4 - 8 DECEMBER 2023

SUPPORTED BY THE LORENTZ CENTER

DIGITAL LEGAL LAB’S WINTER SCHOOL

"DATA, PERSONALIZATION, AND THE LAW 2023"

e-Booklet of proceedings

Edited by Tjaša Petročnik, Alina Girbea, and Gergana Tsvetkova

TABLE OF CONTENTS

NIAS
Lorentz center
Workshop @Oort
Data, Personalization, and The Law
4 - 8 December 2023, Leiden, the Netherlands

This workshop will explore how data aggregation and analytics affect legal norms and values. Image by Colin Anderson. Poster design: SuperNova Studios . NL

FOREWORD FROM THE SCIENTIFIC ORGANISERS

Our society is increasingly transitioning to a digital one, and the implications of this shift raise important questions – among others those related to the fitness of our current regulatory paradigms to handle them. While in the recent years, several regulatory instruments have been introduced to tackle these and other emerging concerns, the issues related to data-driven technologies and law remain at the forefront of scholarly and policy debates. To address these issues, Digital Legal Lab organised a winter school titled “Data, personalization, and the law 2023”, which took place from 4 to 8 December 2023 at the Lorentz Center in Leiden, the Netherlands. The aim of the winter school was to explore how digital technologies like algorithms, big data analytics, personalisation, and automated decision-making affect individuals, markets and economy, and the society and how are the legal assumptions and concepts, paradigms, and regulatory regimes catching up with these technological cha(lle)nges.

Through lectures by the leading experts in their respective fields, including Digital Legal Lab’s own researchers, discussions, and group work, the participants were encouraged to reflect upon the regulation of digital technologies in the EU and more broadly, as well as on how to study and frame the complex and dynamic (societal) implications of such technological developments. For example, one could ask how will the transition to a data-driven society impact legal processes and decision-making and -enforcing; how is law furthering and containing the power of digital platforms; how does digitalisation affect the observance of fundamental rights and values; and how can we, in turn, leverage the potential of digital technology to gain new insights about law and legally-relevant issues and formulate better evidence-based policies.

To these inquiries, various answers were provided throughout the week's programme of the winter school – and further questions raised, including from the truly diverse perspectives of the attending participants. One of the outcomes of the winter school "Data, personalization, and the law 2023" is therefore this e-booklet of proceedings, which comprises the written contributions of all of the researchers that attended it. Each of them was asked to present their own research and situate it in the broader context of Digital Legal Studies, an emerging field of scholarship that aims to advance the knowledge on how digital technologies interact with law and justice. The contributions are arranged according to the cross-cutting themes that emerged and are woven through the participants' research interests, covering i) digital governance considerations, ii) conceptual questions, and iii) specific regulatory issues.

The richness of the contributions contained in the e-booklet points to the variety of the matters discussed throughout the course of the week, and to the wealth of topics early career researchers are exploring in this domain. Even more so, the tapestry of the topics shows that studying (the regulation of) digital technologies will, more than even, require collaboration and interdisciplinarity. Positioned at the intersection of various legal regimes, perspectives, and disciplines, the field of Digital Legal Studies thus seems a perfect avenue to do just that.

To conclude, we would like to thank the participants for their commitment and enthusiasm, as well as the speakers for their valued expertise. The winter school allowed us to hold a meaningful conversation on the pressing issues relating to the (regulation of the) digital economy and society and we hope that this e-booklet opens up the debate also to the wider interested public.

Scientific organisers,

Digital Legal Lab members Tjaša Petročnik, Tilburg University; Dr Ronan Fahy, University of Amsterdam; Dr Aurelia Tamo-Larrieux, Maastricht University/University of Lausanne; Belle Beems, Radboud University; and Yelyzaveta Markova, Radboud University

Acknowledgements: The organisation of the winter school was possible thanks to the funding provided by the Digital Legal Lab and the financial and logistical support from the Lorentz Center, for which we are very grateful.

NIAS
Lorentz center
Workshop @ Oort
Data, Personalization, and The Law
4 - 8 December 2023, Leiden, the Netherlands

DATA LOCALIZATION AND OWNERSHIP AS PATH TOWARD DATA DECOLONIZATION

Pratiksha Ashok

1. Data Colonization

When powerful entities or nations extract and control valuable data from less powerful regions or countries, often mirroring historical colonial practices, it is referred to as data colonization. The mechanics involve exploiting digital resources and information, leading to economic, social, and technological power imbalances. Similar to historical colonization, data colonization can become normalized, with the dominant entities asserting their control over data as if it is a natural state of affairs. This can result in the acceptance of data extraction as a given despite potential negative impacts on local populations and economies.

Data colonization is similar to the traditional, historical concept of colonization where powerful nations established control over foreign territories, often exploiting their resources, imposing cultural dominance, and shaping local institutions to serve colonial interests.

2. Decolonization

Decolonization, on the other hand, signifies the subsequent movement where formerly colonized nations sought independence and the restoration of their sovereignty. This process unfolded in the mid-20th century as a wave of nations across Africa, Asia, and the Americas gained autonomy through diplomatic negotiations, armed struggles, or a combination of both. Decolonization marked a significant shift in global power dynamics, reshaping geopolitical landscapes and fostering a renewed emphasis on self-determination, national identity, and human rights. Despite achieving political independence, many post-colonial nations faced ongoing challenges related to economic development, social cohesion, and the reconciliation of colonial legacies.

Reparation and repatriation are two important concepts that can be considered as methods of decolonization, aiming to address historical injustices and mitigate the enduring impacts of colonization on affected communities. Reparation involves compensating individuals or groups for past harms inflicted during the colonial era. This compensation can take various forms, including financial restitution, land redistribution, or investments in social and economic development. In relation to data decolonization, this will not work because financial compensation for data would mean that there is a certain monetary value attached to the data, making data a tradable commodity. As data and its protection is largely considered as a fundamental right and their monetization and paying reparations for data collections is not an ideal solution.

Repatriation involves the return of displaced populations or cultural artifacts to their places of origin. In the context of decolonization, this can include the return of indigenous lands, repatriation of indigenous peoples forcibly removed from their territories, and the return of cultural artifacts taken during the colonial period. Repatriation in relation to data decolonization will not work because this would mean returning the data to the data subject as an individual or the nation in which they were collected. This would lead to fracturing data sets and for the individual who already has their data, it is not necessitated to return receive their own information from the colonizers.

3. Data Colonization in India

In India, concerns related to data colonization center on the disproportionate influence of multinational tech corporations, predominantly based in Western countries, over the vast amounts of data generated by Indian users. This phenomenon raises apprehensions about economic imbalances and questions the equitable distribution of benefits derived from the data. The discussions around data colonization underscore the importance of India's efforts to establish robust data governance policies to navigate the complexities of the digital economy and safeguard the sovereignty of its data landscape.

4. Data Decolonization in India

4.1. Data Ownership

4.1.1. Traditional Concept

Data ownership refers to the legal and ethical rights a person or entity has over the data they generate, collect, or manage. It involves control over how data is used, shared, and accessed. In the context of individuals, data ownership refers to the rights individuals have over information that pertains to them, such as personal details, preferences, and behaviors. For organizations, data ownership extends to the information they collect, process, and generate in the course of their operations. Data ownership is not actually about ownership. It is about consent and control. When people refer to data ownership, they mean data protected by a property rule, and not actually ownership rights over data. One can see this from the language used in the literature and the emphasis placed on consent.

4.1.2. Data ownership in India

The Draft National e-Commerce Policy (Policy) is aimed to address concerns which go beyond the sale and purchase of products by electronic means. In the era of Industrial Revolution 4.0, economic development is based on data which is generated, stored, transmitted or processed in large volumes. The Policy states that the increasing importance of data warrants treating it at par with other resources on which a country would have sovereign right. The Policy equates data to any other natural resource. like oil and similar to such natural resources, the Government has control over these resources. They represent the will of their citizens and control and distribute natural resources. The Policy recognizes the importance of data while enabling the domestic industry to benefit from the advantages and opportunities created by electronic commerce. Thus, the Government controls the use and distribution of data, like a natural resource.

4.2. Data Localisation

4.2.1. Traditional concept

Data localization or data residency law requires data about a nation's citizens or residents to be collected, processed, and/or stored inside the country, often before being transferred internationally. Such data is usually transferred only after meeting local privacy or data protection laws, such as giving the user notice of how the information will be used, and obtaining their consent. Data localization laws are often seen as protectionist. Consistent with the philosophy whereby trade barriers should be abolished within the EU but erected between the EU and other countries, the EU believes that data localization should be left to the EU to regulate at a pan-EU level, and member states' domestic data localization laws would violate European Union competition law. The EU's General Data Protection Regulation contains extensive regulation of data flow and storage, including restrictions on exporting personal data outside of the EU.

4.2.2. Data Localisation In India

Data localization laws are laws that require businesses to store data within a particular country. These laws are often implemented for security or privacy reasons. Data localization laws can have a significant impact on data control. For example, if a business is required to store data in India, it will not be able to transfer that data to another country without violating the law. This can make it difficult for businesses to operate internationally. In India, the Reserve Bank of India (RBI) has mandated data localization for payment system data, requiring the financial data of Indian customers to be stored only in India. Additionally, the Digital Personal Data Protection Act, 2023, includes provisions on data localization, empowering the Indian government to mandate localization of certain types of sensitive personal data for national security or strategic purposes. especially multinational corporations that handle vast amounts of data. Businesses may face increased compliance costs, operational complexities, and challenges in managing data across various jurisdictions while adhering to localization requirements.

5. DATA DECOLONIZATION IN THE INDIGENOUS COMMUNITY

Data decolonization refers to divesting from colonial, hegemonic models and epistemological frameworks that guide the collection, usage, and dissemination of data. This concept arose in the indigenous communities, prioritizing and centering Indigenous paradigms, frameworks, values, and data practices. Data decolonization is guided by the belief that data pertaining to Indigenous people should be owned and controlled by Indigenous people.

6. WOULD DATA OWNERSHIP AND LOCALISATION FURTHER THE CAUSE OF DATA DECOLONIZATION?

Data ownership and localisation may not further data decolonization as ownership, like a natural resource means that it can be traded and controlled. Though the resource is set to be used for the benefit of their citizens, misuse of natural resources has common precedent. Data ownership would place a price on data, similar to paying reparations for data and data locations would lead to fractured data sets in individual jurisdictions, similar to repatriation of data.

However, data ownership and data localization furthers the cause of data decolonization through the key aspect of control over data.

The assertion that data ownership and data localization contribute to the cause of data decolonization underscores a critical shift in power dynamics surrounding data control. Data ownership, a fundamental aspect of this strategy, enables communities to reclaim agency over the information they generate. By holding the rights to their own data, these communities gain the ability to dictate its usage, mitigating the risk of exploitation by external entities historically characterized as data colonizers. This facet of data decolonization is inherently tied to the principles of self-determination and autonomy, allowing communities to determine the narrative and utility of their data.

In parallel, the emphasis on data localization as a key driver in the pursuit of data decolonization aligns with the notion of safeguarding data within the geographical boundaries of the community that generates it. This strategy serves as a protective measure, reducing external influence and control over sensitive information. By localizing data, communities can curtail the potential for data exploitation and manipulation by external actors, further reinforcing their capacity to wield authority over their digital assets. In essence, the combination of data ownership and localization emerges as a potent approach in reshaping the dynamics of data control, empowering historically marginalized communities in their pursuit of data decolonization.

In conclusion, the twin pillars of data localization and ownership represent a potent pathway toward achieving data decolonization. Empowering communities with the control and rights over their own data not only aligns with the principles of autonomy and self-determination but also acts as a crucial countermeasure against historical imbalances in data dynamics. Through strategic localization, these communities can insulate themselves from external exploitation, reclaiming agency over their digital assets. As the world navigates the complexities of a data-driven era, prioritizing the principles of data ownership and localization emerges as a transformative force, fostering a more equitable and just landscape in the realm of information control and utilization.

REFERENCES

- Betts RF, ‘Decolonization: A Brief History of the Word’ in Els Bogaerts and Remco Raben (eds), *Beyond Empire and Nation* (Brill 2012)
- Chowdhury R, ‘From Black Pain to Rhodes Must Fall: A Rejectionist Perspective’ (2021) 170 Journal of Business Ethics 287
- Erin M, *The Culture Map: Decoding How People Think, Lead, and Get Things Done Across Cultures* (9th Edition, Hachette Book USA 2016)

- Hira S, *Decolonizing The Mind: A Guide to Decolonial Theory and Practice* (1st Edition, Uitgeverij Amrit/Amrit Publishers 2023)

- Ndlovu -Gatsheni Sabelo J., 'Perhaps Decoloniality Is the Answer? Critical Reflections on Development from a Decolonial Epistemic Perspective : Editorial' (2013) 43 Africanus 1

- Quinless JM, *Decolonizing Data: Unsettling Conversations about Social Research Methods* (University of Toronto Press 2021)

- Roberts JS and Montoya LN, 'Decolonisation, Global Data Law, and Indigenous Data Sovereignty'

- Smith LT, *Decolonizing Methodologies: Research and Indigenous Peoples* (3rd Edition, Bloomsbury Academic 2023)

- Srikrishna BN, 'A Free and Fair Digital Economy, Protecting Privacy, Empowering Indians-Committee of Experts under the Chairmanship of Justice B.N. Srikrishna'

- 'White Paper of the Commitee of Experts on a Data Protection Framework for India'

- Tharoor S, 'Saying Sorry to India: Reparations or Atonement' (Harvard International Law Journal)

- Thiong'o NW, *Decolonising the Mind: The Politics of Language in African Literature* (James Currey 1986)

- Webmaster, 'Misunderstandings between Repatriation and Reparations' (*National African American Reparations Commission (NAARC),* 13 May 2022)

- Digital Personal Data Protection Act 2023 (Act No 22 of 2023)

- Draft National E-Commerce Policy- India's Data for India's Development, 2019

- Regulation 2016/679/EU on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) 2016 (OJ L 119, 452016)

- Storage of Payment System Data

Bio:

Pratiksha Ashok is a Researcher for the 'Platform Regulation and Operations in the Sharing Economy' Project and a Ph.D. Student, Faculty of Law, UC Louvain, Belgium. pratiksha.ashok@uclouvain.be.

THE COMMUNITARIAN APPROACH AS A RESPONSE TO THE CHALLENGES OF MULTISTAKEHOLDERISM IN GLOBAL INSTITUTIONAL DECISION-MAKING PROCESSES IN INTERNET GOVERNANCE

Thobias Prado Moura

The digital age has ushered in unprecedented changes, with the Internet at the forefront of this transformation. It has become an integral part of our lives, shaping how we communicate, work, and access information. However, as the digital landscape continues to evolve, questions about its governance and the representation of diverse voices become increasingly important.[1]

In an era where digital technologies are rapidly reshaping the societal, economic, and political landscapes, the need for inclusive and equitable Internet Governance has never been more pressing.[2] How can we ensure inclusive and equitable approach? The answer lies in a paradigm shift towards a communitarian model in Internet Governance.

My research, titled "*Cantos na Lusofonia: a abordagem comunitária como resposta aos desafios do multissetorialismo nos processos institucionais de tomada de decisão global na Governança da Internet*," delves into this realm, proposing a paradigm shift towards a communitarian approach in Internet Governance. To address this, it is important to use a Digital Legal Studies lens. Digital Legal Studies is a dynamic field that confronts various challenges, such as defining common notions, addressing the political nature of digital regulations, and navigating the public-private divide in technology governance. My research addresses these challenges by proposing an approach that is sensitive to the nuances of digital harms, privacy concerns, and the socio-economic power of the Internet Governance.

Employing qualitative methods and a systematic literature review, the research aligns with Digital Legal Studies (DLS), offering a nuanced understanding of the interplay between law, technology,

[1] M. W. Datysgeld, "Understanding the role of States in Global Internet Governance: ICANN and the question of legitimacy" XII Annual GigaNet Symposium, Geneva, December 2017, 12.

