously to it. Its actors – states, legal persons, natural persons – fulfil diverse functions as norm entrepreneurs, norm appliers, and norm enforcers. The order's justification narratives control new norms by assessing their technical consistency and their legal-cultural consonance vis-à-vis the order's purposes. Though not without autonomous elements, the normative order of the internet is interlinked through legitimation relationships with national and international legal orders.

The order is made up of international law, national law, and transnational regulatory arrangements of variable normativity. Apart from international and national norms, a 'third' category of norms exists, a normative tertium, which has only recently emerged as a normative category in its own right. Tertium norms are fundamentally technical standards and soft law norms that emerge in the contested space between technical necessity and socio-legal values. They evidence a variable normativity and transcend binary normative solutions and can thus counteract diffusions of regulatory responsibility in transnational settings.

The order's normativity shapes technicity. The technology-orientation of non-legal normativity, including its focus on code and standards, needs to be reoriented through a value-based normative approach, while the effective internal norm (re) production mechanisms of private standards need to be embraced. It is thus not technicity that shapes normativity. Rather than letting a technical medium define our societal values, it is the values embedded in the normative order of the internet that define the evolution of the internet's underlying technologies through normative framing and regulatory interventions. Value-based normativity must influence standard-setting to ensure the primacy of international legal commitments, and their national legal counterparts, in determining the finality of the normative order of the internet. Rather than accepting arguments out of technical necessity, we demonstrate that technical norms are properly placed within the value-oriented common frame of the normative order of the internet.

The internet's forces of normative disorder can be identified and countered. Centrifugal forces contribute to the emergence of normative redundancies ("normative froth"), real conflicts of norms between regulatory layers and geographically bounded normative spheres ("normative friction"), substantial structural problems ("normative fractures"), and political, commercial and technological fragmentation of the internet. However, technical invariants of the internet exercise defragmentation forces. These are then normatively reified within the normative order of the internet.

The internet has taken a normative turn. A study I have completed last year has shown that a normative turn has taken place on the internet, allowing norms im-

pacting its use and development to self-constitutionalize and – through autonomous normative processes – to develop and legitimize other norms within the order.[13] This approach has considerable explanatory and predictive potential regarding the evolution of norms and how this process will impact the internet. For instance, the study demonstrates that attempts at norm entrepreneurship that are in dissonance with key principles of the normative order, or that do not cohere with other order norms, will fail.

The normative order of the internet is a legal and legitimate order which is connected to, and legitimated by, international and national legal processes. It is further a legitimate order of norms. Processes of legitimation of norms take place within the order, but also through national law and the international legal system. Each field of norms within the order – international law, national law, transnational normative arrangements – is legitimized either through traditional normative processes or by its integration into national legal orders. Each actor group is legitimized directly or indirectly and transfers this legitimacy potential to the normative outcome, which is often – additionally – epistemically legitimate. The normative order itself is legitimate as a necessary order to ensure protection of and from the internet. The process of justifying the order is narrativized. As any order participant has a right to justification against norms and practices generally-reciprocally, the normative order of the internet is an order of justification.

CECI N'EST PAS LE FIN

My approach of a normative order of the internet sits comfortably with the ideas developed by Ingolf. As becomes a *theory* of a normative order of the internet, my analysis remains structural-abstract where his is solution-oriented. But, arguably, the seven steps/elements he has proposed to constitutionalize the internet fit well as norm production and legitimation elements of a coherent normative order of the internet. I have described the normative order of the internet as producing a liquefied normativity which learns from itself. Such a normativity learning from its environment can no longer be modeled in traditional concepts of subjectivity. We might have to re-think the Kantian theory of normativity (of "the law"), which sees self-organization as the principle of life that enables the transcendental constitution of normativity. How does this now relate to global constitutionalization? Can a similar approach be useful to conceptualize a "Constitution for the Internet", a normative order that learns from itself?

If someone can answer these questions, it is Ingolf Pernice. A grand book of his on the constitution(alization) of the internet would be needed now more than

[13] Matthias C. Kettemann, The Normative Order of the Internet (Oxford: Oxford University Press, 2020).

ever. Apart from the book itself I would particularly look forward to the title, as Ingolf has a very subtle hand with sophisticated references. Just think of the 2008 *Ceci n'est pas une Constitution*[14], which invokes René Magritte so aptly (given the subject) that I wouldn't be able to classify the constitutionalist discourse (now and then) much differently than with a nod to the Belgian surrealist. We are accustomed to the subject (harnessing power, legitimating authority), but somehow everything is different (intermediaries?), something is not right, not common place (governance by contract, by algorithm, by affordances?). The German word *Störgefühl* fits well here. Traditional constitutional lawyers have many *Störgefühle*, when seeking to extend their reach online with Karlsruhe in the backpack. Ingolf, however, is happily untraditional and, in a certain way, a surrealist or at least a magical realist of constitutionalism. Which is good, as anyone who writes about constitutionalizing the internet so profoundly and influentially as Ingolf has (and will continue to do so) really needs both ingredients: reality (what does the law say) and magic (what surprising but not impossible development needs to happen to come to a happy ending, a normative outcome that leaves the audience, the stakeholders, satisfied).

Ending where I started, with Ingolf: In the written version of his contribution on *Taking People Seriously*, Ingolf argued:

> "The Internet presents, in particular, new tools for discourses across borders, without limits also to the number of participants. The model of the IGF [...] seems to be particularly appropriate for not only organising the public space regarding global Internet governance, but also as a catalyser and focal point for people around the world interested to participate in the debate on equal terms and so to be respected and taken seriously."[15]

Let us take this suggestion seriously, especially in a year like 2019, when Germany has hosted the Internet Governance Forum in Berlin which might well prove a kick-start for a new generation of value-based internet governance research and practice.[16]

[14] Ingolf Pernice and Evgeni Tanchev (eds.), Ceci n'est pas une Constitution – Constitutionalisation without a Constitution? (Frankfurt am Main: Nomos, 2008).

