CONFERENCE

PUBLIC GOVERNANCE AND EMERGING TECHNOLOGIES: VALUES, TRUST AND COMPLIANCE BY DESIGN

11-12 January 2024

Paushuize, Utrecht

Day 1 – Thursday 11 January 2024

15:00 - 16:00 Coffee & Registration

16:00 - 17:00 **Keynote Prof. Barbara Prainsack, 'Learning from cars and trains: (Re)gaining democratic control over digital practices'**

Department of Political Science, University of Vienna

Professor for Comparative Policy Analysis | Head - Research Platform Governance of digital practices | Chair - European Group on Ethics in Science and New Technologies (EGE)

17:00 - 18:00 Networking drinks

Day 2 – Friday 12 January 2024

08.30 - 09.15 Coffee & registration

09.15- 09.30 **Plenary opening of the conference** (Balzaal)

09.30 - 10.45 **Panels round 1** (3 tracks)

10.45 - 11.00 Coffee

11.05 - 12.20 **Panels round 2** (3 tracks)

12.20 - 13.00 Lunch

13.20 - 14:00 **Keynote Prof. Janneke Gerards, 'Digital technologies and 'ex ante' protection of fundamental rights' (plenary)**

Department of Law, Utrecht University

Professor for Fundamental rights law | Chair – Advisory Council of the Netherlands Human Rights Institute | Chair – Committee for Freedom of Science of the KNAW | Member – Scientific Committee of the EU's Fundamental Rights Agency (FRA)

14:05 - 15:20 **Panels round 3** (3 tracks)

15.20 - 15.35 Coffee

15.40 - 16:55 **Panels round 4** (3 tracks)

17.00 - 18.15 Closing drinks

	1. VALUES TRACK (BALZAAL)	2. REGULATORY COMPLIANCE TRACK ('S JACOBZAAL)	3. GOVERNANCE TRACK (SOETESALON)
9.30 - 10.45	**Public tech: values, valuation, and evaluation** Moderator: Gijs van Maanen **+ Aviva de Groot** *"Whose values? Exploring productively disruptive interventions in tech policy for more inclusive public values"* **+ Gijs van Maanen** *"From values to valuation, and from public values to common goods: a brief reflection on valuable tech development"* **+ Gert Meyers** *"Realising a blockchain solution without blockchain? Blockchain, solutionism, and trust"* **+ Jolien van de Sande** *"Explaining the current state of experimentation with automated decision-making (ADS) in Dutch healthcare - an institutional analysis"*	**Regulating emerging technologies** Moderator: Balazs Bodo **+ Bao Chau** *"Engineering the fiduciary"* **+ Filippo Bagni** *"The Regulatory Sandbox and the Cybersecurity Challenge: from the Artificial Intelligence Act to the Cyber Resilience Act"* **+ Benedetta Venturato** *"Apparent decentralization and trust in blockchain based organizations"* **+ Emily Li** *"Exploring the Operational Framework and Feasibility of Integrating Blockchain Technology with Legal Services for an Intellectual Property Management Platform in the Audiovisual Industry"*	**The governance of cybersecurity** Moderator: Lorenzo Dalla Corte **+ Erik Longo and Elia Cremona** *"The Implementation of Directive NIS2 between Public and Private Governance: The Role of CSIRTs"* **+ Gianmario Demuro** *"Toward a Charter of Fundamental Rights in Cyberspace"* **+ Giovanni Coinu** *"What role for Italian regions in the cybersecurity governance"* **+ Lorenzo Moroni** *"The complicated governance of cybersecurity between technology and policy"* **+ Marco Betzu** *"The Digital Constitutionalism"*

	1. VALUES TRACK (BALZAAL)	2. REGULATORY COMPLIANCE TRACK ('S JACOBZAAL)	3. GOVERNANCE TRACK (SOETESALON)
11.05 - 12.20	**The philosophy of AI** Moderator: Max Velthoven **+ David Hadwick** *"The impact of fiscal algorithmic governance on the fight against tax fraud: a socio-legal perspective"* **+ Eric Marcus & Max Velthoven** *"The Philosophical Foundations of AI and their implications for science and society"* **+ Anouk Wolters** - *discussant*	**Freedom of expression** Moderator: José van Dijck **+ Emma A. Imparato** *"The suspension of freedom of information and new digital technologies during the emergency"* **+ Claudia Marchese** *"New technologies and online public discourse: what form of control by public and private actors in emergency contexts?"* **+ Giacomo Giorgini Pignatiello** *"Freedom of Expression, Technology, and Anti-Hate Speech Laws in Times of Emergencies: A Comparative Constitutional Law Analysis of Hungary and Romania"* **+ Giulio Santini** *"Platform Democracy or Return to Patrimonialism?"* **+ Mathilde Sanders & José van Dijck** *"Decentralized online social networks: A taxonomy of technological and organizational choices to embed public values"*	**Governance of technology** Moderator: Maria Lorena Flores Rojas **+ Anieke Kranenburg** *"Designing institutions for Emerging Technologies: Towards a heuristic model"* **+ Arno Laeven & Tina van der Linden** *"Decentralisation as a Design Parameter for a Public Digital Infrastructure"* **+ Alessia Zornetta** *"Towards a Quantum-Safe Global Encryption Policy: Challenges and Solutions"* **+ Francesca Niola** *"Digital democracy reimagined: navigating the intersection of innovation, governance, and accountability"*