[2] Fernando Filgueiras, Virgílio Almeida, "Governance for the Digital World: neither more state nor more market" [S.I]: Springer International Publishing, 2020, 13.

and society. It addresses DLS challenges such as defining digital concepts, the political aspects of digital regulations, and the public-private sector dynamics in technology governance. By proposing a revised, communitarian-based decision-making model, the research aims to foster more inclusive and equitable Internet Governance, reflecting the diverse global community's voices and interests. One of the fundamental challenges in DLS is navigating the political aspects of digital regulations.[3]

The Internet is not just a technical infrastructure; it is a global arena where political, economic, and social forces collide. The Internet operates as a multi-layered ecosystem, each layer playing a critical role in its functionality and impact on society.[4] At its core, the first layer is the technical infrastructure, encompassing the hardware that enables the Internet to function as a global network.[5] Above the technical layer, the second layer is the protocol layer, which encompasses the various communication protocols and standards that govern how data is transmitted and organized on the Internet. These protocols include HTTP (Hypertext Transfer Protocol) for web communication, SMTP (Simple Mail Transfer Protocol) for email, and TCP/IP (Transmission Control Protocol/Internet Protocol) for data transmission, among others.[6] The third layer, perhaps the most complex and dynamic, involves the political, economic, and social aspects of the Internet. This layer encompasses the governance structures, regulations, and policies that govern how the Internet is used and who benefits from it. Decisions made at this level impact critical issues such as free expression, privacy protection, and access to information.[7]

The interplay between various stakeholders, including governments, corporations, civil society, and users themselves, shapes the rules and norms governing the Internet. Decisions about Internet governance can have profound implications for issues such as free expression, privacy, and access

[3] Daniel F. Runde,; Sundar R Ramanujam, “Global Digital Governance: here′s what you need to know.”Here’s What You Need to Know. 2021. Disponível em: /https://www.csis.org/analysis/global-digital-governance-heres-what-you-need-know/ Accessed on 21 dec. 2023.
[4] Laura DeNardis, Mark Raymond, “Thinking Clearly about Multistakeholder Internet Governance” In: EIGHTH ANNUAL GIGANET SYMPOSIUM, 2013, Bali. Anais... Bali: [s.n.], 2013, 4.
[5] Ibid., 9.
[6] Ibid., 4.
[7] Ibid., 4.

to information. Therefore, understanding the political dimensions of digital regulations is essential to ensure that governance decisions are fair and just.[8]

At the core of Internet Governance lies the multistakeholder approach, which advocates for the participation of various sectors - government, private sector, civil society, and academia - in decision-making processes.[9] However, this approach, while groundbreaking, has shown limitations, especially in representing diverse community voices effectively.[10]

My research focuses on Lusophone countries - Brazil, Portugal, Mozambique, Angola, Guinea-Bissau, Cape Verde, and São Tomé and Príncipe - and key institutions like ICANN and LusNIC. Focusing on these countries and institutions like ICANN and LusNIC, the study evaluates the multistakeholder approach's effectiveness in representing diverse community voices. These countries, sharing a common linguistic and cultural heritage, provide a unique context for exploring the potential of the communitarian model in Internet Governance. It highlights the potential of a communitarian approach to balance individual and collective interests, enhancing the representativeness and inclusivity in digital policy-making.

The communitarian approach, central to my research, posits that community-based values and collective decision-making can enhance the inclusivity and representativeness of Internet Governance.[11] This approach seeks to balance individual interests with the collective good, ensuring that digital policies and regulations serve broader societal needs.

The goal of my research is to propose a revision of the multi-stakeholder decision-making approach. This revised approach, grounded in communitarian principles, aims to foster a more inclusive, representative, and equitable approach to Internet Governance. The journey towards a more equitable and inclusive digital future is complex and multifaceted. By integrating communitarian principles into Internet Governance, we can pave the way for an approach that truly reflects the diverse voices and interests of the global community. My research is a step towards

[8] ITU. Declaração de Princípios de Genebra. In: Documentos da Cúpula Mundial sobre a Sociedade da Informação: Genebra 2003 e Túnis 2005. Genebra: ITU, 2005. Traduzido por CGI.br/NIC.br, 16-20.

[9] Jovan Kurbalija, Eduardo Gelbstein, "Governança da Internet: Questões, atores e cisões. Tradução de Renato Aguiar" DiploFoundation, 2005, 13.

[10] Jovan Kurbalija, "Uma introdução à Governança da Internet. São Paulo: Comitê Gestor da Internet no Brasil", 2016, 219.

[11] Eleni Kanellopoilou, Nikolaos F. Ntounis, "Network Communitarianism as a tool for stakeholder engagement in places: The case of Rog Factory". In: Inclusive Placemaking - 4th Institute of Place Management International Conference. Manchester, UK, 7-8 set. 2017.

this vision, contributing to the field of Digital Legal Studies by offering innovative insights and practical solutions for the challenges of digital governance.

Bio:

Thobias Prado Moura is a PhD candidate at the Nova School of Law Lisbon.

UNDERSTANDING THE COMPLEX NATURE OF DATA FOR AN OPERATIONAL AND BALANCED EU REGULATION

Lola Montero Santos

SUMMARY: In this text I engage with the critical data literature strand, acknowledging its enriching insights but emphasizing the need for more actionable conclusions. My reflection addresses the necessity of balancing data openness and processing – including for economic value generation – with conflicting legal interests, and highlights the importance of understanding data (processing) biases as part of its quality assessment. Emphasizing the complexity of EU data regulation and its global implications, I advocate for the role of Digital Legal Studies and interdisciplinary collaborations to develop a comprehensive and applicable EU data regulation that safeguards fundamental rights and unlocks value creation.

I am a third-year PhD researcher at the European University Institute, in Florence. My work centres on EU data regulation, the digital economy, and their effects on society. These areas are core to Digital Legal Studies. Explicitly, my PhD evaluates EU data regulation within the context of value generation, exploring how data access, portability, and utilization obligations on private sector market actors contribute to innovation and economic development. It assesses the regulatory coherence of EU data regulation with the overarching EU policy goal of achieving a 'data utilization maximization framework' through the adoption of several new regulations, such as the Data Act . Within it, data is deemed necessary for innovation to take place, for improvements in existing products and services, for policies to be drafted more effectively, for government services to be better fitted for societal needs, and as input for the generation of AI systems.

This winter school has been extremely enriching for my research. I have been immersed in academic literature that both critiques and enhances the nuances surrounding various aspects of data (processing) conceptualization that are key to my work. This includes authors who focus on the shortcomings they identify in (big) data analysis and the limitations to the aims it can achieve; and who state that the economic focus of data regulation should be left aside, and is incompatible with existing areas of EU law.

I consider that while many of the reflections contained within this strand of the literature are enriching and thought-provoking, often its conclusions are not fully convincing, or they are not operationalizable (i.e. they lack explicit policy or regulatory actions which can be implemented to effectively change the aspects of EU data regulation that are criticized). This is effectively true if one considers the importance of preserving the competitiveness of the EU economy. For example, I understand the claim that data is not fully objective and can be used to discriminate, or further entrench traditional discrimination. However, this does not negate the value data holds both for economic growth and societal good. Data, in its unprocessed form, exhibits the economic properties of non-rivalry, heterogeneity, intangibility and scalability. A given data point can be employed many times by different entities simultaneously (non-rivalry); for many different ends (heterogeneity); be easily ported across borders (intangibility); and be combined with other data points, generating “recombinant data that possesses new and perhaps much greater economic value” (scalability). Data processing, which compiles “the process whereby information is extracted from the data generat[ing …] value”, can be used to create new goods and services, improve existing ones, and provide recommendations, insights, diagnoses and predictions. These aims can be achieved across many fields.

The importance of understanding where data comes from or the biases within it, should be considered as relevant metadata, essential for the assessment of its quality. I agree that these have so far not been given sufficient importance and that this must be corrected. Reconceptualising data quality traits and measurements is essential to decrease unintended biases or discrimination, and to understand the limitations to the conclusions which can be derived from a given data set. This can also increase the value-generating potential of data and the scope of positive aims it can be utilised for.

Moreover, I consider that there are circumstances where data openness and utilisation must be limited if they enter into conflict with other principles and objectives deserving (equal or greater) protection. In these cases, it will be necessary to make value judgements to determine the appropriate balance between the different protected legal interests. This can be best done through sector-specific regulations, setting clear hierarchical relationships between conflicting rights, and ad hoc mechanisms to set the greatest legal certainty for resolving future conflicts. Regarding conflicts of goals, the discussions, lectures, and informal conversations within this winter school have served me to further reflect on diverging goals. EU data regulation conveys a lot of complexity and the perspectives from which a single obligation can be analysed are ample. This reinforces the importance of interdisciplinarity collaborations. It is unattainable for a single individual or strand in the literature to explore this from all relevant angles. The stakes of properly tackling this task are essential, not only for the proper functioning of the European Single Market and the preservation of EU values, but also due to the likely effects these rules will have worldwide.

To conclude, I am convinced that understanding and incorporating the criticisms contained within critical data literature or data justice will improve the robustness of data regulation (and my PhD), and the contribution I hope to provide to this field. I hope my future work and the field of Digital Legal Studies serve to converge the different positions of the discussion, as I am convinced that the various camps, altogether, bring forth a more complete assessment. This is necessary to decrease the complexity of the regulatory environment and the different goals pursued by data regulation in the EU and beyond. I strive to foster a comprehensive and applicable EU regulation of data, that not only safeguards fundamental rights but also unlocks the untapped economic potential inherent within it.

Bio:

Lola Montero Santos is a Law PhD Researcher at the European University Institute. She investigates the coherence within the obligations on private market operators within EU data regulation and their influence on economic value generation. She holds an LLM from the College of Europe and a double degree in Law and Business Administration.

ALTERNATIVE PLATFORM REGIMES: STATE-LED PLATFORMIZATION IS A SOLUTION OR A THREAT?

Victo Silva

I investigate alternative platformization regimes. Until now, digital platforms have been automatically associated with private companies and initiatives. However, there is a growing movement to support public or state-owned platform models that offer alternatives to platform companies. However, there is still little understanding of how and when the state should participate in the platform economy. Even more worrying is the fact that the initiatives that are beginning to emerge (such as infrastructure platforms in Singapore, e-commerces developed by the Indian national government, urban mobility platforms developed by Barcelona City Council) do not take into account the risks associated with state platformization. When should a state platform be developed - and what should be the governance of the data that flows through this platform? The issue of data abuse, the vulnerabilities of individuals using digital platforms, and the neglect or disrespect of public values by platform companies, take on a new configuration when we consider platforms developed and owned by the state. We need to raise these same questions - and more - so that this alternative regime benefits society, rather than further deepening the power asymmetries between platform controllers and individuals. The winter school touched on points that are crucial and transversal to any ownership regime for digital platforms: privacy and freedom of expression, the contextual definition of what it means to be vulnerable in online environments, the difficulty of transforming Big Tech politics through regulation. These points foreshadow problems or issues that will also arise in alternative regimes, when national or sub-national states, for different reasons, increasingly intervene in the platform economy. Should different safeguards be put in place? Or is the legal system that protects individuals from platform companies enough to protect them from the new state platforms that emerge? Will we see more transparency or even more opacity in the way personal data is handled? Although this alternative regime appears to be hoping to bring more balance to the markets, alternatives for consumers and alignment between the architecture of the platforms and public values, there are also worrying signs that it could bring power plans from the states that control these platforms. We need to think about effective ways of ensuring that, as J Muldoon says in his latest book, we don't replace corporate domination with distant or despotic bureaucrats. To avoid this, there is a lot of work that digital legal studies must undertake.

Public infrastructure or misuse of the State?

One of the manifestations of this alternative platformization regime is the creation of commercial digital platforms by government entities that compete with private alternatives. Observing two cases, one in Brazil and the other in India, are quite illustrative of how the border between public and private in the platform economy will be disputed in the legal sphere. The Indian government supported the formation of an urban mobility (ride-hailing) platform called ‘Namma Yatri’ (https://nammayatri.in/). The platform follows the same model as Uber: it connects passengers with drivers for short trips. The difference is that workers keep the entire amount paid by passengers, substantially increasing their income when compared to the private alternative. After a year and a half of its launch, and operating in five cities in India, the platform has already recorded more than 22 million trips and more than 40 million dollars in income for drivers. In Brazil, a similar initiative was launched by the city of Rio de Janeiro. The ‘Valeu’ app seeks to offer an alternative to private food delivery platforms. It also aimed to increase drivers' income, as it did not charge commissions. However, councilors from the city of Rio de Janeiro took legal action against ‘Valeu’, alleging that it was a public initiative that competed with private initiatives without adequate justification, therefore constituting misuse of the State. This is just one example that demonstrates the complex and varied new institutionality that must be put in place to legitimize or not alternative platform regimes. This example also shows that similar solutions will be more or less well received in different places, due to the constituencies and stakeholders affected by the new platformization regimes. Finally, these examples bring up another worrying point: is this alternative model really that alternative, if it just mirrors the private platformization model but slightly increases workers' income? What about transparency, openness of data, participation in the architecture, and governance of platforms? Despite that, it shows that there is a world of possibilities ahead and the law will be one of the pillars responsible for building it - hopefully in a way that amplifies the well-being and protection of individuals around the world.

Bio:

Victo Silva is an economist specializing in innovation economics, with a focus on digital technologies, especially digital platforms and AI. He explores the dynamics of digital innovation and alternative models for deploying these technologies for socio-economic development. He is currently a postdoctoral fellow at iHub, Radboud University, Nijmegen.

HOW TO THINK ABOUT EQUITY IN THE AI FIELD?

Monique Munarini

SUMMARY: In this text I engage with the critical data literature strand, acknowledging its enriching insights but emphasizing the need for more actionable conclusions. My reflection addresses the necessity of balancing data openness and processing – including for economic value generation – with conflicting legal interests, and highlights the importance of understanding data (processing) biases as part of its quality assessment. Emphasizing the complexity of EU data regulation and its global implications, I advocate for the role of Digital Legal Studies and interdisciplinary collaborations to develop a comprehensive and applicable EU data regulation that safeguards fundamental rights and unlocks value creation.

The intensive use of tools based on artificial intelligence to make the decision-making process more agile has brought numerous benefits and risks.[12] There are many examples where people involved in the development of these tools failed in ensuring that their AI systems would not violate ethical and legal principles. One of the most famous cases was the AI system developed by Amazon to screen candidates' resumes that started to eliminate women's resumes after it was trained with mostly male resumes. When the risks hit the headlines,[13] it became essential to seek regulation of this technology so that human control could be ensured and risks mitigated. This regulation began with the development of ethical principles to guide the development and use of these systems.[14] Faced with the lack of binding character of these frameworks, a race began between governments to establish a standard of legislation that would be replicated around the world.[15] In parallel, while nations are still in the process of developing binding AI-related laws, there has been a proliferation of methodologies to ensure the responsible creation and use of AI.[16][17] There are now many auditing and risk assessment methodologies that promise to ensure the

[12] Vinuesa, R., Azizpour, H., Leite, I. *et al.* (2020). The role of artificial intelligence in achieving the Sustainable Development Goals. *Nat Commun* 11, 233

[13] Dastin, J. (2018). Amazon scraps secret AI recruiting tool that showed bias against women: https://www.reuters.com/article/idUSKCN1MK0AG/.

[14] Hagendorff, T., (2020). The Ethics of AI Ethics: An Evaluation of Guidelines. *Minds and Machines* 30, no. 1 (1 March 2020): 99–120.

[15] Cath C. (2018). Governing artificial intelligence: ethical, legal and technical opportunities and challenges. *Philosophical transactions. Series A, Mathematical, physical, and engineering sciences*, *376*(2133).

[16] Ada Lovelace Institute. (2021). Technical methods for the regulatory inspection of algorithmic systems in social media platforms, accessed on <https://www.adalovelaceinstitute.org/report/ technical-methods-regulatory-inspection>.

[17] Eticas (2023). Adversarial Algorithmic Auditing Guide. Association Eticas Research and Innovation.

effectiveness of AI and the absence of harm. Many of the possible violations of fundamental rights involve the existence of bias.[18] However, it has already been shown that a systematic approach is needed to tackle problems involving bias from a social-technical perspective.[19] To this end, we tend to seek to operationalise ethical principles to guide this process.[20] One of the principles most associated with protection against discrimination and the quest for equality is fairness. However, each branch of knowledge in AI has different conceptions of what this principle is and how to operationalise it.[21] This creates a tendency for many of these methodologies to tackle problems related to bias from just one perspective, while recognising the need for a systematic view.

The use of artificial intelligence impacts society, but the solutions to these problems are sought in the artificial intelligence lifecycle itself. Thus, we scan the possible sources of problems in data and algorithms, how to solve them from this perspective and justify the solution through principles and societal values so that we can say that the goal is a "trustworthy" artificial intelligence.

For systematic work in monitoring artificial intelligence, it is essential to use ethical values built from a multidisciplinary perspective that is easily understood by all those involved.[22] In this landscape, the integration of equity into auditing mechanisms emerges as a key strategy to enhance the reliability of AI systems. As we grapple with the multidisciplinary nature of AI, where individuals from diverse backgrounds collaborate to achieve common goals, establishing agreed-upon definitions becomes a formidable challenge. The lack of consensus on what constitutes AI and equity further complicates regulatory efforts. It is within this complex terrain that the Digital Legal Studies Lab plays a crucial role.

The Digital Legal Studies Lab seeks to unravel the regulatory paradigm shift induced by AI, offering insights into how to shape regulation that are aligned with ethical values such as equity and promote fundamental rights compliance. Understanding equity as a concept within the diverse

[18] Crawford, K. (2021). *The Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence*. Yale University Press.

[19] Coeckelbergh, M., (2019), Artificial Intelligence: some ethical issues and regulatory challenges, *Technology and regulation*, 31–34.

[20] AI Ethics Impact Group. (2020). From principles to practice—An interdisciplinary framework to operationalise AI ethics. AI Ethics Impact Group, VDE Association for Electrical Electronic & Information Technologies e.V., Bertelsmann Stiftung, 1–56.