[15] Pernice (2015), 37.

[16] See the ideas contained in Wolfgang Kleinwächter, Matthias C. Kettemann, Max Senges (eds.), Towards a Global Framework for Cyber Peace and Digital Cooperation: An Agenda for the 2020s (Hamburg: Verlag Hans-Bredow-Institut, 2019), https://leibniz-hbi.de/de/publikationen/towards-a-global-framework-for-cyber-peace-and-digital-cooperation.

AUTHOR

PD Mag. Dr. Matthias C. Kettemann, LL.M. (Harvard) is Chair of the Research Program Regulatory Structures and the Emergence of Rules in Online Spaces, Leibniz Institute for Media Research | Hans-Bredow-Institut, Hamburg; project leader The Public International Law of the Internet, Alexander von Humboldt Institute for Internet and Society (HIIG), Berlin; Visiting Professor of International Law at the University of Jena; research group leader Platform and Content Governance, Sustainable Computing Lab, Vienna University of Economics and Business. The research presented here was conducted at the DFG-funded Cluster of Excellence "The Formation of Normative Orders", University of Frankfurt/Main. Contact: matthias.kettemann@hiig.de

"Data Spaces": Data Structures as a Question of Law

KAI VON LEWINSKI[1]

Big data and large databases are resources of power, both in the political and the economic context. The law has so far responded to this new challenge almost exclusively with the means and instruments of data protection law. However, (traditional and current) data protection law has a specific micro-perspective since it primarily regulates individual data processing in relation to a single "data subject". Structural aspects, on the other hand, are almost not addressed at all by current data protection law. It is remarkable to what detail the processing of personal data relating to the gender of a person is regulated, but there are no general legal requirements for the (non-)representation of gender attributes (male, female, or any other) in databases—neither for individuals, nor for groups, and not for society as such.

Data structures are a social power resource although it is not in the research focus yet. This is not only true for databases, but also for taxonomies and formats on which they are based. Those who have the power of definition over data structures decide on whether and how the content is represented in such data structures; and no legal regulatory regime exists so far for this informational power yet. There are no rights to data structures, and there are hardly any obligations regarding the structuring of data, at least not explicitly. Informatic system analysis shows that by the means of structure, type and format decisions with regard to data, "data spaces" may be created and established. And these "data spaces" represent social reality in a specific way, and at the same time "data spaces" do have an impact on social reality. "Data spaces" are means of power which limit the possibilities of others. This demands for legal containment.

It should be the aim of research and politics to address the lack of a legal description of the power emanating from data spaces and to develop a new approach to their legal containment: How can power emanating from data structures be translated into legal categories (beyond the insofar unsuitable data protection law)? What legal instruments exist with regard to this power constellation? Which legal instruments are missing, and what could they look like?

[1] Prof. Dr., University of Passau, Researcher at the HIIG 2013/14.—This text has very much gained from the discussions with *Jörg Pohle* (HIIG) whom I have to thank very much for his computer science ("Informatik") perspective and input.

SOCIAL SIGNIFICANCE OF DATA STRUCTURES, TYPES AND FORMATS

The question of the structure of data and represented data classes is not only a question of theoretical interest. Formal or other restrictions, for example on database entries, can lead to such results that personal names are not mapped according to social reality, at least not according to the identity of the person concerned; more complicated personal names do not easily fit into data fields, especially if foreign letters (umlauts and others) and spellings have to be transcribed. Fiscal budgets and public registers represent only a limited cut-out of reality with a more or less narrow perspective. The same applies to statistics in general.

In addition, the layout of a database can have an effect beyond its original purpose. Every operationally used database forms a "data space" (here not used in its mathematical or informatic meaning) which then interacts with the social reality: It is the purpose of every set of data (database) that it connects data to the person or entity it represents. Such, a representation of features means controllability and the possibility of linking, whereas a non-representation results in non-regulation and the impossibility of linking—or even to the representation of non-existence. An abrogation of the personal status "gender" would, for example, make it impossible to link individuals or groups to their gender; ultimately, this would mean in practice that gender equality programs would no longer be possible, because one cannot distinguish men from women anymore. Another example has been (in Germany until recently) the restriction of data base entries in public resident registers to the binary gender order (male/female) which left existing third genders unrepresented and unrepresentable and consequently administratively non-existing.

Inclusion and exclusion of attributes in data structures have a social effect as well as an individual one. Anyone who can and may decide on the representation of sections of social reality in the logical space of data structures also influences the associated representation of informatic systems in (and into) society. For example, non-existent categories in (sectorial) planning mean that these aspects cannot be taken into account, whereas existing categories produce their (own) relevance.

Whoever determines such a space of possibility, whoever has the power to define storable and then reflected reality, controls a resource of power. In this respect, "data spaces" are also spaces of domination. It is the task of jurisprudence and law to describe and, if necessary, to limit them.

LEGAL BLIND SPOTS AND REGULATORY GAPS

Today's data protection law is narrowed to a concrete close-up perspective and is therefore blind regarding structural concentrations of power. The early data protec-

tion discourse[2], which was strongly linked to the legal informatics of the time in terms of personnel and methods, certainly had had this perspective. The later data protection jurisprudence lost this structural perspective—until today. The (German) Federal Data Protection Acts (Bundesdatenschutzgesetz, BDSG) since 1977 and the EU General Data Protection Regulation (GDPR) focus almost exclusively on the individual. Register law discusses data structures purely descriptively as well[3]. And the findings in computer science, which certainly analyses the social potential of data structures[4], are not translated into legal solution categories.

