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.