[21] Niels van Berkel, Sarsenbayeva, Z., Goncalves, J. (2023). The methodology of studying fairness perceptions in Artificial Intelligence: Contrasting CHI and FAccT, *International Journal of Human-Computer Studies*, V. 170.

[22] Prabhakaran, V., Mitchell, M., Gebru, T., Gabriel, I. (2022). A human rights-based approach to responsible AI, in *2022 ACM Conference on Equity and Access in Algorithms, Mechanisms, and Optimization or (EAAMO '22)*.

fields of the AI ecosystem is paramount for the effective governance of this technology. The lab's focus on the synergy between digital technologies, AI, and fundamental rights acknowledges the intricate relationship between these elements. The Digital Legal Studies Lab opens up a dialogue on the necessity for more transdisciplinary research and the active involvement of diverse communities in shaping AI governance, as remarked in the Winter School on Data, Personalisation and the Law. The challenges of regulating AI necessitate collaboration across disciplines to foster a comprehensive understanding of its implications. The lab's emphasis on active community participation reflects the recognition that diverse voices are essential for achieving positive results in AI governance.

As we navigate the ethical horizon of AI, the role of equity in auditing mechanisms becomes increasingly crucial. Auditing ensures accountability and transparency, serving as a check against biases and unfair practices embedded in AI systems.[23] By integrating equity into auditing processes, we can identify and rectify potential biases, thereby enhancing the overall reliability of AI technologies. However, the path to equitable AI auditing is fraught with challenges. The multidisciplinary nature of AI demands a convergence of perspectives from computer science, ethics, law, and various other fields. Establishing a common language and framework for assessing equity in AI proves to be a formidable task.

This article proposes to look at equity from an alternative vision that can be operationalised by various branches of knowledge, mainly legal, ethical and technical. This is only possible because the proposed definition can be found in each of these branches, but is not based exclusively on them. Moreover, some of the problems identified in the operationalisation of ethical principles derived from traditional philosophy, such as the Theory of Justice from John Rawls or fairness from Aristotle involved the attempts to translate them in legal articles that prescribe conducts or in numerical metrics that ended up representing just an hegemonic perspective that was not inclusive, therefore leaving social issues that were "inherited" by AI systems unsolved.[24] The idea

[23] Mökander, J., & Floridi, L. (2021). Ethics-based auditing to develop trustworthy AI. *Minds & Machines, 31*, 323–327.

[24] Ibid, 120.

of this article was to look at how society has defined equity over time and to extract common elements that can create a definition that can be applied in the most diverse environments.

The discussion about equitable outcomes is very strong in the educational field from philosophy of education,[25] computer science[26] to policy making.[27] Equity is always surrounded by ideas of diversity, belonging and inclusivity. It is not possible to disentangle inclusion and intersectionality from the feminist thinking. Beauvoir[28][29] and Lorde[30] also worked on the notion of leaving no one behind and assessing what are the tools that need to be available that can empower a whole community and not only the dominant perspective. In the legal field, equity is again related to the same notions in emerging research on legal design and design justice.[31][32] There are groups working on equity from a computer science perspective with the goal to uphold marginalised groups and bring them to datasets used to create AI systems without sacrificing performance.[33][34] From all these variable sources, equity can be understood as giving to the ones who need the necessary tools to belong in a particular community. This definition itself already shows that equity cannot be operationalised from just one perspective as the sense of belonging cannot be quantified in metrics, but tools to this end, needs to be a practical action. In the same way, thinking of the groups in need needs a social and legal analysis to build systems that are aligned with the preservation of fundamental rights.

In conclusion, as AI continues to shape our future, it is imperative to address the ethical and equity considerations embedded in its development and deployment. The Digital Legal Studies Lab plays a pivotal role in this endeavour, providing valuable insights into the regulatory paradigm shift

[25] Freire, P. (1997). Direitos humanos e educação libertadora: gestão democrática da educação pública na cidade de São Paulo. Paz e Terra.

[26] Chang, M.A. & Roschelle, J. (2023). Ethics and Equity in AI for Collaborative Learning. Communications of the ACM.

[27] Fengchun, M., Wayne, H., Giannini, S., Tawil, S., (2023). Guidance on generative AI in education and research. UNESCO. https://unesdoc.unesco.org/ark:/48223/pf0000386693.

[28] Beauvoir, S., (1945). *Les bouches inutiles*. Gallimard.

[29] ________, (1949). The Second Sex. Parshley.

[30] Lorde, A., (2019). Sister outsider: Essays and Speeches. England: Penguin Books, 166.

[31] Titi, C., (2021) . The Function of Equity in International Law. Oxford University Press.

[32] Costanza-Chock, S., (2020). Design Justice: Community-led Practices to Build the Worlds We Need. Cambridge, Massachusetts, The MIT Press.

[33] Katell, M., Young, M., Dailey, D., Herman, B., Guetler, V., Tam, A., Bintz, C., Raz, D., & Krafft, P. M. (2020). Toward situated interventions for algorithmic equity: Lessons from the field. *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency*, 45–55.

[34] Queer in AI. (2023). Queer in AI: A Case Study in Community-Led Participatory AI. *Proceedings of the 2023 Conference on Fairness, Accountability, and Transparency*, 1882-1895.

induced by AI. By promoting transdisciplinary research, the lab contributes to the ongoing dialogue surrounding AI governance. As we strive to harness the transformative potential of AI, it is essential to develop frameworks that uphold ethical principles, safeguards human rights, and ensures the equitable deployment of AI technologies for the benefit of all.

Bio:

Monique Munarini is a Brazilian qualified lawyer. PhD candidate in the Italian National PhD in AI at the University of Pisa. MA in Human Rights and Multi-level Governance at the University of Padova, and LLM in Law, Economics, and Management at the University of Grenoble-Alpes. Available at: monique.munarini[at]phd.unipi.it.

DATA AND CONTENT IN THE DIGITAL WORLD: REVISITING PROPORTIONALITY IN THE EU LEGAL ORDER

Spyros Syrrakos

SUMMARY: The boundaries between the offline and online dimensions have been blurred due to the disruptive digitalisation of our societies. The data power of digital platforms enables them to exert decisive influence on digital content and to shape the digital architecture through contractual relationships. The plurality of conflicts among multiple fundamental rights and interests in the online space exemplifies the importance of proportionality, which has assumed a prominent, albeit contestable place in the modern legal discourse. The 'polycentric' nature of proportionality, and the distinct challenges of the digital space create lead to crucial questions for effective digital regulation, and the future of fundamental rights within the EU constitutional order.

Setting the Scene

Data constitute the bedrock of the modern digital society, catalysing innovative forms of digital content and new business models. The online space creates distinct challenges[35] tied with the global reach and transnational nature of the internet. Information can be disseminated at an exponential rate, transcending geographical borders. Across the constantly evolving digital landscape, the critical role of digital platforms has disrupted the traditional power relationship between the state and individuals. Digital platforms are not mere conduits anymore – they possess a systemic role by shaping the selection of online content on the basis of their data power,[36] as well as the rules for dissemination and access on behalf of online users.[37] The democratisation of content through technology should be recognised as an empowering driver for the exercise of the freedom of expression, however it has also given rise to major challenges, notably the dissemination of illegal content and the wide sharing of copyrighted works, in particular. Crucially,

[35] See also Chris Reed, 'Online and Offline Equivalence: Aspiration and Achievement' (2010) 18 International Journal of Law and Information Technology, 248, 258.

[36] Orla Lynskey, 'Grappling with "Data Power": Normative Nudges from Data Protection and Privacy' (2019) 20 Theoretical Inquiries Law, 189.

[37] Jack Balkin, 'Free Speech is a Triangle' (2018) 118 Columbia Law Review 2011. See also on the privatisation of the online public sphere Tarleton Gillespie, *Custodians of the Internet* (Yale University Press 2018). The power of digital platforms in the algorithmic society is a central tenet of the framework defined by certain scholars as 'digital constitutionalism', see Giovanni de Gregorio, *Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society* (CUP 2022); Edoardo Celeste, *Digital Constitutionalism* (Routledge 2022); Oreste Pollicino, *Judicial Protection of Fundamental Rights on the Internet: A Road Towards Digital Constitutionalism?* (Hart Publishing 2021).

the internet facilitates the simultaneous interaction among millions of users via digital intermediaries, however this multi-sided interaction amplifies possible conflicts among several fundamental rights and interests in horizontal settings. The protection of EU fundamental rights in the digital society, as well as the preservation of public values and the rule of law more broadly have been placed at the heart of the policy and legal discourse around digital regulation. The EU fundamental rights normative starting point and the challenges of the digital space, primarily in relation to the plurality of fundamental rights conflicts, brings to the fore the polycentric role of proportionality in the digital space. Proportionality lays down the conditions for the legitimate conduct of public bodies and the judicial adjudication of conflicts between rights and interests, constituting 'one of the defining features of global constitutionalism'.[38] Advocates of proportionality highlight its structured apparatus in guiding judicial reasoning amid convoluted legal quandaries in search of constitutional legitimacy,[39] whereas those who critique proportionality contend that proportionality is a façade for unconstrained judicial discretion due to its abstract and subjective nature and the inexorable difficulty of balancing incommensurable values.

PhD Project

My PhD project aims to delve into the intricacies of proportionality in the online context within the EU legal order, and to examine whether the traditional view of proportionality should be revisited in the light of the digital challenges. 'Data' and 'content' constitute the two substantive pillars of the PhD project, since data, positioned at the core of the platform ecosystem, cannot be viewed in isolation from digital content, and, in a way, constitute two sides of the same coin. The challenges of proportionality are being examined on the basis of two distinct, yet closely linked lenses which best reflect the challenges of the 'data' and 'content' anchors: data protection, and freedom of expression. A systematic analysis of this interplay remains largely incipient. Academic attention has been dedicated to specific elements of proportionality in data protection,[40] intellectual

[38] Alec Stone Sweet and Jud Mathews, 'Proportionality Balancing and Global Constitutionalism' 47 Columbia Journal of Transnational Law, 73, 75.

[39] For instance Kai Möller, *The global model of constitutional rights* (OUP 2012), 179.

[40] See notably Lorenzo Dalla Corte, 'On Proportionality in the Data Protection Jurisprudence of the CJEU' (2022) 12 International Data Privacy Law 259. Other valuable contributions on the matter: Janneke Gerards, 'The age of balancing revisited? (2020) 1 EDPL 13; Audrey Guinchard, 'Taking proportionality seriously: The use of contextual integrity for a more informed and transparent analysis in EU data protection law' (2018) 24 European Law Journal 434; Bart van der Sloot, 'The practical and theoretical problems with balancing: *Delfi, Coty* and the redundancy of the

property,[41] and platform regulation,[42] however this *ad hoc* analysis, usually in response to a certain ruling issued by the Court of Justice of the European Union ('CJEU'), leads to a fragmented understanding, and does not necessarily reflect the wider and abstract claims made on that basis. The main questions my PhD project aims to answer are the following: to what extent is the prominent recourse to fundamental rights proportionality used in the digital field as a judicial self-empowerment vehicle and a constitutionalisation instrument furthering EU integration in the harmonisation process? Has the CJEU assumed the role of digital regulator by 'failing to take into account all relevant considerations',[43] and is its proportionality reasoning lacking coherence in shaping the legislative content of the EU fundamental rights at stake?

The field of Digital Legal Studies constitutes an interdisciplinary frame which enable us to critically explore and understand the complex relationship between law, regulation, and digital technologies. My PhD project aims at providing a valuable contribution towards the objectives of the field of Digital Legal Studies by exploring the role of proportionality within the wider EU constitutional context in relation to the regulation of the digital space. The originality of this contribution lies in the critical exploration of the interaction between proportionality, data protection and freedom of expression in the online context, on the basis of different strands of literature (IT law, constitutional rights, EU law literatures), and primarily driven by an empirical analysis of the CJEU jurisprudence in these fields. Bringing together the proportionality approaches in the areas of data protection and freedom of expression allows us to gain more clarity on the expansion of fundamental rights proportionality analysis in the online context, and to grasp

human rights framework' (2016) 23 MJ 439; Charlotte Bagger Tranberg, 'Proportionality and data protection in the case law of the European Court of Justice' (2011) 1 IDPL 239. The need for further academic research has been underscored by D Kloza and L Drechsler, 'Proportionality has come to the GDPR' (09 December 2020), *European Law Blog,* at <https://europeanlawblog.eu/2020/12/09/proportionality-has-come-to-the-gdpr/> accessed 10 October 2022.

[41] Notably Tuomas Mylly, 'Regulating with rights proportionality? Copyright, fundamental rights and internet in the case law of the Court of Justice of the European Union' in Oreste Pollicino, Giovanni Maria Riccio and Marco Bassini (eds) *Copyright and Fundamental Rights in the Digital Age* (2020, Elgar) 54; Tuomas Mylly 'Proportionality in the CJEU's Internet Copyright Case Law: Invasive or Resilient?' in Ulf Bernitz, Xavier Groussot, Jaan Paju, Sybe A. de Vries (eds) *General Principles of EU Law and the EU Digital Order* (Kluwer 2020); Martin Husovec, 'Intellectual Property Rights and Integration by Conflict: The Past, Present and Future' (2016) 18 Cambridge Yearbook of European Legal Studies, 239.

[42] Notably Evelyn Douek, 'Governing Online Speech: From "Posts-as-Trumps" to Proportionality and Probability' 121 Columbia Law Review 759; Enguerrand Marique and Yseult Marique, 'Sanctions on digital platforms: Balancing proportionality in a modern public square' (2020) 36 Computer Law & Security Review 105372.

[43] Kai Möller, 'Proportionality: Challenging the critics' (2012) 10 International Journal of Constitutional Law, 709.

a more holistic understanding of the interplay between proportionality and EU fundamental rights in the digital space.

Bio:

Spyros Syrrakos is a PhD candidate at the LSE Law School. His research interests concern all aspects of EU law, as well as the effective protection of digital rights. Spyros is a qualified lawyer, with experience in the field of EU technology policy within the European Commission in Brussels and Luxembourg.

ONCE BITTEN, TWICE SHY: LEARNING FROM CRITICISMS ON FAIRNESS WHEN DEVELOPING METRICS FOR DIVERSITY

Sanne Vrijenhoek

News recommender systems are machine learning systems that suggest news articles a reader might be interested in reading next. As such, they influence what news gets exposed to the public, and thus public discourse and eventually democracy.[44] In doing so, they are taking over the traditionally editorial task of determining which articles get exposure, and which do not. During the winter school, I sought to expand my knowledge on relevant regulatory frameworks around algorithms, media and platforms, and how technology and algorithms can(not) effectively inform policy.

Currently the standard approach for news recommender systems is to predict which articles a user might want to engage with based on which articles they have interacted with before and/or the interactions of other people. This is stark opposition to the norms and guidelines human editors follow, and is suspected to induce filter bubbles and selective exposure.[45] Theoretically, news media organizations could also take a more normative approach and deploy algorithms that allow readers to find the news that expands their horizons, rather than propagating sensationalist content that readers might be inclined to click on, but which won't help them in the long term. The challenge, however, lies in determining *what* the normative criteria to evaluate news recommender systems on are, if not engagement and prediction accuracy. Normative goals are often quite abstract, and may even be contradictory; we may want to foster tolerance and empathy, have a fair and unbiased overview of the public debate, or inspire readers to take action against existing injustices.[46] This makes it hard to translate normative goals into something measurable, preferably a value between 0 and 1, which is necessary for an algorithm. Doing so is a challenge that cannot be resolved by computer scientists alone. In previous work, we have started the construction of so-called *diversity metrics*, inspired by media scholars' conception of the term, which could

[44] Neil Thurman, Judith Moeller, Natali Helberger and Damian Trilling, 'My Friends, Editors, Algorithms, and I' (2019) 7(4) Digital Journalism 447 ⟨https://doi.org/10.1080/21670811.2018. 1493936⟩; Sanne Vrijenhoek, 'Do you MIND? Reflections on the MIND dataset for research on diversity in news recommendations' (2023) arXiv preprint arXiv:2304.08253.

[45] Lien Michiels and others, 'How Should We Measure Filter Bubbles? A Regression Model and Evidence for Online News' (2023), 640.

[46] Natali Helberger, 'On the democratic role of news recommenders' (2021), 14.

eventually inform recommender systems.[47] However, even with these metrics a range of questions remain current. Can and should news recommender systems be regulated? How does this relate to media freedom? What would an effective policy look like? How and where can the metrics we developed provide the information necessary for policy-making and enforcement, and where should we rely on more procedural approaches?

The Winter School touched upon these subjects in several ways. Lotje van Beek, from Bits of Freedom, warned of the dangers of misinformation, and the stakes large corporations have in keeping it in place. Professor Natali Helberger spoke about the onset of generative AI, and how the big tech companies are put in the position of safeguarding our public values. The workshop "Towards data justice: ethical paths through a datafied world", hosted by Linnet Taylor, stood out to me in particular. While the talk was not directly about the media or diversity, it provided many insights on the effects and success of another 'beyond accuracy' metric: fairness. Professor Taylor argued that fairness, with its focus on statistical parity or, in the best cases, on notions of equity and/or equality, had become a mere tool for large companies to self-regulate and provide validity to otherwise self-serving practices.[48] She argued for the emergence of 'macroethics': instead of asking how a particular system should be behave, we should focus on what that particular system will have for an effect on the world, and to what future it may lead.