The existing (European) database law (Database Directive 96/9/EC) refers only to the (intellectual property) right to a database as a whole[5]. Consequently, database law is structurally blind in the sense that it does not address the specific structure of databases, but only a specifically structured data stock. Register law contains only very specific regulations which do not take into account the aspect of concentration of power through structural and format decisions. And data protection law has—as already mentioned—a narrowed and individualistic perspective on data processing and is in particular procedural but does neither address nor even know the category of data structures, or data pools, or data power ("Datenmacht").

In up-and-coming areas like data law and algorithms law as well as in the field of big data, two main approaches are discussed to limit informational and data power: on the one hand, the regulation of algorithms as such and, on the other hand, the limitation of the processing of the underlying data[6]. The former is primarily dealt with in the context of protection against discrimination and in duties to algorithm transparency, the latter is discussed in connection with data protection law (esp. data minimization) or intellectual property figures (so-called "data ownership"). In addition to the regulation of computation itself (algorithm regulation in a narrower

[2] In particular *Steinmüller*, EDV und Recht, 1970; *Simitis*, Informationskrise des Rechts und Datenverarbeitung, 1970; *Kerkau*, Automatische Datenverarbeitung (ADV) – Kybernetik in Rechtswissenschaft und Praxis, 1970; *Dammann*, Datenbanken und Datenschutz, 1974.

[3] For Germany cf. *Krafka*, Einführung in das Registerrecht, 2nd ed. 2008.

[4] Cf. *Stachowiak*, Allgemeine Modelltheorie, 1973; *Stachowiak* (ed.), Modelle – Konstruktion der Wirklichkeit, 1983; *Mahr*, Die Informatik und die Logik der Modelle, Informatik Spektrum 2009, pp. 228–249; *Desrosières*, Die Politik der großen Zahlen, 2005, esp. chap. 8; most recently *Guagnin/Pohle*, Welt -> Modell -> Einschreibung -> Welt', fiffkon18, 2018 (https://media.ccc.de/v/fiffkon18-10-welt_-_modell_-_einschreibung_-_welt).

[5] Comprehensive for the law making process *Indranath Gupta*, Footprints of Feist in European Database Directive: A Legal Analysis of IP Law-making in Europe, 2017; from a German perspective *Conrad/Grützmacher* (eds.), Recht der Daten und Datenbanken im Unternehmen (= Festschrift J. Schneider), 2014.

[6] Cf. the research project „Algorithmenkontrolle als Regulierungsaufgabe" at the University of Speyer by *Mario Marini* et al. (http://www.foev-speyer.de/en/research/digitization/data-driven-performance-of-public-sector-tasks/algorithm-control-as-regulatory-task.php?p_id=1904).

sense) and the regulation of data as such (conventional data protection; intellectual property law), the structure of data bases must also become a subject of regulative considerations. This is a third legal dimension in the field of data law, which has not yet been examined in detail.

This clearly shows a blind spot in legal science and legal informatics. An analysis of the existing legal regulations shows that so far no regulation addresses the problem of data structures as a power resource as such, let alone interactions between IT system and social reality.

PERSPECTIVES AND FIELDS OF FURTHER RESEARCH

For a better social understanding of information society, legislation and courts should become aware of relevant constellations of inclusion and exclusion in "data spaces", be it the name which is now only computer-compatible but incorrectly written, be it the consideration of a category relevant to planning but not provided for in planning law, be it a third gender.

A first research step would be a comprehensive collection of relevant regulations and regulatory perspectives. Since—as mentioned above—data protection law and intellectual property law do not offer the full answer, register law could turn out to be a productive source which has received only little scientific attention yet. Another important field of reference will be tax law, rules for the public budget and accounting law as well as planning law.

Additionally, the early years of legal informatics (esp. in Germany, the so-called "Rechtsinformatik" of the 1970s), should be re-visited and re-read. Researchers in these years had described the interaction and retroactivity of informatic and social systems with the means of the (meanwhile forgotten) system-theoretical "classical" legal informatics[7] (initially also known as "legal cybernetics" ["Rechtskybernetik"])[8]. This approach might add the perspective, that data structures and taxonomies form "data spaces" in which and through which power can be exercised and which constitute a means of control.

If it turns out to be true that jurisprudence has a blind spot regarding "data spaces" and data structures, it has to be filled with light. Such light might come from

[7] E.g. *Podlech*, Information – Modell – Abbildung – Eine Skizze, in: Steinmüller (ed.), Informationsrecht und Informationspolitik, 1976, pp. 21–24; *Harbordt*, Computersimulation in den Sozialwissenschaften 1 – Einführung und Anleitung, 1974; *Dammann*, Datenbanken und Datenschutz, 1974; retrospectively *Heibey*, Zu den Anfängen der informatischen Wirkungsforschung: Die Theorie der Informationsveränderungen, in: Garstka/Coy (eds.), Wovon – für wen – wozu. Systemdenken wider die Diktatur der Daten (= Gedächtnisschrift Steinmüller), 2014, pp. 131–144; comprehensively to the early years of the "Rechtsinformatik" *Gräwe*, Die Entstehung der Rechtsinformatik, 2011.