This debate is relevant to our work on diversity metrics in several ways. Similar to fairness, the diversity metrics aim to translate a complex social concept into a number, and as such are at risk of losing important nuance. Furthermore, without proper checks and procedures in place, they may prove to be a tool for 'ethicswashing': a company may claim good diversity scores, whilst the metrics in practice do not measure what they aim to measure.[49]

After hearing this talk, I aim to do a more in-depth analysis of the criticisms against fairness, and with those take a critical look at how and why they also apply on our metrics for diversity. I will argue where concerns are and are not valid and, if possible, propose potential mitigation strategies.

[47] Sanne Vrijenhoek and others, 'Recommenders with a mission: assessing diversity in news recommendations' [2021] 173; Sanne Vrijenhoek and others, 'RADio–Rank-Aware Divergence Metrics to Measure Normative Diversity in News Recommendations' (2022), 208.

[48] Linnet Taylor and Lina Dencik, 'Constructing commercial data ethics' (2020) 2020 Technology and Regulation 1; Reuben Binns and others, ''It's Reducing a Human Being to a Percentage' Perceptions of Justice in Algorithmic Decisions' (2018), 1.

[49] Os Keyes, Jevan Hutson, and Meredith Durbin, 'A mulching proposal: Analysing and improving an algorithmic system for turning the elderly into high-nutrient slurry' (2019), 1.

This will be a great opportunity to reflect on the work that has been done over the past years, and allow me to identify concrete steps that still need to be taken before adoption of the diversity metrics, and perhaps in the far future regulation based on them, becomes possible.

Bio:

Sanne Vrijenhoek is a PhD researcher at the University of Amsterdam.

DIGITAL PLATFORM'S LIABILITY

Adam Feher

SUMMARY: New regulations are emerging to address the increase of illegal content on online platforms, highlighted by initiatives like the Digital Services Act. his paper presents a theoretical model examining how such regulations shift the economic incentives for social media platforms to moderate user-generated content. A key issue is platforms' strategic use of their technological advantage in detecting offenses, leading to practices like cherry-picking, where they selectively enforce rules to appear compliant. To combat cherry-picking, the regulator may enhance its technology to monitor more content and adjust fines based on the ex-post observable relative types of users. Intriguingly, under this approach, the optimal fine might be reduced when more users commit violations.

The economic and societal relevance of online platforms has been on the rise. Platforms like Facebook, Twitter, and YouTube have attained immense popularity. According to Cook [2023] more than 5 billion YouTube videos are viewed daily, and Twitter publishes over 500 million tweets posted each day as of December 2023.[50] However, hosting platforms also contribute to disseminating illegal material, such as hate speech on social media platforms or copyright violations on media platforms. In response, today's online intermediaries regulate users' access to platforms and police their behavior and expression on their platforms. Despite their efforts,[51] the public pressure is mounting on platforms to do more to combat offenses committed under their supervision and on regulators to force platforms to police [Buiten et al, 2020]. The Directive on electronic commerce in the European Union and Section 230 in the United States Communications Decency Act granted immunity to online platforms with respect to third-party content for the past 20 years. The German Network Enforcement Act (Netzwerkdurchsetzungsgesetz) was enacted in 2018. Moreover, the Digital Services and Markets Act in Europe, the online safety bill in the UK [52], and a heated policy debate on reform and court cases in the US indicate an increased liability platforms are facing.[53]

[50] The daily number of tweets is reported by worldometers.info.

[51] In 2019, Facebook CEO Mark Zuckerberg declared that they would be allocating 5\% of the firm revenues, 3.7 billion, on content moderation (Roettgers [2019]).

[52] https://bills.parliament.uk/bills/3137.

[53] See, for example, the court cases and rulings of Bolger v. Amazon, Loomis v. Amazon, and Reed [2023] for legislative changes.

A fundamental question is how a regulator can enforce social media platforms' liability for offenses committed by platform users. The key friction is that the platform has a technological advantage over the regulator in detecting offenses and may strategically use it to circumvent regulatory objectives. The theoretical model introduces a novel aspect wherein the platform engages in cherry-picking, to opportunistically punish select users on the platform.[54] The platform's aim is to create an illusion of compliance with regulatory standards and avoid sanctions. By selectively punishing certain users, the platform reduces the likelihood of the regulator discovering violations and subsequently penalizing the platform. Cherry-picking is particularly harmful if the platform provides preferential treatment to users with large audiences whose contributions to the platform's profit are the largest, but whose offenses can cause the greatest societal damage. A key example of the phenomenon depicted by the model is Twitch's "do-not-ban-list." This list reveals that top streamers were given special treatment when it came to suspending their streaming account [Greyson, 2021].

Regulations that do not take cherry-picking into account can actually incentivize this behavior and decrease social welfare. To prevent cherry-picking, the regulator can implement a mechanism where the size of the fine depends on how the platform handles violations by users with small audiences compared to users with large audiences. The optimal schedule for sanctions can be nonmonotonic in the offenses the regulator discovers on the platform. Specifically, the sanction may be higher when the regulator discovers fewer violations on the platform. The reason is that from the regulator's point of view, there are two punishable actions: the offense by the user and the cherry-picking by the platform.

The second question explores whether liability for offenses committed by the agent, such as spreading misinformation, should rest with the platform or the user, and whether enforcement should be undertaken by a private or public entity. The model builds on an early study by Polinsky [1980]. The primary tradeoff lies in the fact that users, who can modify content ex ante, are more easily deterred, while platforms can only act ex post by removing content. However, holding the platform liable incentivizes the platform to invest in moderation technology. Early results indicate that assigning liability to users results in higher social welfare provided the platform has sufficient

[54] The idea that under certain liability regimes platforms may cherry-pick on what to remove (because risky) and what to maintain (because generating substantial revenues) first appears in Lefouili and Madio [2022].

intrinsic incentives to invest in content moderation without being liable. Nonetheless, regardless of the chosen regime, private enforcement consistently leads to underenforcement.

References

Y. Lefouili and L. Madio. The economics of platform liability, volume 53. Springer US, 2022. ISBN 0123456789. doi: 10.1007/s10657-022-09728-7. URL https://doi.org/10.1007/s10657-022-09728-7.

B. Reed. Biden tech advisor : Hold social media companies accountable for what their users post. pages 1–7, 2023. URL: https://www.cnbc.com/2020/12/02/biden-advisor-bruce-reed-hints-that-section-230-needs-reform.html

J. Roettgers. Mark Zuckerberg Says Facebook Will Spend More Than 3.7 Billion on Safety ,Security in 2019. URL https://variety.com/2019/digital/news/facebook-2019-safety-speding-1203128797/

A. M. Polinsky. Private versus Public Enforcement of Fines A. The Journal of Legal Studies, 9(1):105–127, 1980

Bio:

Adam Feher is a PhD candidate at the University of Amsterdam at the Amsterdam Center for Law and Economics, is currently a researcher at Trier University and the Institute for Labour Law and Industrial Relations in the European Union. His general research interest lies in the intersection of law and economics, with a current focus on topics related to digital platforms.

NAVIGATING THE MINEFIELD OF THE EU'S APPROACH TO REGULATING DIGITAL HATE SPEECH: WHAT IS REALLY AT STAKE?

Stevi Kitsou

Hate speech is a phenomenon of legal relevance, marked by conceptual vagueness and obscurity. There is a missing consensus on its conceptualisation. This missing harmonised definition leads to States, institutions, and researchers interpreting it through the lens of their own legal traditions and philosophical orientations. This context begs a critical question: how do we regulate a phenomenon that defies clear definition?

This question goes beyond a mere academic discussion. It acquires vital and practical significance for the victims of hate speech in instances where speech, though not classified as 'illegal' (criminal), is nevertheless harmful. This latter communication does not meet the necessary threshold for legal action, yet it still undermines the human dignity of victims and challenges the core fundamental values of the EU.

The purpose here is not to answer the critical question. It is, however, to point out to the difficulties and obstacles that stand in the way of reaching a consensus in the EU, as well as they link to broader societal and legal issues. I highlight, first, that a main obstacle is the EU's intricate identity, combining an amalgam of national cultural and legal experiences. I, then, zoom in to the digital landscape, signalling the concrete steps taken towards common regulatory approach to the phenomenon with the DSA.

THE CHALLENGE BEHIND EU'S DEVELOPING APPROACH TO COMBATING HATE SPEECH

In this context, the EU too joins the effort to define, regulate, and combat hate speech. This effort reflects its long-standing commitment[55] to address inequalities and intolerance, which is at the core

[55] Key developments include indicatively joint declarations in the 1980s, non-binding Council resolutions in the 1990s, the establishment of the European Monitoring Centre on Racism and Xenophobia in 1997, the adoption of binding legislation such as the Council Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law, the Code of Conduct on Countering Illegal Hate Speech Online, and more recently the Commission's proposal for the extension of the list of EU crimes to hate speech and hate crime based on Article 83(1) of the TFEU. The initiative runs in parallel to and in support of the EU anti-racism Action Plan, the EU Gender Equality Strategy 2020- 2025 addressing among other forms of gender-based violence, misogynous and sexist hate speech; and the LGBTIQ Equality Strategy 2020-2025 that seeks to target hate speech against the LGBTIQ people and community, thus highlighting the other grounds of immutable characteristics apart from the ones laid down in the Framework Decision. The initiative is also

of an ‘ever closer Union’.[56] However, the EU’s effort is equally challenged by its own intricate identity and architecture. Though an ‘ever closer Union’, the EU is still shaped by its Member States’ diverse historical experiences and constitutional traditions, which together create a mosaic of perceptions on fundamental values[57]. This diversity in turn influences the understanding of what constitutes hate speech. Then, once again, even in the EU, the subsisting question remains how to move towards a unified understanding of hate speech?

Given its damaging effects on individuals and the EU’s core principles, the necessity for a harmonised approach stands out clearly. The success of an EU-wide strategy largely depends on the extent to which Member States' values can strongly and uniformly be aligned in practice. This is inherently tied to the EU’s legitimacy to tackle hatred and upholding fundamental rights and the rule of law. Thus, the main concern stretches beyond hate speech alone, becoming a question of how united the EU and, implicitly its Member States, stand around core values. Considering the growing global digitalisation, this question is even more salient.

Hate Speech in the Digital Era

The shift to digitalisation has significantly altered how hate speech online is regulated. This change is due to the Internet's cross-border and rapidly evolving nature and the varying levels of fundamental rights protections among Member States. This stresses the need to confront online hate speech at the Union level, maintaining the overarching principle that 'what is illegal offline should remain illegal online’.[58] Here we can see an approximation towards a common EU approach.

complementary to the EU Strategy on combating Antisemitism and fostering Jewish life in the EU , the EU Strategy for the Rights of Persons with Disabilities 2021-2030 as well as the EU strategy on Victims' Rights 2020-2025 and the Directive 2012/29/EU that replaced the Council Framework Decision 2001/220/JHA (‘Victims’ Rights Directive’) , which requires the criminalization of hate speech and hate crime at a national or EU level as a prior for a victim to fall under the scope of the Directive and to have access to supportive measures

[56] For further detail see: Philip Alston and Joseph H. H. Weiler, ‘An 'Ever Closer Union' in Need of a Human Rights Policy: The European Union and Human Rights (1998). European Journal of International Law, Vol. 9, 673

[57] Claes, M. 'How Common Are The Values Of The European Union?' Croatian Yearbook of European Law & Policy [2019] 15(1) VII-XVI. Available at: https://www.cyelp.com/index.php/cyelp/article/view/373

[58] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions,Tackling Illegal Content Online Towards an enhanced responsibility of online platforms, Brussels, 28.9.2017 COM(2017) 555 final

‘What is illegal offline should remain illegal online’ is central tenet to the relatively new Digital Services Act (DSA).[59] This new legislative instrument introduces a horizontal framework for regulatory oversight, transparency, and accountability, thereby advancing EU digital service regulation for a safer online space for EU citizens. Building upon the E-Commerce Directive, the DSA has already established transparency guarantees, e.g. the DSA Transparency Hub.[60] It has also 'showed its teeth’ in terms of imposing stringent rules for managing illegal content and moderating platforms.[61] Additionally, the DSA incorporates due diligence processes that offer procedural safeguards for the protection of fundamental rights. These safeguards are designed to regulate the process of online activity rather than the speech itself within such contexts. Nevertheless, as in the E-Commerce Directive, the DSA still approaches hate speech as a type of illegal activity, without explicitly defining illegality. What is illegal remains therefore determined by either EU law or national law in accordance with EU law.[62] Consequently, the DSA does not aim to independently (re)define the illegality of online content.

In this context, the DSA still does not give an answer to the two questions posed in the beginning. The question of what hate speech is remains equally untouched in the digital realm. While the EU’s DSA offers comprehensive procedural safeguards, it seems to address contentious issues like 'illegal hate speech' in a peripheral and ambiguous manner hindering common, comprehensive, and effective approach at the EU level. In addition, we witness the creation of a new digital constitutional framework for platform governance, raising questions about where decision-making authority resides and what procedural norms and protections are in place. This further fragment the landscape of regulating hate speech.

Conclusion

In conclusion, the EU, despite some efforts to combat hate speech, remains challenged by the lack of a comprehensive definition of this phenomenon. As explained, the EU’s core values and, by consequence, its understanding of hate speech is shaped by the Member States’ perceptions and constitutional traditions. This brings two crucial questions. First, it begs a reflection on the extent

[59] European Parliament and Council of the European Union, 'Regulation (EU) 2022/2065 of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)' OJ L 277/1

[60] https://transparency.dsa.ec.europa.eu/

[61] https://ec.europa.eu/commission/presscorner/detail/en/IP_23_6709

[62] Regulation (EU) 2022/2065, rec 12

to which core EU values are in fact shared values. Second, it requires to ask how and to what extent this translates into an obstacle for a harmonised approach to regulating hate speech.

Looking closer to the digital sector, the fragmented approach of the DSA points in the direction of these two questions. The transition to digital platforms has highlighted ongoing challenges in decision-making processes including content moderation complexities and the imperative to support democratic engagement. The DSA lays down significant procedural safeguards, yet the EU's strategy towards managing online hate speech and devising a cohesive framework remains a challenge. The Act's effectiveness will ultimately be judged by how it is applied and enforced in practice.

In the end, the ability of the EU to navigate these questions will serve as a crucial test of its capacity to protect public values. It determines the extent to which the EU can create a safe space for its citizens, where the exercise of fundamental rights is not hindered by illegal and harmful hate speech.

Bio:

Stevi Kitsou is a PhD Researcher at the Department of International and European Law at Maastricht University.

COURT DATA AS A VALUABLE TOOL TO RESEARCH DIGITAL LEGAL STUDIES

Andrii Koshman

SUMMARY: My PhD project delves into court data and aims at proposing its common conceptual understanding and categorisation, while at the same time investigating how a better-quality court data can improve the public understanding of court systems and judicial accountability. The research contributes to the Digital Legal Studies and aligns with themes of digital dispute resolution and computational analysis of legal complexities by addressing issues of court data comprehensibility and quality.

The Winter School "Data, Personalisation and the Law 2023" was a rewarding experience, full of thought-provoking lectures and workshops on a wide range of topics at the intersection of technology and law. Engaging conversations on both theoretical and practical dimensions of data, such as data justice, data governance, data representation for legal network analysis, sparked new ideas for the advancement of my research project. I would like to reflect on the ways in which my research project can contribute to the further development of Digital Legal Studies.

My PhD project focuses on court data, i.e. data generated in the process of delivering and administering justice. Despite the growing recognition that court data is central to evidence-based policy in the justice system,[63] the court data itself remains an elusive category. Policymakers, court administrators and academics around the world have different views on what constitutes court data and why a particular type of data may or may not be considered court data.[64] By examining approaches to defining court data in the UK and other jurisdictions, my project seeks to propose a common conceptual understanding of the court data and its general characteristics. Based on the findings and existing interpretations, the project will propose a theory-grounded typology (not a taxonomy) of court data and their sources. These theoretical inputs can be used to help justice systems around the world to capture and utilize their data more accurately.

Moving from the conceptual to the practical side, my research explores court data quality by looking at how to measure, ensure and improve court data quality. High-quality court data is vital

[63] European Commission for the Efficiency of Justice (CEPEJ), 'Guidelines on Judicial Statistics (GOJUST)' (2008).
[64] Judith Townend and Cassandra Wiener, *Justice system data: a comparative study* (The Legal Education Foundation, 2021).

in ensuring that justice is administered in an evidence-informed manner, in holding the judiciary and the judges accountable, in understanding key court processes and users' routes through the justice system, and in researching and evaluating justice effectiveness.[65] Building on the knowledge gained, the project will examine the impact of the quality of court data on the public understanding of the justice system and on judicial accountability. The project's findings will contribute to the wider enterprise of building a user-centric and accountable justice system.

All in all, by exploring the court data and its quality, my research paves the way for data-oriented understanding and research of the justice systems. This objective fits within the data, law, technology scope of Digital Legal Studies and specifically aligns with two of its four main research themes – digital dispute resolution and data science for law. As part of their research of digital dispute resolution and digitalisation of justice, the researchers at Radboud University are dealing with court data. Ultimately, court data is a starting point and a main source of contextual information in exploring how technology affects and transforms courts and dispute resolution. The digitisation of justice has substantial impact on the data landscape of the legal systems, changing the way data is collected, stored, used, and accessed.[66] The ability to capture and disseminate more data is growing exponentially as court infrastructure becomes increasingly digital.[67] However, the data collected is often of questionable quality, which limits its usefulness and can compromise the reliability of research analysis.[68] My project addresses the issue of data quality seeing it as a necessary condition for the productive use of data, i.e. for revealing reliable insights about court processes, outcomes, experiences, and impacts. In identifying opportunities and specific ways to improve the court data quality, my aim is to enhance the value and utility of court data as a tool for research and evaluation of digital dispute resolution and digitalisation of justice.

Furthermore, my findings can be useful for the computational research on the complexity of the legal system, carried out by the Law and Tech Lab at the University of Maastricht. Despite the huge potential of modelling big legal data using computational techniques and quantitative methods, there are challenges in using appropriate data. The aforementioned confusion over the

[65] HMCTS, *HMCTS Data Strategy* (2021).
[66] V. Janeček, 'Digitalised Legal Information: Towards a New Publication Model' in C Ohman and D Watson (eds), The 2018 Yearbook of the Digital Ethics Lab (Springer, 2019).
[67] M, Fabri, 'Will COVID-19 Accelerate Implementation of ICT in Courts?' (2021) 12 IJCA 1.
[68] H. McDonald and L. Haultain, *Calibrating Justice: The Use and Utility of Administrative Data in Victoria's Civil Justice System* (Victoria Law Foundation, 2023).

types and sources of court data inevitably affects the suitability and reliability of datasets (collections of court data) used for computational analysis. Considerable effort is required to ensure that the dataset contains appropriate and representative court data, sufficient to answer the relevant research questions in a data-driven way. By laying the groundwork – categorising court data types and its sources – my project aims to improve understanding on what data, where and by whom is produced and collected. Such an understanding is essential for the compilation of the appropriate datasets and their confident use in the computational analysis of complex legal issues.

Overall, court data, either alone or in combination with other types of legal data, is a valuable tool to research Digital Legal Studies. Good quality court data provides concrete and verifiable information for analysing and drawing conclusions about interplay between digital technology, law, and justice. My research focus on court data and project's findings can be instrumental in further developing the evolving field of Digital Legal Studies.

Bio:

Andrii Koshman is a doctoral researcher at the University of Bristol Law School. Andrii has been a legal adviser to the European Union, Council of Europe, and UNDP projects in Ukraine and has more than ten years of experience in public administration, including senior positions in the Ministry of Justice and the Parliamentary Staff.

COULD DIGITAL LEGAL STUDIES HELP WITH GOVERNING DIGITAL IMMORTALITY IN THE DIGITAL AFTERLIFE?

Khadiza Laskor

SUMMARY: *'Digital Immortality'* (DI)[69] and *'Digital Afterlife'* (DA)[70] have been framed since the turn of the century as capabilities to continue a digital existence posthumously. These range from the practical (making arrangements over your digital assets), foreseeable (curating a digital chatbot or avatar by someone terminally ill or by someone immensely bereft[71]), or ideological (*'mind-uploading'*[72 73]). Regardless of how believable these are, DI and DA essentially concerns the data one leaves behind after death: it does not vanish when a person takes their last breath but the scale and potential uses may be future dilemmas for policymakers.

RESEARCH GAPS & UNDERLYING THEORIES

The thesis behind this post asks *'how DI and DA should be governed, if at all?'* (it is worth noting that *'governance'* is being used as an umbrella term within the thesis to include both hard and soft approaches). Within academic circles, debates regarding dignity, privacy, personality and ethics have highlighted gaps within legal and policy frameworks, including issues such as the rights of the deceased, survivors, and those of AI and avatar. These intersect with the moral and spiritual complexities associated with grief, loss and bereavement. These also connect with curation and memorialisation, and thus archaeology. Further, a digital immortal could be seen in the same light as a human cadaver, overlapping medical, funeral and bioethical practices.

However, governance of DI and DA could be in conflict with perceived connotations of the potential *'Death Tech', 'Grieftech', 'Digital Death'* or *'Post-Life'* industry being buzzwords[74]. Regardless, this area remains uncertain and under-researched. Further, history has shown that it

[69] G. Bell and J. Gray, 'Digital Immortality' (Association for Computing Machinery, Inc., 2000), accessed on <https://www.microsoft.com/en-us/research/publication/digital-immortality/>.
[70] M. Savin-Baden and V. Mason-Robbie, eds., *Digital Afterlife: Death Matters in a Digital Age* (Chapman and Hall/CRC, 2020).
[71] E. Harbinja, L. Edwards, and M. McVey, 'Governing Ghostbots', *Computer Law & Security Review* 48 (2023): 105791, accessed on <https://doi.org/10.1016/j.clsr.2023.105791>.
[72] R. Kurzweil, *The Singularity Is near : When Humans Transcend Biology* (Penguin Books, 2006), accessed on <http://books.google.com/books?isbn=0143037889>.
[73] M.A. Rothblatt, *Virtually Human : The Promise---and the Peril---of Digital Immortality* (St. Martin's Press, 2014).
[74] A. Cornwall, 'Buzzwords and Fuzzwords: Deconstructing Development Discourse', *Development in Practice* 17, no. 4–5 (2007): 471–84, accessed on <https://doi.org/10.1080/09614520701469302>.

often repeats itself as previous attempts at governing other technologies have occurred during long lags between innovation, understanding of its wider impacts and a governance response or is too late as a 'lock-in' has occurred[75] [76]. But has recent efforts in regulating AI finally demonstrated that policymakers do indeed now take technology more seriously and proactively than they had before[77]? If so, a well-timed and collaborative approach with strong stakeholder and public engagement could promote anticipatory governance frameworks for future technological innovation.

Accordingly, a design of such an anticipatory governance framework is being explored in this thesis with DI and DA as use cases. The flexible design approach, where later studies are determined by earlier findings[78], commenced with a systematic literature review of the framing of both DI and DA, and the governance landscape that currently exists. The reason for enquiring about the framing is that any underlying messages are ideological[79] which has been evident when comparing the various AI regulatory artefacts from China[80], EU, UK[81] and USA[82]. The review followed a management evidential methodology and incorporated grey literature in addition to academic material[83] [84]. Grey literature is considered contemporary in dynamic areas where academic studies are few and thus, ideal here.

[75] D. Collingridge, *The Social Control of Technology* (Open University Press, 1980).
[76] J. Lanier, *You Are Not a Gadget : A Manifesto*, Updated [ed.]. (Penguin, 2011).
[77] L. O'Carroll, 'EU Agrees "Historic" Deal with World's First Laws to Regulate AI', *The Guardian*, 9 December 2023, sec. World news, accessed on <https://www.theguardian.com/world/2023/dec/08/eu-agrees-historic-deal-with-worlds-first-laws-to-regulate-ai>.
[78] C. Robson and K. McCartan, *Real World Research : A Resource for Users of Social Research Methods in Applied Settings*, Fourth edition. (Wiley, 2016), accessed on <http://www.wiley.com/college/robson>.
[79] G. Keren, *Perspectives on Framing* (Psychology Press, 2011), accessed on <https://www.taylorfrancis.com/books/mono/10.4324/9780203854167/perspectives-framing-gideon-keren>.
[80] PricewaterhouseCoopers, 'Regulatory and Legislation: China's Interim Measures for the Management of Generative Artificial Intelligence Services Officially Implemented', PwC, accessed 10 December 2023 on <https://www.pwccn.com/en/industries/telecommunications-media-and-technology/publications/interim-measures-for-generative-ai-services-implemented-aug2023.html>.
[81] A. Charlesworth et al., 'Response to the UK's March 2023 White Paper "A pro-Innovation Approach to AI Regulation"', *SSRN Electronic Journal*, 2023, accessed on <https://doi.org/10.2139/ssrn.4477368>.
[82] The White House, 'FACT SHEET: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence', The White House, 30 October 2023, accessed on <https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/>.
[83] D. Denyer and D. Tranfield, 'Producing a Systematic Review', in *The Sage Handbook of Organizational Research Methods* (Thousand Oaks, CA: Sage Publications Ltd, 2009), 671–89.
[84] R.J. Adams, P. Smart, and A. Sigismund Huff, 'Shades of Grey: Guidelines for Working with the Grey Literature in Systematic Reviews for Management and Organizational Studies', *International Journal of Management Reviews* 19, no. 4 (2017): 432–54, accessed on <https://doi.org/10.1111/ijmr.12102>.

Key to the thesis is the theory of *‘Responsible Innovation’* (RI) which combines social, natural and physical sciences with ethical, legal and social implications from innovation[85]. An important aspect of RI is *‘Deliberative’*[86]: this requires open discussions with stakeholders, including the public, over expectations and impacts of innovation which seems to have not been evident in AI regulation. The RI framework also includes *‘Anticipatory, Reflective and Responsive’* and will influence subsequent studies in the thesis.

Additionally, the theory of code being law is important[87] [88]. However, due to the nature of some DI and DA products and services, *‘virtual governance’* will need to be considered too, specifically over how *‘real’* and valuable intangible virtual objects are[89]. These notions are prominent in studies relating to gaming which have been used to debate governance scenarios that overlap with ethics and the applicability of *‘real-world’* rules into cyberspace[90].

Lastly, as the foci is on data that remains after one has passed away (and its various diverse presentations, representations and interpretations), examining its multi-usage will be vital. It would incorporate topics such as, biopolitics but not just the kind enacted by authoritarian states but that enforced obliviously by technologists[91] [92] [93]. The latter may not be much of a surprise if one considers that most technological innovation stems from the USA; there lies also the foundation of DI and DA encapsulating opportune developments within the Life Extension industry and immersive technology since after the Second World War, coinciding with the deconstruction of human thinking through cybernetics and computational intelligence. Recent incidents of technological mishandling of data are increasing and while some technologists appear to be acting

[85] R. Owen, P. Macnaghten, and J. Stilgoe, ‘Responsible Research and Innovation: From Science in Society to Science for Society, with Society’, *Science and Public Policy* 39, no. 6 (2012), 751–60, accessed on <https://doi.org/10.1093/scipol/scs093>.

[86] J. Stilgoe, R. Owen, and P. Macnaghten, ‘Developing a Framework for Responsible Innovation’, *Research Policy* 42, no. 9 (2013): 1568–80, accessed on <https://doi.org/10.1016/j.respol.2013.05.008>.

[87] L. Lessig, *Code : Version 2.0*, [2nd ed.]. (Basic Books, 2006).

[88] A. Murray, *The Regulation of Cyberspace : Control in the Online Environment* (Routledge-Cavendish, 2007), accessed on <http://catdir.loc.gov/catdir/toc/ecip0616/2006020898.html>.

[89] F. Gregory. Lastowka, *Virtual Justice : The New Laws of Online Worlds* (Yale University Press, 2010), accessed on <https://doi.org/10.12987/9780300146134>.

[90] B. Chester Cheong, ‘Avatars in the Metaverse: Potential Legal Issues and Remedies’, *International Cybersecurity Law Review* 3, no. 2 (2022): 467–94, accessed on <https://doi.org/10.1365/s43439-022-00056-9>.

[91] M. Foucault et al., *Technologies of the Self : A Seminar with Michel Foucault* (University of Massachusetts Press, 1988), accessed on <http://www.gbv.de/dms/bowker/toc/9780870235924.pdf>.

[92] S. Zuboff, *The Age of Surveillance Capitalism : The Fight for a Human Future at the New Frontier of Power* (London: Profile Books, 2019).

[93] ‘The Great Hack (2019) - IMDb’, accessed 21 October 2022 on <https://www.imdb.com/title/tt4736550/>.

more responsibly, there is a notion of *'ethics-washing'*: a shield to keep formal regulators at a distance.[94]

LESSONS LEARNED FROM THE WINTER SCHOOL

Succinctly, *'yes'* would be the answer to this blog's title. To expand, apart from *'Data Justice'*[95] being exceptionally relevant from the Winter School to the thesis, other pertinent themes included at least vulnerability[96] [97] and harms [98] [99]. Consequently, *'Data Ethics'*[100] could probably be seen as the overarching category within Digital Legal Studies (DLS) especially with references to the work of Professor Luciano Floridi[101]. Although it is foreseen that there will be a lag for any legal or regulatory acceptance of legal concepts associated with DI and DA, one of the main hurdles could be due to dignity being difficult to prove objectively but *'data dignity'* is more nascent and is a potential avenue to pursue[102]. This could perhaps also help in recognising other new concepts which stem from dignity, specifically *'Post-Mortem Privacy'*[103].

However, a key aspect that was not discussed as much as one anticipated was that of the user; this may be due to DLS taking a data-centric position as opposed to a user-centric one. Nevertheless, the recurring theme throughout the programme was of fundamental rights which undoubtably revolves around individuals, though collective rights was highlighted which is a growing

[94] A. Charlesworth, 'Regulating Algorithmic Assemblages: Looking beyond Corporatist AI Ethics', in *Data-Driven Personalisation in Markets, Politics and Law*, ed. Uta Kohl and Jacob Eisler, 1st ed. (Cambridge University Press, 2021), 243–62, accessed on <https://www.cambridge.org/core/product/identifier/9781108891325%23CN-bp-14/type/book_part>.

[95] L. Taylor, 'What Is Data Justice? The Case for Connecting Digital Rights and Freedoms Globally', *Big Data & Society* 4, no. 2 (1 December 2017): 2053951717736335, accessed on <https://doi.org/10.1177/2053951717736335>.

[96] C. Rigotti and G. Malgieri, 'Human Vulnerability in the Metaverse', n.d.

[97] R.A. Belliotti, *Posthumous Harm: Why the Dead Are Still Vulnerable* (Lexington Books, 2011), accessed on <http://ebookcentral.proquest.com/lib/bristol/detail.action?docID=3031660>.

[98] I. Graef and B. Van Der Slot, 'Collective Data Harms at the Crossroads of Data Protection and Competition Law: Moving Beyond Individual Empowerment', *European Business Law Review* 33, no. Issue 4 (1 June 2022): 513–36, accessed on <https://doi.org/10.54648/EULR2022024>.

[99] Harbinja, Edwards, and McVey, 'Governing Ghostbots'.

[100] E. Keymolen and L. Taylor, 'Data Ethics and Data Science: An Uneasy Marriage?', in *Data Science for Entrepreneurship*, ed. Werner Liebregts, Willem-Jan Van Den Heuvel, and Arjan Van Den Born, Classroom Companion: Business (Cham: Springer International Publishing, 2023), 481–99, accessed on <https://doi.org/10.1007/978-3-031-19554-9_20>.

[101] L. Floridi, *The 4th Revolution : How the Infosphere Is Reshaping Human Reality* (Oxford University Press, 2016).

[102] J. Lanier and E. Glen Weyl, 'A Blueprint for a Better Digital Society', *Harvard Business Review*, 2018, accessed on <https://hbr.org/2018/09/a-blueprint-for-a-better-digital-society>.

[103] E. Harbinja, 'Post-Mortem Privacy 2.0: Theory, Law, and Technology', *International Review of Law, Computers & Technology* 31, no. 1 (2017): 26–42, accessed on <https://doi.org/10.1080/13600869.2017.1275116>.

consideration with AI inferences. Therefore, could *'Interops'* – a consensus between technology, users or their data, policymakers and institutions[104] – and *'Value-Sensitive Design'*[105] also help DLS?

The user also circles back to RI as the subsequent studies the thesis aims for are analysing opinions from stakeholders and the public regarding the use and potential governance of DI and DA. One of the main preliminary themes is of ownership[106] but how can one own something that is intangible and predominantly out of their control?

This is one of many future research questions that DLS could potentially ask. The programme broadly demonstrated that DLS is a multi-disciplinary research initiative and if the collaboration and enthusiasm observed maintains, the future of DLS has exciting prospects but a more global reach is strongly encouraged as it proceeds and expands.

Bio:

Khadiza Laskor is a third-year PhD candidate at the University of Bristol's *'Engineering and Physical Sciences Research Council Centre for Doctoral Training in Cyber Security'*. Prior to joining the Centre, she worked in the Banking Industry in roles across IT audit, risk and compliance.

[104] J. Palfrey and U. Gasser, *Interop : The Promise and Perils of Highly Interconnected Systems* (Basic Books, 2012).