[8] Cf. *Simitis*, Rechtliche Anwendungsmöglichkeiten kybernetischer Systeme, 1966; *Suhr*, Zur Einführung: Recht und Kybernetik, JuS [Juristische Schulung] 1968, pp. 351–353; *Haft*, Nutzanwendungen kybernetischer Systeme im Recht (Diss. jur. Gießen) 1968; *Podlech*, Rechtskybernetik – Eine juristische Disziplin der Zukunft, in: Erdsiek (ed.), Juristen-Jahrbuch 10 (1969/1970), pp. 157 et seq. – The term „Rechtskybernetik" came out of use soon.

constitutional law. An innovative idea might be whether an unwritten fundamental right to identity[9] would include a right to self-determined representation in "data spaces". Other (and more conventional) constitutional law categories should be considered, adapted and adopted as well, such as the rule of law. These fundamental values can then be reflected and mirrored back on the existing legal provisions to outline applicable solutions for the legal practice.

To put it into a nutshell: The outlined new legal approach tries to understand structures of "data spaces" and the format of data sets not merely as immaterial property but as an informational resource of social power.

[9] *Kieck*, Der Schutz individueller Identität als verfassungsrechtliche Aufgabe, 2019.

On Measuring Fundamental Rights Protection: Can and Should Data Protection Law Learn From Environmental Law?

JÖRG POHLE

Data protection, understood as the protection from the negative consequences of the increasing 'datafication' of the world[1] and 'industrialization' of information processing[2] for individuals, groups and the society, and environmental protection share three structural characteristics.[3]

The first common feature is the universality of the problems. Both data protection and environmental protection are responses to an ever increasing scope and permeation of today's technology that has made the whole earth the prerequisite, the object and the result of technical processes, the natural world as well as the social world. Data protection is the response to the fact that information technologies make information universally available and computable, fundamentally change forms, situations and contents of individual and societal communication, and allow for those who control these technologies to amass power and to amplify, consolidate and perpetuate control over their environment.[4]

The second common feature of the two problem areas is that they both touch on the very identity of modern Western societies, they are what in the past has been called "existential". They are both downsides of progress – or: "progress" –, which for a very long time was perceived along the lines of: progress in enlightenment, progress in technology, progress in living conditions. Both regarding the industrialisation of material production and of information processing, the limits to growth, the limits to (technological) progress are becoming ever more visible.

At least in Germany, and maybe more generally in the European Union as well, there is a third common feature: political demands are mainly directed towards the state, touching on a particular understanding of the (constitutional) state. Both data

[1] Fiedler, Herbert (1975), Datenschutz und Gesellschaft. In: Siefkes, D. (ed.), *GI – 4. Jahrestagung*. Berlin: Springer, pp. 68–84.

[2] Steinmüller, Wilhelm (1981), Die Zweite industrielle Revolution hat eben begonnen – Über die Technisierung der geistigen Arbeit. In: *Kursbuch* 66, pp. 152-188.

[3] Podlech, Adalbert (1987), Der Datenschutz und die Akzeptabilität unserer Gesellschaftsordnung. In: Hohmann, H. (ed.), *Freiheitssicherung durch Datenschutz*. Frankfurt am Main: Suhrkamp, pp. 19–24.

[4] For an introduction to this broad understanding of data protection see Pohle, Jörg (2016), Transparenz und Berechenbarkeit vs. Autonomie- und Kontrollverlust: Die Industrialisierung der gesellschaftlichen Informationsverarbeitung und ihre Folgen. In: *Mediale Kontrolle unter Beobachtung* 5(1), Article 5.

protection and environmental protection are thus eminently political issues, which at the same time defy the oversimplified dichotomy of "an affirmation of the strong state and the subordination of data protection to state necessities vs. an emphasis on the freedom of the citizen and a preference of data protection over the effectiveness of government action".[5]

ENVIRONMENTAL LAW'S INCREASING DRIVE TOWARDS QUANTIFICATION

Against this background, it is rather surprising that the overlap between data protection and environmental protection has not extensively been covered in the scholarly literature. This contribution to the *liber amicorum* for Ingolf Pernice will shed some light on a peculiar aspect of the last decades' development in both the environmental protection discourse and law that may provide a possible starting point for investigating how today's data protection law might be further developed in order to strengthen its application as well as its enforcement in practice: the drive towards quantification.

At the very same time, this idea taps well into Ingolf Pernice's extensive experience in shaping environmental protection law and institutions: as a member of the European Commission's Legal Service from 1987 to 1993, Ingolf Pernice not only encouraged the founding of the European Environment Agency (EEA), but also participated as a legal advisor of the European negotiating delegation at the United Nations Conference on Environment and Development (UNCED), better known as the Rio Summit, in 1992. Both the EEA and the Rio Summit are deeply linked to environmental law's increasing reliance on quantification.[6]

The EEA's mission is to provide independent information on the environment for policy-makers. This information is based on the DPSIR framework – Drivers, Pressures, State, Impact and Response model of intervention –, a causal framework describing the interdependent interactions between society and the environment,[7] which is an extension of the PSR model – Pressure, State, Response – developed by OECD in the 1980s.[8]

The most important achievement of the Rio Summit, held in June 1992, was an agreement on the United Nations Framework Convention on Climate Change (UNFCCC) which in turn led to the Kyoto Protocol, adopted in 1997, and the Paris Agreement, adopted in 2015. Whether the UNFCCC's objective of stabilising

[5] Podlech (1987), op. cit., pp. 22–23. The German text refers to "Bürger", it most probably means "subjects of fundamental rights" though.

[6] Moldan, Bedrich; Janoušková, Svatava & Hák, Tomáš (2012), How to understand and measure environmental sustainability: Indicators and targets. In: *Ecological Indicators* 17, pp. 4–13.

[7] Smeets, Edith & Weterings, Rob (1999), *Environmental indicators: Typology and overview.* European Environment Agency, Technical report No. 25.

[8] Lehtonen, Markku (2008), Mainstreaming sustainable development in the OECD through indicators and peer reviews. In: *Sustainable Development* 16, pp. 241–250.

greenhouse gas concentrations in the atmosphere, the Kyoto Protocol's objective of reducing greenhouse gas emissions or the Paris Agreement's objective of decreasing global warming – they all demand for and depend on quantifying properties of the environment to create indicators that guide the implementation of policies, the selection of specific measures as well as the monitoring of achievements.

QUANTIFICATION'S JANUS-FACEDNESS

The greatest challenge with regards to quantification is that it's not just a new or different description of the social and the natural world, but a means of reconfiguring them. The very process of quantification imposes new meanings on the world and makes old ones disappear.[9] At the same time, it is a *social* process of assigning numbers to the natural and the social environment.[10] Quantification has been identified as a potential driver towards a (further) depoliticization of inherently political issues,[11] which fundamental rights certainly are, and merely attempting to quantify fundamental rights like human dignity or personal freedom might result in a loss of legitimacy.[12] It has advantages as well, though, and that's the very reason for exploring its applicability. The main advantage is that it simplifies comparison between different approaches and means of protection, and at the same time goes beyond subjective views and individual interests. For example, quantification, or more broadly: formalization, would prevent (supreme or constitutional) courts from simply generating cloudy outpourings, as they do now, that in the end must lead to arbitrary results, which not only structurally undermines fundamental rights, but also the courts' legitimacy.[13] The very process of making things auditable[14] would demand greater clarity, though it would also introduce more contingency, regarding the object of protection and the conditions under which they are or may be threatened in order to develop suitable as well as societally acceptable indicators for their protection. It would thus prevent scholars, legislators and engineers from hiding behind the smoke screens that are produced by mingling arbitrary, one-sided understandings of essentially

[9] Porter, Theodore M. (1994), Making Things Quantitative. In: *Science in Context* 7(3), pp. 389–407.

[10] "It is *we* who assign numbers to nature." Carnap, Rudolf (1966), *Philosophical Foundations of Physics: An Introduction to the Philosophy of Science.* New York: Basic Books, p. 100.

[11] Harbordt, Steffen (1975), Die Gefahr computerunterstützter administrativer Entscheidungsprozesse: Technokratisierung statt Demokratisierung. In: Hoffmann, G. E.; Tietze, B. & Podlech, A. (eds.), *Numerierte Bürger*. Wuppertal: Peter Hammer Verlag, pp. 71–77; Lischka, Konrad & Stöcker, Christian (2017), *Digitale Öffentlichkeit: Wie algorithmische Prozesse den gesellschaftlichen Diskurs beeinflussen*. Working paper, ed. by Bertelsmann Stiftung.

[12] Grechenig, Kristoffel & Lachmayer, Konrad (2011), Zur Abwägung von Menschenleben – Gedanken zur Leistungsfähigkeit der Verfassung. In: *Journal für Rechtspolitik* 19, pp. 35–45.

[13] For an early critique on this development see Schlink, Bernhard (1974), *Abwägung im Verfassungsrecht.* Berlin: Duncker & Humblot.

[14] Power, Michael (1996), Making Things Auditable. Accounting. In: *Organizations and Society* 21(2/3), pp. 289–315.

contested concepts[15] with terminological coincidence, such as "privacy", "anonymity" or "dignity", as it is common practice nowadays.

FORMALIZATION AND QUANTIFICATION IN PRIVACY AND DATA PROTECTION LAW (DISCOURSE)

The field of privacy and data protection law has a long, but thin and severely lopsided history of discourses on measuring both risks, or threats, and protection from these risks and threats.

ON MEASURING PRIVACY AND ANONYMITY

The first proposal of a measurable indicator for protecting the privacy of people was made in the 1960s in the Senate Hearings on Computer Privacy. In what has much later been called *k*-anonymity, a computer system would be built to allow "output data only in aggregates that contain a sufficient number of individual respondents to make identification of individuals difficult"[16], with the *k*, i.e. the number of people among which an individual would be indistinguishable, hence *k*-anonymity, chosen according to the risks, threats or possible damages caused by an attacker being able to identify an individual. This kind of "statistical disclosure control"[17] thus obviously builds upon the assumption that identifiability of the individual is a causal condition for the kind of consequences that this understanding of privacy aims to prevent or mitigate.

This assumption of causality between the individuals' identifiability and the impact on their fundamental rights and freedoms has been the leitmotif of both the research and the public discussion regarding suitable indicators for privacy protection ever since. It is thus no surprise that anonymity is generally seen as a guarantee for the protection of the data subjects' rights and freedoms, and thus perceived as a meaningful goal for both regulation and systems design.[18] Unfortunately, this assumption of causality between identifiability and impact is not only hardly ever made explicit, but also never proven.[19]

At the same time, this common reference to anonymity does not imply a shared understanding of the very concept of anonymity across disciplines, such as between

[15] Gallie, Walter Bryce (1956), Essentially Contested Concepts. In: *Proceedings of the Aristotelian Society* 56, pp. 167–198.

[16] Miller, Arthur Raphael (1969), Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information-Oriented Society. In: *Michigan Law Review* 67(6), pp 1089–1246, 1217.

[17] Dalenius, Tore (1977), Towards a methodology for statistical disclosure control. In: *Statistik Tidskrift* 15, pp. 429–444.