[105] V. Galvao, C. Maciel, and J. Viterbo, 'Human Values Expressed by Users Regarding Digital Immortality', in *IHC 2018: Proceedings of the 17th Brazilian Symposium on Human Factors in Computing Systems*, 2018, accessed on <https://doi.org/10.1145/3274192.3274240>.

[106] B. Custers and G. Malgieri, 'Priceless Data: Why the EU Fundamental Right to Data Protection Is at Odds with Trade in Personal Data', *Computer Law & Security Review* 45 (1 July 2022): 105683, accessed on <https://doi.org/10.1016/j.clsr.2022.105683>.

DECEPTIVE DESIGN PRACTICES: AN OVERVIEW OF THE DEVELOPMENTS IN TURKEY

Sinem Özyiğit

Trust is undeniably the key ingredient for better functioning of online platforms. However, the fact is that the appeal of deceptive design strategies prevents target persons from making "*autonomous and informed choices or decisions,*"[107] which in turn undermines trust. Especially when artificial intelligence is employed, subconscious decisions may even be triggered.[108] As such, there is an urgent need for the most efficient regulation. In order to contribute to the comparative legal literature, this contribution takes a closer look at the developments in Turkey.

Deceptive design practices have been on the agenda of the Turkish legislator since 2022. In this sense, an initial attempt has been made on 1 February 2022 to improve consumer protection law, and a new misleading (and thus unfair) commercial practice was included in the Annex A(22) of the Commercial Advertising and Unfair Commercial Practices Regulation[109] ("**Regulation**"), which is: "applying methods that adversely impact consumers' decision-making or choice, or that aim to bring about changes in favor of the seller or provider in the decision consumers would make under normal circumstances - through tools such as guiding interface designs, options or expressions concerning a good or service on the internet." Thus, the Advertising Board of Turkey ("**Board**") has become charged with investigating complaints regarding deceptive design practices.

The Regulation neither reflects the terminology adopted by the legislator nor offers any definition in its Article 4 (Definitions). However, the term "dark (commercial) patterns" has been used for the first time in the public announcement of the Board Meeting No: 336 convened on 8 August 2023.[110] This announcement reflected that, in the eyes of the Board, "dark (commercial) patterns"

[107] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act), OJ L 277, 27.10.2022, Rec. 67.

[108] M. R. Leiser. (2023). Psychological Patterns and Article 5 of the AI Act Proposal. SSRN, p. 3; L. E. Willis. (2020). Deception by Design. Harvard Journal of Law & Technology, 34(1), 115-190.

[109] Official Gazette No: 29232, Official Gazette Date: 10.01.2015. The Regulation is based on the Turkish Consumer Protection Law No: 6502 (Official Gazette No: 28835, Official Gazette Date: 28.11.2013).

[110] The announcement, which was published on 10 August 2023 on the website of the Turkish Ministry of Trade, is available at: <https://ticaret.gov.tr/haberler/reklam-kurulu-tarafindan-karanlik-ticari-tasarimlar-incelemeye-alindi>.

materially distort the economic behavior of consumers and violate the principle of good faith. Although sanctions were imposed by several decisions of the Board Meeting No: 336 based on the Annex A(22) of the Regulation, these decisions did not explicitly use the term “dark (commercial) patterns.” In the following paragraphs, a brief summary of these decisions will be provided.

Decision No: 2023/6011 is regarding an event ticketing platform, on which: (**i**) tickets were offered for events that were not available, (**ii**) these tickets were priced significantly higher than what is feasible, and (**iii**) notifications were presented to users indicating that many other users were also in the process of buying tickets. Referring to the Annex A(22) of the Regulation, the Board decided to impose an administrative fine of 347.128TL and to order cessation of the aforementioned practices.

A telecommunication service provider, in *Decision No: 2023/229*, offered special plans for lines available on its website. It directed consumers who preferred an annual subscription to the payment page, while directing those who preferred a monthly subscription to the information page. It is obvious that a relatively easy process was anticipated for an annual subscription, and this encouraged consumers to subscribe for a longer period. As such, the Board found this practice misleading in light of the Annex A(22) of the Regulation and thus ordered its cessation.

In *Decision No: 2023/230*, an online streaming platform presented on the payment page an annual plan with a 43% discount in a pre-selected manner. Given that this advertisement led consumers to subscribe for a longer period by intervening in their decision-making, the Board concluded that it is misleading according to the Annex A(22) of the Regulation and thus ordered its cessation. The Board reached the same conclusion in *Decision No: 2023/5991* where the seller displayed the discounted assembly service in a pre-selected manner on the payment page and in *Decision No: 2023/5986* where a six-month magazine subscription was offered in a pre-selected manner on the payment page among four plans with a duration of one, three, six and twelve month(s).

According to *Decision No: 2023/233*, in an advertisement of a software company, the option to keep the existing operating system is displayed at the bottom and in a less prominent manner, compared to the option to upgrade the operating system. The Board concluded that the advertisement is misleading according to the Annex A(22) of the Regulation and ordered its cessation, since this interference drove consumers to upgrade the operating system.

Bio:

Sinem Özyiğit is a PhD researcher at the Yeditepe University Faculty of Law.

THE NEGLIGENT LIABILITY: SOLUTION FOR THE LIABILITY ISSUES FOR AUTONOMOUS SYSTEMS?

Şura Nur Pelit

SUMMARY: Transition from instruction-based systems to autonomous technologies has brought so many legal liability problems because in the spectrum leading to automatization and then to autonomization, the casual link between human action and the consequences has become blurred. The process of perception of the environment through sensors, processing the data obtained and acting based on that accordingly, weakened human agent-control over its actions. Therefore, the questions with regards to liability, has become inevitable especially in the criminal law, which stands on the foundations of individual responsibility and guilt-based liability. In this study, the criminal liability issues caused by autonomous systems is examined from the perspective of the manufacturer/provider. Since the main problem arises in liability from negligence, production of autonomous systems to cause wrongfulness purposely and knowingly is excluded for this study. Negligent liability of the manifacturer because of the wrongfulness caused by autonomous systems is discussed in terms of two limiting factors of negligent liability: foreseeability of occurance of this wrongfulness for the manifacturer and the concept of permitted risk (erlaubtes risiko). By comparing the legal regulations of USA and Germany, which have already made regulations for the introduction of autonomous vehicles in the road traffic, it was concluded that abstract determination of foreseeability is not an enough basis for negligent liability of the manifacturer in the guilt-based criminal law liability system.

Keywords: *permitted risk, autonomous vehicles, forseeability, human dignity, criminal liability, negligence*

1. RESEARCH PROJECT: THE NEGLİGENT LİABİLİTY: SOLUTİON FOR THE LİABİLİTY ISSUES FOR AUTONOMOUS SYSTEMS?

Criminal law as an ultima ratio tool to protect legal values has an important role in securing legal order that fundamental rights of the citizens are respected. However in the age of autonomous technologies, finding and punishing the perpetrator is not an easy task because of the weakening of the human agent control over its actions. By means of the introduction of the self-learning technologies, digital devices are more than being a mere tool for human agent actions. Since the causal link between human action and wrongful result has become blurred, autonomous systems have the risk of creating "responsibility gaps" that no one could be held liable and therefore, go beyond the limits of legal coverage.

The risks posed by automated and autonomous decision systems with regard to liability and protection of fundamental rights could not be prevented with a prohibition of these technologies. For this reason, an examination of the existing criminal liability mechanism is required to decide whether the existing regulations provide an adequate solution or a revision of existing rules is needed.

In this study, which focuses on the negligent criminal liability of the manufacturer, the foreseeability of the wrongfulness for the manufacturer and the concept of permitted risk (erlaubtes risiko) which are put forward to limit the manufacturer’s negligent liability will be critically examined.

Since the effect autonomous feature of the systems on criminal liability is appearant in negligent liability by its nature, production of autonomous systems to commit crimes purposely and knowingly is excluded for this study. In order to examine the negligent criminal liability of the manifacturer in the case of autonomous systems, first the criminal negligent liability and its conditions will be examined in general. Then the technical features of the systems in the spectrum leading to automatization and then to autonomization will be revealed in order to determine the effect of those systems to the casual link that exist human agent action and the wrongful result. Finally, the foreseeability condition of the negligent liability and the permitted risk, as two concepts with a limiting effect the negligent liability will be examined. Germany and the United States, which have legal regulations regarding autonomous vehicles and represent two different legal systems with guilty-dependent criminal liability and tort-like criminal liability regulations, are selected for the examination in order to clarify the issues regarding the liability.

2. The Research Project Through the Lens of Digital Legal Studies

The research project deals with the central question of Digital Law Studies -how to regulate emerging technologies- from the perspective of autonomous systems. Therefore, the project is an attempt to make a contribution from the field of criminal law to the argument that the replacement of human decision-makers with automated decision-makers undermines the existing legal norms.

Legal issues brought about by the transition to autonomous systems constitute the intersection cluster that both Digital Legal Studies and the research project focus on. In this direction, the Winter School, which devoted one day to Autonomous Decision-Making Systems, helped me to re-evaluate and shape the relevant parts of my project.

In addition to the challenges regarding governance of decision makers, the programme of the Winter School with a critical insight into the EU regulations such as DSA and DMA, helped to address the problem of defining the content of the due diligence in negligent liability from perspectives other than criminal law. On the other hand, criminal law focus of the reserach project offered a new perspective to the liability issues to target automated decision making.

I would like to take this opportunity to thank the organising team for bringing us together for a week with colleagues working on different issues within the scope of the Digital Legal Studies, in Leiden, 200 km from Brussels, where the negotiations on the proposed AI Act are still ongoing.

Bio:

Following her bachelor's degree in law, Şura Nur Pelit completed her master's degree with her thesis on “Criminal Law Approach to Hate Crimes”. As a PhD student, currently, she is working on the interpretation of the concept of risk as a criterion for determining the duty of care in negligent liability in the field of criminal law.

“USER IS LAW”: ACCOUNTING FOR USER EXPERIENCES TO REGULATE MANIPULATIVE DESIGNS

Lorena Sánchez Chamorro

SUMMARY: *“Only two more left! Don’t be a fool! Are you sure you don’t want to accept this amazing deal? Are you? Are you certain? And now?”* The prevalence of manipulative designs – i.e. dark patterns[111], design elements that steer users to make decisions that, if fully informed, they would not make – in online interfaces is a rising concern among scholars and policymakers. These designs are raising attention given their impact on users' autonomy and their associated privacy, financial, and well-being harms[112]. Understanding and regulating manipulative designs requires a holistic approach that accounts for users' contexts and experiences when interacting with these platforms. Bringing perspectives from Human-Computer Interaction (“HCI”) scholarship will allow Digital Legal Studies to advance quickly and efficiently, towards flexible regulations on manipulative designs.

1. DARK PATTERNS – A TERM THAT LEAVES MUCH TO BE DESIRED.

The term ‘dark patterns’ was coined by interaction design scholars and practitioners to describe the misuse of experience design techniques[113]. The hyper-personalisation in the design of experiences online and the misuse of UX research methods to steer user behaviours – intentionally

[111] The term ‘dark patterns’ is used in this post to criticise its usage and situate it in a specific subset of literature within the legal and HCI community. I embrace the critiques that communities of colour have regarding the term and therefore I use the term manipulative designs instead, which I also find more accurate. For more details see also Lorena Sánchez Chamorro, Kerstin Bongard-Blanchy and Vincent Koenig, ‘Ethical Tensions in UX Design Practice: Exploring the Fine Line Between Persuasion and Manipulation in Online Interfaces’ (2023); Alberto Monge Roffarello, Kai Lukoff and Luigi De Russis, ‘Defining and Identifying Attention Capture Deceptive Designs in Digital Interfaces’, *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems* (ACM 2023) <https://dl.acm.org/doi/10.1145/3544548.3580729> accessed 1 August 2023; ACM. Association for Computing Machinery, ‘Words Matter: Alternatives for Charged Terminology in the Computing Profession’ (2023) <https://www.acm.org/diversity-inclusion/words-matter> accessed 8 May 2023.

[112] A. Mathur, M. Kshirsagar and J. Mayer, ‘What Makes a Dark Pattern... Dark?: Design Attributes, Normative Considerations, and Measurement Methods’, *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (ACM 2021) <https://dl.acm.org/doi/10.1145/3411764.3445610> accessed 2 November 2022; Johanna Gunawan, Cristiana Santos and Irene Kamara, ‘Redress for Dark Patterns Privacy Harms? A Case Study on Consent Interactions’, *Proceedings of the 2022 Symposium on Computer Science and Law* (ACM 2022) <https://dl.acm.org/doi/10.1145/3511265.3550448> accessed 8 September 2023.

[113] I. Obi et al., ‘Let’s Talk About Socio-Technical Angst: Tracing the History and Evolution of Dark Patterns on Twitter from 2010–2021’ 31; Colin M Gray and others, ‘The Dark (Patterns) Side of UX Design’, *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (ACM 2018) <https://dl.acm.org/doi/10.1145/3173574.3174108> accessed 2 November 2022.

or not – led to the exploitation of users' data to design these techniques that steer them into decisions that they would not agree to if fully aware and informed[114].

The use of these malpractices by service providers and platforms has caught the attention of policymakers and regulators who have tried to define and ban these practices. In the realm of data protection, - the GDPR[115], data protection authorities, and the European Data Protection Board-, and in consumer protection, - the UCPD[116]. Furthermore, in the realm of online platforms, the Digital Services Act, among others, has put special emphasis on these practices. Although on the surface, this may sound like they would help regulate dark patterns, when we look in more detail, we see that the different ways to describe dark patterns are not consistent and that these definitions are simultaneously too inclusive and exclusive to comprehend all the types of dark patterns that can be found in interfaces.

Some regulators have failed to understand the ontological problem of manipulative designs. As widely reported in the HCI community, dark patterns is a broad and vague term that has led to a multiplicity of definitions[117]. This issue can lead to legal uncertainty and, therefore, become ineffective despite regulators' efforts. The DSA contributes to exemplifying this problem. In its recitals, it establishes the following about 'dark patterns':

“*[…] Those practices can be used to persuade the recipients of the service to engage in unwanted behaviours or into undesired decisions which have negative consequences for them. Providers of online platforms should therefore be prohibited from deceiving or nudging recipients of the service […].”*

[114] A. Mathur et al. 'Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites' (2019) 3 Proceedings of the ACM on Human-Computer Interaction 1.

[115] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC 2016 [2016/679].

[116] DIRECTIVE 2005/29/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive') [2005/29/EC].

[117] C.M. Gray, Cristiana Santos and Nataliia Bielova, 'Towards a Preliminary Ontology of Dark Patterns Knowledge', *Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems* (ACM 2023) <https://dl.acm.org/doi/10.1145/3544549.3585676> accessed 17 July 2023; Mathur, Kshirsagar and Mayer (n 2).

While the article 25 states:

"*Providers of online platforms shall not design, organise or operate their online interfaces in a way that deceives or manipulates the recipients of their service […].*"

The combination of the recital and the article 25 already points out the ontological problem: using the terms persuade, deceive, nudge or manipulate as exchangeable terms poses uncertainty about the practices that are not permitted. Indeed, the article 25.2 continues by announcing the European Commission would issue guidelines to apply the article 25.1 that remain ambiguous. Taking the approach of Susser et al.[118], persuasion differs from manipulation because it is a rational way of influencing in a transparent way, while manipulation tries to steer by exploiting users' vulnerabilities. Coercion and deception can be both means of manipulation. They consist of restricting the possible options and instilling false beliefs into the recipient, respectively. But how they can manipulation and persuasion be distinguishable when looking at a user interface?

2. Using HCI theory to inform the regulatory landscape of online manipulation.

Persuasive design is meant to change attitudes and behaviours[119] – it is even considered inherent to the nature of design *per se*[120] –, and is commonly used, among others, for the design of technologies for behavioural change – e.g., health and well-being. However, these design strategies overlap with many practices that have been categorised as 'dark patterns'. Let's take the example of using 'computers as social actors' like sending a supportive message via notification to the user to encourage to the use continue the course to learn a new language: is it just persuasion or is it a 'dark pattern'? It nags the user – asking for a user interaction repeatedly – and uses social engineering techniques – using emotional techniques in the user interaction[121]. The amalgam of definitions that have been associated with the term dark patterns do not make it easy to recognise them. While some of them clearly work in the realm of deceiving users – e.g. instilling false statements to users – and others on coercive tactics – e.g. removing options –, many of these design

[118] D. Susser, B. Roessler and H.F. Nissenbaum, 'Online Manipulation: Hidden Influences in a Digital World' [2018] SSRN Electronic Journal <https://www.ssrn.com/abstract=3306006> accessed 14 September 2021.
[119] B.J. Fogg, 'Computers as Persuasive Tools', *Persuasive Technology* (Stanford University 2003).
[120] J. Redström, 'Persuasive Design: Fringes and Foundations' in Wijnand A IJsselsteijn and others (eds), *Persuasive Technology*, vol 3962 (Springer Berlin Heidelberg 2006) <http://link.springer.com/10.1007/11755494_17> accessed 25 July 2022.
[121] Gray, Santos and Bielova (n 7).

techniques do not fall under those categories[122]. With current regulations, the line between what a 'dark pattern' is and what it is not remains blurred.