[18] Van Rossum, H. et al. (1995), *Privacy-Enhancing Technologies: The Path to Anonymity*. Information and Privacy Commissioner / Ontario, Canada & Registratiekamer, The Netherlands.

[19] Pohle, Jörg (to appear), Technisch abgesicherter Freiheitsschutz jenseits von Privatheit. Folgerungen aus der produktivsten Phase der Datenschutzdebatte für die Digitalmobilität. In: Klumpp, D. (ed.), *Datengovernance für Digitalmobilität*.

law and computer science,[20] as terminological coincidence does not imply conceptual similarity. It thus seems rather counterproductive for the protection of fundamental rights and freedoms that developments such as *k*-anonymity and its derivatives like *l*-diversity[21] or *t*-closeness[22], or differential privacy[23], but also secure multi-party computation[24] or federated machine learning[25], which are currently very in vogue, are uniformly acclaimed and the companies that use such methods are widely praised.

Even more questionable is that the applicable data protection law, such as the EU General Data Protection Regulation, is built upon and strongly depends on this false assumption of causality. It is thus the only legal implementation of a protection of fundamental rights in which this protection is made dependent on the fact that those who infringe on the fundamental rights – more precisely: the actors who create or operate sources of risk for such rights – have positively identified or are able to identify the particular fundamental rights' holders beforehand.[26]

There are other privacy metrics beyond those that are based on the equation of privacy with anonymity.[27] Unfortunately, they all refer to understandings of privacy where privacy equals either secrecy or confidentiality, and always – at least implicitly – confined to "sensitive" information.[28] This problem is aggravated by increasingly placing hopes in technical privacy solutions, which are oftentimes collectively called Privacy-Enhancing Technologies (PETs): the very way these technical solutions are

[20] Hölzel, Julian (2019), Differential Privacy and the GDPR. In: *European Data Protection Law Review* 5(2), pp. 184–196.

[21] Machanavajjhala, A. (2007), *l*-Diversity: Privacy Beyond *k*-Anonymity. In: *ACM Transactions on Knowledge Discovery from Data (TKDD)* 1(1), article no. 3.

[22] Li, Ninghui; Li, Tiancheng & Venkatasubramanian, Suresh (2007), *t*-Closeness: Privacy Beyond *k*-Anonymity and *l*-Diversity. In: Chirkova, R. et al. (eds.), *Proceedings of the 23rd International Conference on Data Engineering (ICDE 2007)*. Washington, DC: IEEE Computer Society, pp. 106–115.

[23] Dwork, Cynthia (2006), Differential Privacy. In: *Automata, languages and programming (ICALP 2006)*. Part II. Berlin: Springer, pp. 1–12.

[24] Chaum, David; Damgård, Ivan B. & van de Graaf, Jeroen (1988), Multiparty Computations Ensuring Privacy of Each Party's Input and Correctness of the Result. In: Pomerance, C. et al. (eds.), *Advances in Cryptology — CRYPTO '87*. Berlin: Springer, pp. 87–119.

[25] Bonawitz, Keith et al. (2017), Practical Secure Aggregation for Privacy-Preserving Machine Learning. In: Thuraisingham, B. et al. (eds.), In: *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS '17)*. New York: ACM, pp. 1175–1191.

[26] For an early critique on this self-limitation see Brinckmann, Hans (1982), Vom Datenschutzrecht zum Recht des Verbraucher-, Arbeits- und Umweltschutzes. In: *Datenschutz und Datensicherung* 6(3), pp. 157–164, 158. See also the contribution of Julian Hölzel in this volume.

[27] For an exhaustive overview see Wagner, Isabel & Eckhoff, David (2018), Technical Privacy Metrics: A Systematic Survey. In: *ACM Computing Surveys (CSUR)* 51(3), article 57.

[28] It has been long established that all sensitivity classification is arbitrary, especially in the field of law, see Simitis, Spiros (1990), „Sensitive Daten" – Zur Geschichte und Wirkung einer Fiktion. In: Brem, E. et al. (eds.), *Festschrift zum 65. Geburtstag von Mario M. Pedrazzini*. Berne: Stämpfli & Cie, pp. 469–493. It has also been shown early in the debate that sensitivity is not a property of information, see Steinmüller, Wilhelm et al. (1971), *Grundfragen des Datenschutzes*. Expertise on behalf of the German Ministry of the Interior, German Bundestag Record No. VI/3826, Appendix 1, p. 73.

constructed, i.e. as computable representations of the world, both drives and is driven by the apparent straightforwardness of these metrics and the illusive ease of their application.

ON (NOT) MEASURING DATA PROTECTION

The data protection debate always had a focus on anonymity as strong as the privacy debate[29], but much less so on secrecy or confidentiality. It has, however, also looked beyond anonymity, secrecy and confidentiality in its search for formalization and measurability of fundamental rights protection – though with mixed results.

Against the backdrop of extensive research in the field of legal informatics, which had a particular focus on how to formulate legal provisions in order to ensure their suitability for automation,[30] for some time the debate strongly engaged with the formalization of legal requirements for fundamental rights protection, including the "descriptiveness of the necessity relation", "model adequacy", or "sufficient validity".[31] Within this research field, particular attention has been paid to the formalization of purpose(s), the relations between purposes as well as purposes and sub-purposes, and purpose-binding[32] – though without any long-term effects on the broader data protection research or practice.

Explicit attempts to employ quantifiable indicators for both risks to and protection of fundamental rights have long been limited to references to the quantity of data about individuals to be processed.[33] The very construction of this indicator is based on the assumption that the less personal data about an individual is collected, stored and processed, the smaller the risks are for the individual's fundamental rights.[34]

The main strand of the debate has instead focused on procedural measures, such as codes of conduct, data protection authorities' decisions or sanctions imposed on non-compliant data controllers.[35] A key argument was that attempting to establish per-

[29] Starting as early as 1970, cf. Steinmüller, Wilhelm (1970), *EDV und Recht – Einführung in die Rechtsinformatik*. Berlin: J. Schweitzer Verlag, p. 88.