A look at the HCI and design scholarship would take us to the proposal of new ontological configurations. Mathur et al. already pointed out dark patterns as designs do not solely consist of specific patterns, but a whole mechanism[123]; therefore, looking into patterns would not ease the task of fighting and regulating them. Monge Roffarello et al.[124] explained how some "attention capture deceptive designs" fall under the idea of deception, while some others fall under the idea of seductive design because they exploit users' vulnerabilities. Looking at theoretical approaches, this idea of seductive design is the same as 'manipulative designs', used to differentiating them from deceptive, coercive, and persuasive ones[125]. With clear categories and their distinction from design theory perspectives, Digital Legal Studies will be ready to aim for a more resilient regulation and a better understanding of what regulating these designs might imply.

3. "User is law": user experience to improve users' protection against online manipulation

HCI approaches can also tell us about how users experience and live the technology, and help us understand when manipulation occurs in the presence of these designs[126]. Taking a phenomenological approach that accounts for users' experience when facing manipulative designs becomes a crucial point for different reasons. First, when regulators take relational approaches, in other words, if they consider manipulative designs only exist in relation to a user. For instance, the DSA considers manipulative designs existing when they 'materially distort or impair users' autonomy', but only users can teach us about in which ways their autonomy is distorted. Second, the users' point of view is vital to regulate manipulative designs if, by definition, manipulation is about "exploiting users' vulnerabilities". Lastly, the systemic risk approach of the DSA, which aims to evaluate mental health risks coming from platforms and might be related to manipulative designs, requires a deep understanding of users' experiences.

[122] Sánchez Chamorro, Bongard-Blanchy and Koenig (n 1).
[123] A. Mathur, J. Mayer and M. Kshirsagar, 'What Makes a Dark Pattern... Dark? Design Attributes, Normative Considerations, and Measurement Methods' [2021] arXiv:2101.04843 [cs] <http://arxiv.org/abs/2101.04843> accessed 21 February 2021.
[124] Monge Roffarello, Lukoff and De Russis (n 1).
[125] Sánchez Chamorro, Bongard-Blanchy and Koenig (n 1).
[126] C.M. Gray et al., 'End User Accounts of Dark Patterns as Felt Manipulation' (2021) 5 Proc. ACM Hum.-Comput. Interact 26.

If “code is law”, and the technological artefacts shape how the world works, why are users not law as well? Digital Legal Studies cannot overlook that the user has a role in the ‘digital design’ domain, a more comprehensive study of the technological context would not only enrich Digital Legal Studies, but also would help to advance more efficiently and quicker towards flexible regulations, which are required for the online domain. The example of manipulative designs can be the starting point to give user experiences the role they deserve in the legal context.

Bio:

Lorena Sánchez Chamorro is a doctoral researcher in the Human-Computer Interaction Research Group at the University of Luxembourg. Her current research concerns the experiences of user vulnerability towards manipulative designs to define interventions that empower users, improve the design of interfaces and, ultimately, inform policymaking. She draws on perspectives from critical human-computer interaction, socio-digital inequalities, and critical design.

DIGITAL LEGAL STUDIES IN ACTION: EMPIRICAL ASSESSMENT OF CONTENT MODERATION QUALITY UNDER THE DSA

Marie-Therese Sekwenz

SUMMARY: Researching socio-technical systems, like online platforms, demands novel methodologies and tests for assessing compliance under new regulations like the Digital Services Act (DSA). Proposing empirically based approaches for testing content moderation of online platforms like Facebook, YouTube or X should promote robust claims about compliance with the new law. By simultaneously admitting that content moderation as a process has an external perspective as well, needs to be mirrored as well in the chosen methodologies for risk assessments under Art 34 and 37 DSA, and needs to include this wide view on audits on the composition of auditing teams, the complex interplay of rules like the Terms and Conditions of platforms, or the transparency mechanisms in place as sources of information. By making use of a holistic understanding of the compliance and obligations within the European Union's attempt to expand the so-called Brussels effect to online speech spheres.

1. Is Elon Musk's X Violating Rules of the Digital Services Act?

On December 18, 2023, the European Commission initiated legal proceedings against a Very Large Online Platform (VLOP)[127] under the Digital Services Act. This new regulation aims to establish harmonized rules for content moderation and address undesirable speech on the internet.[128] The VLOP the Commission is investigating is X, the microblogging service formerly known as Twitter for potential failures of their content moderation systems regarding illegal content and manipulation of their service, their approach to DSA-compliant transparency, and deceptive design practices.[129]

To find out if platform X has infringed its obligations under the law, however, will have to answer the question: What determines effective compliance under the DSA?

Within my research, I also pose similar questions linked to this initial investigation of the Commission.

[127] Very Large Online Platforms and Very Large Search Engines are defined in Art 31 DSA, as online platforms with a large user base in the European Union.

[128] 'Commission Opens Formal Proceedings against X under the DSA' <https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6709> accessed 19 December 2023.

[129] The Commission is testing infringements with Art 34 (1), 34 (2) and 35 (1), 16 (5) and 16 (6), 25 (1), 39 and 40 (12) of the DSA.

2. Orchestration of Digital Legal Research Outlooks

In a classical music comparison of my research project, we would be starting with an overture about empirically based risk assessments[130] under the DSA's draft on selected content samples and tested an initial systemic risk assessment in the context of the German Federal elections 2021 under the draft of the DSA at the time.[131]

In the first Act of the research project we tried to further investigate this research gap of DSA compliance regarding systemic risk assessments and empirically analysed content focusing on one risk class of the DSA – the dissemination of illegal content – and the closely looked at the intersection of Terms and Conditions[132] violations.[133] For this empirically grounded analysis we used legal coding teams and utilized sampling techniques to conduct systemic risk assessments for VLOPs to further refine the methodology used in the first study.[134] Such empirically grounded legal analysis is just one of the examples of Digital Legal research that comes to mind when the Commission is now investigating for the first time. Due to the degree of complexity of such compliance decisions regarding socio-technical systems multidisciplinary teams of researchers are needed to meaningfully address these intertwined demands like conducting systemic risk assessments or external audits.

The second Act of my research project additionally wants to clarify the conditions to assess systemic risk in an audit and refine methodologies used in prior research to create tailored solutions for conducting risk assessments under the now final version of the DSA. This article should focus on sampling techniques for auditing under the law and how risks could demand special variants of sampling. If sampling is used in the process of auditing systemic risks, like the spread of illegal content on an online platform like X, sampling techniques (e.g. cluster sampling, simple random

[130] Systemic risk assessments have to be conducted under Art 34 DSA and have to cover four risk categories, like the spread of illegal content, negative effects on the electoral process or gender-based violence.
[131] Johanne Kübler and others, 'The 2021 German Federal Election on Social Media: Analysing Electoral Risks Created by Twitter and Facebook' (2023).
[132] See Art 14 DSA.
[133] See Art 34 (1) lit a DSA.
[134] B. Wagner and others, 'Forthcoming. Blurring Legal Boundaries. Recoding Interpretations of Law and Terms of Service in Online Content Governance'.

sampling etc.) should be curated to promote representativeness of the sample and should minimize errors of the audit to make an informed decision as an auditor.[135]

The third act of the research project, however, wants to see sampling techniques and legal coding methodologies for content annotation in action and will perform a systemic risk assessment on samples of data for two VLOPs.

The metaphorical fourth act considers the rules the DSA created to further increase transparency on the platform's content moderation decisions, like Statements of Reason,[136] Transparency Reports,[137] advertising repositories[138] or Terms and Conditions[139] to study simultaneously different mechanisms of compliance under the new law.

The Fourth act, on the other hand, is taking a closer look at the ex-ante content moderation[140] practices of platforms that are mostly facilitated with content moderation systems supported by Artificial Intelligence and human content moderators alike. Only by including humans in the loop of content moderation the problem of increasing masses of illegal content and Terms and Conditions violations can be kept under control. By better understanding and testing this sequence of moderation steps under the DSA, we want to shed light on the fuzzy edges of (automatically) making decisions about different forms of speech.

Finally, in the Fifth act, this research project admits that (ex-post) content moderation is also influenced by external parties like other users, Trusted Flaggers,[141] public authorities,[142] Digital Service Coordinators, or the Commission. [143] By focusing on these essential external parts of moderation we want to show the layered orchestration of content moderation systems and the need

[135] 'Delegated Regulation on Independent Audits under the Digital Services Act' (20 October 2023) <https://digital-strategy.ec.europa.eu/en/library/delegated-regulation-independent-audits-under-digital-services-act> accessed 21 October 2023.
[136] See Art 17 DSA.
[137] See Art 15, 24 and 42 DSA.
[138] See Art 39 DSA.
[139] See Art 14 DSA.
[140] Ex ante content moderation, in contrast to ex post content moderation should be regarded as a form of content moderation taking place before the upload on an online platform. Ex post content moderation on the other hand should be understood as moderation taking place after the content was made available to the public. E.g., a user is flagging a piece of content on the platform and because of this notice the platform is moderating the content in question.
[141] See Art 22 DSA.
[142] See Art 9 and 10 DSA.
[143] See Art 49 DSA.

to include these additional perspectives meaningfully in the systemic risk assessments under the DSA.

3. An Open End for X and a Filled Research Agenda for Digital Legal Scholars

The filing of the proceeding against X will now further clarify what Europe will classify as DSA compliance or violation and how to test VLOPs under the DSA. Not only is a challenge for newly come-into-force regulation like the DSA a source of legal uncertainty and missing jurisdiction, but also an instrument to study regarding enforcement and legal interpretation.

It nevertheless will still be a source of renewing research interest for digital-legal scholars for the years to come, to find out what is acceptable in the newly regulated European Union’s online sphere.

Bio:

Marie-Therese Sekwenz is a PhD candidate at TU Delft’s Institute of Technology, Policy and Management and a member of the AI Futures Lab of the university. She asks questions addressing aspects of rights and justice in her research which focuses on content moderation, platform governance and regulation, Artificial Intelligence, and legal-socio-technical system design.

THE NEW AREA OF ‘CYBERSECURITY LAW’ AND CO-OPERATION IN DIGITAL LEGAL STUDIES

Mattis van ‘t Schip

SUMMARY: My research focuses on European cybersecurity law, which is an evolving field in the digital legal studies realm. After the evolution of data protection law, artificial intelligence regulation, and digital platform regulation, cybersecurity law is a new evolving framework in EU legislation for the digital economy. With this new framework come new research questions which, in my view, uniquely highlight the interdisciplinary co-operation required in the field of digital legal studies.

INTRODUCTION

In this blog post I would like to highlight recent developments that shape a new field of ‘cybersecurity law’ and, simultaneously, cybersecurity law scholarship. My research situates in this evolving field, as I study how the European Union aims to regulate cybersecurity of the Internet of Things. This new field, in my view, shows how digital legal scholars need to understand both the ‘digital’ and the ‘legal’.

CYBERSECURITY LAW THEN

Recent years have shown a proliferation of cybersecurity incidents, ranging from significant issues for critical organisations (e.g., hospitals, energy companies) to attackers accessing entire networks of interconnected devices.[144]

Digital legal scholars, around 2016, mainly had their eyes on the General Data Protection Regulation, the big new EU privacy legislation. Cybersecurity issues were thus often viewed through the GDPR: when hackers could access certain personal data (e.g., patient information in hospital servers), the General Data Protection Regulation spoke of a ‘data breach’ and the organisation could receive significant fines for not providing suitable security measures.[145] This is

[144] Manos Antonakakis and others, ‘Understanding the Mirai Botnet’, *26th USENIX Security Symposium (USENIX Security 17)* (USENIX Association 2017) <https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis>; Alex Hern, ‘WannaCry, Petya, NotPetya: How Ransomware Hit the Big Time in 2017’ *The Guardian* (30 December 2017) <https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware> accessed 19 December 2023.

[145] See Art 4(12) & Art 32 GDPR.

where such cybersecurity issues remained: as a subcategory of data protection, without clear guidance as to what 'security' meant or how organisations should implement 'security'.[146]

Cybersecurity Law Recently

The European Union acknowledged this gap and recently started legislating cybersecurity issues.[147]

The Cyber Resilience Act proposal, for instance, came in September 2022.[148] The proposal consists of cybersecurity requirements that manufacturers must implement in virtually all software and hardware products, a rather significant scope.[149]

In the same year, EU legislators adopted the NIS2 Directive. The NIS2 Directive reworked the NIS1 Directive, which was supposed to harmonise cybersecurity levels across critical organisations in the EU (e.g., hospitals, energy providers).[150] The EU realised that malicious attackers are indeed most interested in the critical sectors, as their business continuity is vital to everyday life of citizens. Imagine, for instance, that you are in a hospital which loses access to all their computer systems due to 'ransomware' (i.e., a computer virus that locks access to all data on a system and requires payment to 'unlock' that data). Critical organisations can no longer perform their daily operations without those systems.

Cybersecurity Law and Digital Legal Studies

The evolution of cybersecurity law brings a new dimension to the field of digital legal studies. As stated above, most studies of cybersecurity incidents remained within the realm of data protection scholarship: what does the General Data Protection Regulation demand in terms of security levels, given that security must be in line with the 'risks' posed to the organisation? Meanwhile, scholars

[146] P.T.J. Wolters, 'The Security of Personal Data under the GDPR: A Harmonized Duty or a Shared Responsibility?' (2017) 7 International Data Privacy Law, 165.

[147] See for an overview of recent legislation: Pier Giorgio Chiara, 'The IoT and the New EU Cybersecurity Regulatory Landscape' [2022] International Review of Law, Computers & Technology, 1.

[148] Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 COM(2022) 454 final [Cyber Resilience Act].

[149] M. van 't Schip, 'The Cyber Resilience Act in the Context of the Internet of Things' (*EULawAnalysis*, 18 November 2022) <https://eulawanalysis.blogspot.com/2022/11/the-cyber-resilience-act-in-context-of.html> accessed 5 December 2022.

[150] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive) [2022] OJ L333/80.

paid attention to the rise of artificial intelligence and law, given shape by the EU AI Act.[151] Scholars equally focused on the proliferation of digital platforms as our modern public forums, which the EU responded to with, inter alia, the Digital Services Act.[152]

Cybersecurity law, however, remained in the shadows of these giant – and important! -- areas of studies. It is a new field of studies which is both independent and overarching: cybersecurity law scholars can study the legislation discussed above, from the Cyber Resilience Act proposal to the NIS2 Directive, but they can also pay attention to how artificial intelligence shapes cyberattack and defence capabilities in the digital realm. Furthermore, digital platforms, like the hospitals mentioned before, cannot operate without sufficient cybersecurity measures.[153] Cybersecurity law is a developing field of legislation, but simultaneously an issue that involves all areas of digitalisation and the law.[154]

Furthermore, cybersecurity law challenges digital legal scholars. The legislator leaves many of the legal interpretations of cybersecurity law to technical standards (e.g., “state of the art” security measures). Computer scientists or technical experts develop these standards. It is the lawyers who must interpret ex-post whether those standards fit within the larger legal framework.[155] Cybersecurity law, it seems, forces lawyers to understand the technical details of technology and the computer scientists to understand law.

I would argue for such ‘forced’ co-operation in digital legal studies too. Let the computer scientist and legal scholars work together![156] Without insights from other disciplines, how can lawyers know how technology functions and how it impacts society? What do security specialists think when they hear about the Cyber *Resilience* Act, which in security terms is different from

[151] Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules On Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts COM(2021) 206 final [AI Act].

[152] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L277/1.

[153] ‘How Your Personal Data Is Being Scraped from Social Media’ *BBC News* (15 July 2021) <https://www.bbc.com/news/business-57841239> accessed 20 December 2023.

[154] As is often the case with questions of law and technology or technology and law!

[155] Hans-W Micklitz, ‘An Outsider’s View on Law and Technology’ in Bartosz Brożek, Olia Kanevskaia and Przemysław Pałka (eds), *Research Handbook on Law and Technology* (Edward Elgar Publishing 2023) <https://www.elgaronline.com/view/book/9781803921327/chapter23.xml> accessed 19 December 2023.

[156] As I am thankfully currently ‘forced’ to do in my own wonderful interdisciplinary research group (iHub) at Radboud University and within the multidisciplinary INTERSCT research project through which my research is funded (intersct.nl).

cyber*security*? For all these questions, co-operation between disciplines is vital. If there is one thing I take away from the digital legal studies workshop, and from my own foray into the evolving field of cybersecurity law, it is this: let us make some technical standards that force disciplines to co-operate.

Conclusion

Cybersecurity law will continue to develop: soon we will see more and more cybersecurity law conferences, next to the existing list of wonderful events about data protection law, digital platform regulation, and artificial intelligence and the law. Simultaneously, these events will highlight how we must proceed with digital legal studies: by acknowledging that digital legal studies requires us to conduct co-operative studies with a multitude of disciplines.