[30] Cf. von Berg, Malte (1968), *Automationsgerechte Rechts- und Verwaltungsvorschriften*. Cologne: G. Grote'sche Verlagsbuchhandlung.

[31] Podlech, Adalbert (1982), Individualdatenschutz – Systemdatenschutz. Brückner, K. & Dalichau, G. (eds.), *Beiträge zum Sozialrecht – Festgabe für Grüner*. Percha: Verlag R. S. Schulz, pp. 451–462.

[32] Hoffmann, Bernhard (1991), *Zweckbindung als Kernpunkt eines prozeduralen Datenschutzansatzes*. Baden-Baden: Nomos Verlagsgesellschaft.

[33] Starting as early as 40 years ago, e.g. Burkert, Herbert (1985), *Datenschutz und Informations- und Kommunikationstechnik. Eine Problemskizze*. Workshop report no. 6. Ministry for Labour, Health and Welfare North Rhine-Westphalia, pp. 14ff.

[34] Pohle, Jörg (2014) Kausalitäten, Korrelationen und Datenschutzrecht. In: Pohle, J.; Knaut, A. (eds.), *Fundationes I: Geschichte und Theorie des Datenschutzes*. Münster: Monsenstein und Vannerdat, pp. 85–105 (paragraph 28).

[35] This has been quite harshly criticised by many scholars, cf. e.g. De Hert, Paul & Gutwirth, Serge (2006), Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power. In: Claes, E.; Duff, A. & Gutwirth, S. (eds.), *Privacy and the Criminal Law*. Antwerpen: Intersentia, pp. 61–104 (71, 77f., 87ff.).

formance indicators is fraught with the central difficulty of data protection law's goals being vague and contested.[36] While this argument is based on an understanding of data protection laws' goal being the protection of privacy, with privacy itself being essentially contested,[37] it hasn't yet been re-evaluated against the backdrop of the EU General Data Protection Regulation's clear and unambiguous formulation of the law's goal in Article 1(2), i.e. to protect "fundamental rights and freedoms of natural persons".

Where the General Data Protection Regulation refers to measurable indicators, most of them are constructed from the perspective of the controller and the controller's information processing, not from the perspective of the data subject. For example, Articles 24, 25 and 32 GDPR refer to the scope of the processing, while Recitals 62, 75 and 91 refer to the number of data subjects. Thus, in essence these indicators don't indicate risks to fundamental rights. Instead, they seem to be used for the simple reason that they are measurable.[38] The only exception is the Regulation's reference to the likelihood and severity of risks for fundamental rights and freedoms in Articles 24, 25 and 32, though both the scholarly literature and the commentaries then fail to operationalise fundamental rights and freedoms. They all simply refer to the list in Recital 75, which includes references to the amount and other properties of the personal data, the number of data subjects affected, but also the unauthorised reversal of pseudonymisation. Explicit references to fundamental rights and freedoms are both scarce and superficial: "discrimination" and "where data subjects might be deprived of their rights and freedoms". A similar superficiality can be observed in the scholarly literature, which conflicts with the extensive coverage of other harms, such as distress, anxiety or to the individual's reputation.[39]

Last but not least, there is a small strand of research that focuses on using formal models to translate data protection requirements into technical requirements which are then to be implemented into ICT systems.[40]

[36] Raab, Charles D. & Bennett, Colin J. (1996), Taking the measure of privacy: can data protection be evaluated? In: *International Review of Administrative Sciences* 62, pp. 535–556.

[37] Mulligan, Deirdre K.; Koopman, Colin & Doty, Nick (2016), Privacy is an essentially contested concept: a multi-dimensional analytic for mapping privacy. In: *Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences* 374(2083), p. 20160118.

[38] Such shift has long been observed in organisational studies, see Kling, Rob (1980), Social analyses of computing: Theoretical perspectives in recent empirical research. In: *ACM Computing Surveys (CSUR)* 12(1), pp. 61–110 (81–83).

[39] Cf. e.g. Wagner, Isabel & Boiten, Eerke (2018), Privacy Risk Assessment: From Art to Science, by Metrics. In: Garcia-Alfaro, J. et al. (eds.), *Data Privacy Management, Cryptocurrencies and Blockchain Technology. ESORICS 2018 International Workshops, DPM 2018 and CBT 2018, Proceedings.* Cham : Springer, pp. 225–241.

[40] See e.g. Bräutigam, Lothar; Höller, Heinzpeter & Scholz, Renate (1990), *Datenschutz als Anforderung an die Systemgestaltung.* Opladen: Westdeutscher Verlag; or Fischer-Hübner, Simone (1994), Ein formales Datenschutz-Modell. In: Bauknecht, K. & Teufel, S. (eds.), *Sicherheit in Informationssystemen.* Zurich: vdf Hochschulverlag AG, pp. 107–119.

TOWARDS MEASURABLE INDICATORS FOR FUNDAMENTAL RIGHTS PROTECTION

The debate has yet to produce meaningful indicators for both risks to and protection of fundamental rights and freedoms, let alone measurable indicators, that takes into account what these rights and freedoms actually guarantee.[41]

The simplest approach would be to count the number of rights and freedoms affected, whether because there is data collected on the exercise of these rights and freedoms, the processing or use of data impinges on their exercise, or their exercise is affected, e.g. inhibited, restricted or controlled, by the information and communication technology imposed upon or used by the fundamental rights' holder. The impact on fundamental rights could either be direct or indirect, e.g. by chilling effects[42], with the latter being much harder to assess than the former.[43] A sociological equivalent to the fundamental rights coverage might be the number of societal subsystems (Talcott Parsons, Niklas Luhmann), subfields (Pierre Bourdieu) or spheres of life (Ferdinand Schoeman) covered or affected by the data, the data processing and use, or the technology.[44] Another alternative indicator might be the number of covered or affected social roles, i.e. sets of rights, duties, expectations, norms and behaviors that an individual has to face and fulfill.[45] The most well-known societal roles include citizens, family members, employees, customers, or patients, with data protection then understood as protecting the functional differentiation of these social roles with their associated promises of freedom vis-à-vis powerful organisations.[46]

This reference to powerful organisations might lead to a second indicator that could be made quantifiable: the power imbalance between such organisations and those that depend on them, e.g. their audiences, or are affected by their informational activities or the technology they design, develop and operate. This approach would tap into the long history of understanding data protection as a means for condition-

[41] On this understanding of fundamental rights and freedoms see Rusteberg, Benjamin (2009), *Der grundrechtliche Gewährleistungsgehalt : Eine veränderte Perspektive auf die Grundrechtsdogmatik durch eine präzise Schutzbereichsbestimmung*. Tübingen: Mohr Siebeck.

[42] White, Gregory L. & Zimbardo, Philip G. (1975), *The Chilling Effects of Surveillance: Deindividuation and Reactance*. ONR Technical Report Z-15, Los Angeles: Office of Naval Research.

[43] Cf. Staben, Julian (2016), *Der Abschreckungseffekt auf die Grundrechtsausübung – Strukturen eines verfassungsrechtlichen Arguments*. Tübingen: Mohr Siebeck.

[44] Cf. Pohle, Jörg (2012), Social Networks, Functional Differentiation of Society, and Data Protection. *arXiv:1206.3027* [cs.CY]. Retrieved from https://arxiv.org/abs/1206.3027.

[45] The concept of (social) role was originally introduced by Linton, Ralph (1936), *The Study of Man : An Introduction*. New York: Appleton-Century-Crofts, pp. 113–131; and strongly shaped by Parsons, Talcott (1951), *The Social System*. Glencoe: Free Press.

[46] Müller, Paul J. (1975), Funktionen des Datenschutzes aus soziologischer Sicht. In: *Datenverarbeitung im Recht* 4, pp. 107–118.

ing of power asymmetries.[47] One the one hand, this indicator would be somewhat related to the size of a data controller, which is used in Section 38(1) German Federal Data Protection Act to define whether a data protection officer must be appointed. On the other hand, the size of a data controller itself has been shown to be a bad indicator for the risks posed by an organisation in the digital era.[48]

Regarding the individual rights and freedoms, societal subsystems or social roles, a sensitive indicator could be how extensive is the coverage or how much meaningful freedom is left unsurveilled, unrecorded or uncontrolled.[49] Unfortunately, this indicator does not seem to allow for easy quantification, though it is already used indirectly to assess the "additive encroachment on fundamental rights".[50]

Thus, the situation seems quite daunting: most attempts to quantification and measurement in the privacy and data protection field have ended up in a blind alley, either by producing indicators that do not indicate risks to or protection of fundamental rights and freedoms, or by getting forgotten in the meandering discourse of the past fifty years in this field. It is time to go beyond the oversimplified quantifications that characterise today's debate, the almost sole focus on the data subjects' identifiability or the number of affected people. It is time to restart the quest for suitable measurable indicators that directly address the fundamental rights and freedoms at stake, with the promises they entail and the spheres of freedom they create.

[47] Cf. Scheuch, Erwin K. (1974), Datenschutz als Machtkontrolle. In: Dammann, U. et al. (eds.), *Datenbanken und Datenschutz*. Frankfurt am Main: Herder & Herder, pp. 171–176; Rost, Martin (2014), Neun Thesen zum Datenschutz. In: Pohle, J. & Knaut, A. (eds.), *Fundationes I: Geschichte und Theorie des Datenschutzes.* Münster: Monsenstein und Vannerdat, pp. 37–44.

[48] Pohle, Jörg (2018), *Datenschutz und Technikgestaltung: Geschichte und Theorie des Datenschutzes aus informatischer Sicht und Folgerungen für die Technikgestaltung.* Doctoral dissertation, Humboldt-Universität zu Berlin, Germany, p. 241. Retrieved from https://edoc.hu-berlin.de/handle/18452/19886.

[49] See for an approach to construct an analysis of the remaining freedoms Pohle, Jörg (2019), Freiheitsbestandsanalyse statt Überwachungs-Gesamtrechnung – Ein Alternativvorschlag. In: *FIfF-Kommunikation* 36(4), pp. 37–42.

[50] Starnecker, Tobias (2017), *Videoüberwachung zur Risikovorsorge. Body-Cam zur Eigensicherung und Dashcam zur Beweissicherung – Eine verfassungs- und datenschutzrechtliche Analyse.* Berlin: Duncker & Humblot, pp. 365–366.

IMPRINT

PUBLICATION
July 2020

EDITORS
The Global Constitutionalism and the Internet Working Group (HIIG)

Alexander von Humboldt Institute for Internet and Society
Französische Straße 9
10117 Berlin
Germany
www.hiig.de

LAYOUT
Jörg Pohle (HIIG)

Softcover ISBN: 978-3-9821760-1-7
eBook ISBN: 978-3-9821760-2-4