Bio:

Mattis van 't Schip works as a PhD Candidate at Radboud University (iHub) in the Netherlands. His research project, which is part of INTERSCT (intersct.nl), analyses European cybersecurity regulation for Internet of Things devices which consumers use in their daily lives (e.g., connected speakers, refrigerators).

DIGITAL LEGAL STUDIES – MOVING BEYOND THE INDIVIDUAL AND APPLYING METHODS

Pia Groenewolt

SUMMARY: This blog reflects on interplay of data, personalization, and law, as revealed by a winter school program emphasizing the emerging field of digital legal studies. It highlights the contrast between Europe's evolving regulatory frameworks, such as the Digital Services Act and GDPR, and academic focus on collective data implications and AI's ethical challenges. The research underscores the need for nuanced approaches to address collective data rights and privacy concerns, advocating for continued dialogue and research in this rapidly evolving domain. Key methodologies like legal network analysis are noted for their role in clarifying the complex interplay between data and regulations, emphasizing the balance between individual privacy and collective insights for a just digital future.

What are the key takeaways from the interplay of data, personalisation, and law? The winter school provided a foundational understanding on what were the developments leading to the subsection of law which is digital legal studies. From the outcome of the winter school, digital legal studies encompasses a diverse range of topics and approaches, such as employing legal network analysis to unravel the connections between CJEU judgments[157], exploring data subject rights through the lens of data vulnerabilities or injustices[158], examining the imbalance in applying collective data subject rights versus those of an individual[159], and addressing the injustices stemming from automated decision-making[160]. These varied themes are unified by a digital thread, echoing Lessig's seminal idea that code itself can function as a form of law[161].

[157] D. van Kuppevelt and G. Dijck, *Answering legal research questions about dutch case law with network analysis and visualization* (IOS Press 2017) Note: in the workshop given, granted its international audience, the methods described in the article cited where applied to CJEU judgements.

[158] B. Custers and G. Malgieri, 'Priceless data:: why the EU fundamental right to data protection is at odds with trade in personal data' (2022) 45 Computer Law & Security Review 105683Gianclaudio Malgieri and Jędrzej Niklas, 'Vulnerable data subjects' (2020) 37 Computer Law & Security Review 105415: L.Taylor, 'What is data justice? The case for connecting digital rights and freedoms globally' (2017) 4 Big Data & Society 2053951717736335.

[159] I. Graef and B. van der Sloot, 'Collective data harms at the crossroads of data protection and competition law: Moving beyond individual empowerment' (2022) 33 European Business Law Review.

[160] F.J. Zuiderveen Borgesius, 'Strengthening legal protection against discrimination by algorithms and artificial intelligence' (2020) 24 The International Journal of Human Rights, 1572.

[161] L. Lessig, *Code: And other laws of cyberspace* (ReadHowYouWant. com 2009), The thesis refered to Lessid was followed by Code Version 2.0.

The interplay between regulatory developments and academic scholarship in digital and legal studies is articulated along different axes. On one hand, Europe is witnessing an increased progression in the regulatory landscape, with the enactment of significant legislations like the Digital Services Act (DSA), Digital Markets Act (DMA), Data Governance Act, and Data Act. These regulations are pivotal in establishing clear guidelines and protections for individual data subjects, ensuring privacy and fair practices in the digital space.

On the other hand, academic scholarship is exploring a different dimension of the digital legal paradigm. It extends beyond the data subject-centric approach of current regulations, delving into the concept of collectives of data subjects. This area of study acknowledges that the impact of data and technology often transcends individual experiences, affecting groups or communities as a whole with the capitalist accumulation of data and recognition of patterns.

Scholars are acknowledging the need to address this collective aspect, which is not yet adequately represented in existing laws. For instance, how the data of a community is used, and the collective implications of such usage remain underexplored in legal frameworks.

In our modern world, the collection and recording of data occur in almost every aspect of our lives, far beyond the boundaries of direct online interactions. From the products we purchase in stores to sensors counting the number of vehicles on a street, nearly every action we take, no matter how mundane, is captured and logged. This ubiquitous data collection extends to an array of sensors and recording devices embedded in our environment, documenting our daily routines and feeding it to machines or people to make decisions based on the patterns which appear[162]. My personal scholastic interest lies in examining the scope of this realm of data linked to everyday behaviors.

The perspective that data collection is limited to our direct interactions with digital devices is short-sighted. In reality, our interactions with various technologies, whether through purchases, movement in urban spaces, or even through home appliances, contribute to our digital shadow. This vast array of data collection points is intricately linked to our identities, with most devices requiring user verification through passwords or biometric data. Such actions and interactions are

[162] A. Tupasela, K. Snell and H. Tarkkala, 'The Nordic data imaginary' (2020) 7 Big Data &amp; Society 205395172090710: P. de Pedraza and I. Vollbracht, *The Semicircular Flow of the Data Economy and the Data Sharing Laffer curve*, 2020): S. Zuboff, 'Big other: surveillance capitalism and the prospects of an information civilization' (2015) 30 Journal of information technology, 75.

well encapsulated within the scope of regulations like the General Data Protection Regulation (GDPR), which primarily addresses individual data rights and protections. However, there's another dimension to this data collection that is often overlooked: the collective aspect. Data is not only recorded at an individual level but also aggregated to discern patterns and behaviors of groups. This collective data provides insights into societal trends, preferences, and behaviors, offering a rich tapestry of information that can be used for various purposes, from urban planning to targeted advertising. This aggregation of data shifts the focus from the individual to the group, bringing forth new challenges and vulnerabilities.

AI's role in critical areas like crime, employment, and finance poses challenges, notably in upholding human rights like non-discrimination[163]. The internet amplifies epistemic injustice through an overwhelming amount of information, often difficult to validate. Addressing this, our site provides reliable and actionable resources to bridge the gap between AI's capabilities and ethical obligations[164]. While acknowledging critiques of Zuboff's 'The Age of Surveillance Capitalism,' particularly its capitalist bias, her analysis of data capture and extraction processes sheds light on the complexities of datafication[165].

As mentioned, data recording extends beyond personal computers, with everyday actions increasingly being captured by sensors. In this context, the methodology of legal network analysis serves as a valuable tool. It facilitates a descriptive approach that speeds up the process, paving the way for more in-depth explanatory research. While this method is not complete, or particularly advance, it can help give clarity to the increasing complex interplay of data, and regulations.

While regulations like the GDPR are robust in safeguarding individual data rights, the protection and ethical use of collective data represent a frontier that is yet to be fully addressed. The nuances of how group data is utilized, the implications for privacy and consent, and the potential for both beneficial and harmful uses of such aggregated information are complex issues that require careful consideration. As we navigate this era of pervasive data collection, the balance between individual

[163] H. Matsumi and D.J. Solove, 'The Prediction Society: Algorithms and the Problems of Forecasting the Future' (2023) Available at SSRN.
[164] C. D'ignazio and L.F. Klein, *Data feminism* (MIT press. 2023).
[165] Zuboff, 'Big other: surveillance capitalism and the prospects of an information civilization'.

privacy, collective insights, and the responsible use of data emerges as a crucial area for ongoing discussion, regulation, and scholarly investigation.

In conclusion, the winter school has illuminated the interplay between data, personalization, and law, highlighting the need for a nuanced approach in this evolving field. The adoption of methodologies like legal network analysis, while still developing, provides valuable insights into this. As we delve deeper into the digital age, the challenge lies not only in safeguarding individual data rights through regulations like the GDPR but also in addressing the less-explored realm of collective data rights and implications. Balancing individual privacy with collective insights and ensuring responsible data use are essential in shaping a fair and just digital future. Ongoing scholarship from now would engage in continuous dialogue, innovative regulation, and in-depth scholarly research to navigate the complexities of data and its profound impact on society.

References:

D'ignazio C and Klein LF, *Data feminism* (MIT press 2023)

Lessig L, *Code: And other laws of cyberspace* (ReadHowYouWant. com 2009)

Kuppevelt Dv and Dijck G, *Answering legal research questions about dutch case law with network analysis and visualization* (IOS Press 2017)

Custers B and Malgieri G, 'Priceless data:: why the EU fundamental right to data protection is at odds with trade in personal data' (2022) 45 Computer Law & Security Review 105683

Edelson L, Graef I and Lancieri F, 'Access to Data and Algorithms: For an Effective DMA and DSA Implementation' (2023) CERRE, March

Graef I and van der Sloot B, 'Collective data harms at the crossroads of data protection and competition law: Moving beyond individual empowerment' (2022) 33 European Business Law Review

Malgieri G and Niklas J, 'Vulnerable data subjects' (2020) 37 Computer Law & Security Review 105415

Matsumi H and Solove DJ, 'The Prediction Society: Algorithms and the Problems of Forecasting the Future' (2023) Available at SSRN

Taylor L, 'What is data justice? The case for connecting digital rights and freedoms globally' (2017) 4 Big Data & Society 2053951717736335

Tupasela A, Snell K and Tarkkala H, 'The Nordic data imaginary' (2020) 7 Big Data &amp; Society 205395172090710

Zuboff S, 'Big other: surveillance capitalism and the prospects of an information civilization' (2015) 30 Journal of information technology 75

Zuiderveen Borgesius FJ, 'Strengthening legal protection against discrimination by algorithms and artificial intelligence' (2020) 24 The International Journal of Human Rights 1572

de Pedraza P and Vollbracht I, *The Semicircular Flow of the Data Economy and the Data Sharing Laffer curve*, 2020)

Bio:

Pia Groenewolt joined VUB's Law, Science, Technology and Society research group in September 2022 as a Ph.D. candidate working on the Data4food2030 project and is supervised Prof. Dr. Niels van Dijk at the d.pia.lab. She has a diverse educational background with a Bachelor's degree in Sociology and Political Science from the University of Calgary, and Masters's in Sociology from the University of Helsinki, Political Science from ULB, in Human Rights from Université Saint-Louis and IP and ICT law from KULeuven. Her professional experience includes roles at the International Labour Organisation, the Finnish Ministry of Foreign Affairs, the Swiss Academy for Development, ALL DIGITAL aisbl, and European SchoolNet.

NAVIGATING THE COMPLEXITIES OF OUR DIGITAL SOCIETY NECESSITATES INTERDISCIPLINARY FORCES FOR SUCCESS.

Samuel Groesch

As part of the emerging field of Digital Legal Studies, encompassing calls for heightened regulation of artificial intelligence and the desire to curb the power of digital platforms, endeavours to influence digital transformation for the betterment of society are evident across various academic domains. However, distinct traditions and perspectives exist within each field addressing these emerging issues. While the conventional academic approach may attribute this to the inherent nature of universities, I argue that digital transformation demands an interdisciplinary approach.

COLLABORATION AS THE KEY TO SUCCESS

The Winter School organized by the Digital Legal Lab has exemplified the critical importance of interdisciplinary exchange in fostering a shared understanding of both technical and social developments. Whether engaging in Hard Law for the formulation of new legislative initiatives at European and national levels or delving into the analysis of Soft Law pertaining to moderation guidelines or terms of conditions of platform providers, the synergy of social science investigations, technical expertise from computer sciences, coupled with insights from psychological behavioural research or economic expertise regarding affected businesses, can significantly enhance the efficacy and overall quality of smart governance.

Given that digital enterprises primarily prioritize profit maximization, a collaborative effort involving academia, civil society, and policymakers is essential to counteract the influence of large and powerful players and comprehend the risks associated with digital transformation.

USING EMPIRICAL EVIDENCE

In my own research endeavours, I seek to apply methods from computer science to address innovative research questions within the field of communication science. Legal interpretations of these findings are particularly promising when deriving practical implications from acquired knowledge. For instance, examining the role of visual content in social networks, identifying prevalent themes in shared images, and evaluating the presence and implications of misinformation and disinformation in this format. Processing vast amounts of visual data requires novel computer-assisted methods, with the results necessitating social science contextualization and interpretation.

Making these findings usable to hold technology and underlying platforms accountable is an immensely significant opportunity in the field of legal sciences and serves as a compelling example of a stronger integration of various disciplines.

Institutionalising interdisciplinary research

I am convinced that there is a need for more initiatives and institutes that bring together different disciplines and engage in digital transformation. While there are already initial efforts in this direction, they are far from sufficient given the magnitude of the task. Interdisciplinary projects are always a challenge, precisely because individuals with diverse perspectives and varying levels of knowledge approach the same problems. Effective collaboration is only possible through adequate communication, allowing for constructive and goal-oriented cooperation. Nevertheless, one can be certain that collaborative exchange will yield innovative solutions and make addressing the significant challenges of technological change more manageable.

My institute is currently working on an interdisciplinary project with two computer science partners. In this collaboration, they are modeling a social network that will provide valuable input on governance instruments. Simulating policy instruments in such a scenario is promising for implementing regulations not simply based on individual preferences and thoughts but on rules that have been previously tested for suitability and effectiveness. Results from such projects could have a much stronger influence on political policy formulation, providing media regulators with effective tools against major corporations.

Opportunities for Digital Legal Studies

However, the same applies to Digital Legal Studies, as demonstrated in Leiden, which has highlighted the untouched potential in the field of legal sciences to apply new methods that were previously unused in the discipline to answer research questions that remained unanswered. In this regard, formats such as summer and winter schools are well-suited for expanding personal networks across disciplines, fostering an understanding of different perspectives, and initiating collaborations that should be more strongly targeted and promoted at the institutional level.

The impacts of digital technology and, more recently, technological advancements such as artificial intelligence are so fundamental and extensive that only a comprehensive holistic analysis can do justice to their effects. Otherwise, regulation may occur blindly or rely on corporate lobbying interests, leading to the societal acceptance of purportedly inherent structures of technology. This must not happen and needs to be prevented. As a community of scholars, we are doing our best to understand digitization and leverage our understanding to transpose freedom and civil rights into the digital era. This is a central task that can only be achieved through collaborative interdisciplinary efforts.

Bio:

Samuel Groesch is a Research and Teaching Associate in the Media & Internet Governance Division at the University of Zurich.

NAVIGATING THE NEXUS OF LAW AND TECHNOLOGY: INSIGHTS FROM THE WINTER SCHOOL ON DATA PERSONALIZATION AND LAW

Jean De Meyere

Participating in the Digital Legal Lab's winter school, "Data, Personalization, and the Law" was a wonderful experience. This event, hosted at the Lorentz Center in Leiden, has been an opportunity to exchange with 40 participants from diverse backgrounds to explore the multifaceted relationship between digital technologies and law.

An introduction to Digital Legal Studies

The winter school offered an extensive curriculum that embraced a wide array of topics at the intersection of technology and law. It delved into the intricacies of digital technologies such as algorithms, big data analytics, personalization, and automated decision-making, examining how the law influences technology and how technology influences the law. The sessions explored the evolution of data-centric regulations, the normative effects of digital transformation on decision-making, the role of online platforms as privacy regulators, the implications of generative AI on fundamental rights, and the nuances of data governance at the EU level. Each day provided a deep dive into different aspects of digital legal studies, emphasizing the dynamic and reciprocal relationship between legal frameworks and technological advancements. All in whole, it was a perfect introduction to the larger discussion surrounding digital legal studies.

Law's Influence on Technology

A significant portion of the discussions was dedicated to how law influences technological advancement. We debated the notion that while technology is a rapidly evolving tool, it is not beyond the realm of regulation. Regulatory frameworks can be designed to instill societal values within technological developments and emphasizing human rights such as privacy. We explored various global approaches to regulating technology, scrutinizing the balance between innovation and ethical standards. The school provided numerous examples of how legislation like the GDPR or the Digital Services Act (DSA) has the potential to shape the trajectory of technological development, ensuring that innovations align with broader societal goals.

Technological Impacts on Legal Research

Conversely, we delved into how technology is reshaping the legal landscape. The lack of digitization in legal domains poses a significant challenge, hindering the integration of innovative tools in legal research and practice. We highlighted the need for a more robust partnership between legal scholars, social scientists, and technical experts to push the boundaries of what's possible in legal studies. The sessions discuss how technology, particularly AI and big data, can been leveraged to enhance legal research, improve access to justice, and streamline legal processes. However, the discussions also acknowledged the ethical and practical challenges in implementing these technologies, stressing the need for continued vigilance and adaptive legal frameworks.

Conclusion

The winter school concluded with a synthesis of the week's discussions and an outline of a future research agenda for Digital Legal Studies. We collectively reflected on the pressing issues at the intersection of digital technology and law, acknowledging the complexities and the opportunities ahead. The experience was not only an academic exercise but also a call to action for all participants to continue exploring, questioning, and shaping the future of digital legal studies.

As I look back on the week, the conversation, the debates, and the shared learning experiences, it's clear that the winter school was a pivotal moment in my understanding of the intricate relationship between technology and law. The discussions went beyond theoretical concepts, touching on real-world implications and ethical considerations. The event was a reminder of the ongoing need for dialogue, collaboration, and innovation between various fields. As technology continues to advance at a rapid pace, the legal world must keep up, ensuring that the digital age is marked by fairness, accountability, and justice. With the insights and connections gained from this experience, I am more equipped and inspired to contribute to this vital field of study.

Bio:

Jean De Meyere is a PhD researcher at UC Louvain.