	1. VALUES TRACK (BALZAAL)	2. REGULATORY COMPLIANCE TRACK ('S JACOBZAAL)	3. GOVERNANCE TRACK (SOETESALON)
14.05 - 15.20	**(Un)Biased AI in public governance** Moderator: Merel Noorman **+ Merijn Bruijnes** *"Developing a Workable AI Ethics Process at the Netherlands Police"* **+ Isabelle C. Fest** *"Values? Camera? Action!"* **+ Corso Tozzi Martelli** *"Ensuring accountability and reliability in the implementation of AI in the decision-making processes of public administrations"* **+ Stefano Rossa** *"Notes on the juridical regulation of predictive policing algorithms: disruptive technology vs. emerging rights risk"*	**Global perspectives on regulation** Moderator: Johan Wolswinkel **+ Davide Clementi** *"Who controls data rules All under Heaven": Chinese data regulation between State interventionism and Shanghai Data Exchange model"* **+ Virga Dwi Efendi & Haryo Putro Dirgantoro** *"Navigating the Crossroads: Data Privacy, Security, and Responsible AI Implementation in Indonesia"* **+ Madhav Shankar** *"Incorporating Human Centric Design into Algorithmic Governance: Lessons From Past Experiences"* **+ Katarzyna Łakomiec** *"Necessity - an underutilized tool in the regulation of new technologies"* **+ Manuel Protasio** *"Rethinking public acceptance mechanisms for emerging technologies and regulatory efficiency in the EU"*	**Governance by technology** Moderator: Evrim Tan **+ Anja Gjærum** *"Digitalization in rural municipalities - the role of suppliers"* **+ Maarten Bouwmeester** *"Disentangling digital welfare dystopia: Towards a general understanding of system failures in social security enforcement"* **+Bárbara da Rosa Lazarotto** *"The Role of Technology in Citizens' Right to Good Administration: Examining the Impact of Smart Governments"* **+ Lucas Haitsma, Barbara Brink & Elliot Mayhew** *"Searching for Complementarity: A Comprehensive Literature Review of Human Intervention in (Semi-)Automated Administrative Decision-Making"* **+ Sajal Sharma** *"The legal implications of the use of Artificial intelligence by public actors: The common global challenges related to trust, transparency and accountability"*

	1. VALUES TRACK (BALZAAL)	2. REGULATORY COMPLIANCE TRACK ('S JACOBZAAL)	3. GOVERNANCE TRACK (SOETESALON)
15.40 - 16.55	**Public values under pressure** Moderator: Wessel Reijers **+ Tony Giorgio** *"Remote voting and elective assemblies: the functioning of Parliaments during the emergency"* **+ Laurens Gijsbers** *"The public value of local energy systems"* **+ Banu Buruk** *"Ethical Evaluation of Risk-Benefit Analysis Approaches to AI by Different Stakeholders"* **+ Joséphine Sangaré** *"The Malabo Convention and Public-Private Partnerships – A New Route to Due Diligence?"* **+ Marc-Olivier Busslinger** *"Trust in chatbots and AI on Swiss government platforms - are the current terms of use sufficient?"*	**Ex-ante approaches to regulation** Moderator: Janneke Gerards **+ Éric Pardoux & Angeliki Kerasidou** *"Artificial Intelligence and Compliance by Design in Healthcare"* **+ Kostina Prifti, Claudio Novelli, Jessica Morley & Luciano Floridi** *"Rethinking regulation by design"* **+Georgios Bouchagiar** *"A Fundamental Rights Impact Assessment for DLT-programmes targeted at the public sphere"* **+ Charlotte van Oirsouw** *"Networked algorithmic administrative decision-making"* **+ Julia Iunes** *"The need for responsible use of artificial intelligence by the Public Administration: Algorithmic Impact Assessments (AIA) as instruments for accountability and social control"*	**Governance by and of technology** Moderator: Barbara Prainsack **+ Fulvia Abbondante** *"Utopian Visions, Dystopian Concerns, and the Legal Realities of Blockchain and AI"* **+ Milana Pisaric** *"Privatization of criminal investigation"* **+ Zelin Li** *"Heading to Resemblance? The Redress Mechanisms in the Personal Data Protection Policies of International Organizations"* **+ Giuseppe Naglieri** *"From the Denationalisation of Money to the Central Bank Digital Currencies: a comparative analysis of a new monetary instrument"* **+ Giulia Sulpizi** *"Political parties dealing with digitalization: campaigning rules and electoral process as fields of cooperation between public and private actors"*

1. VALUES TRACK

(BALZAAL)

9.30 – 10.45 Public tech: values, valuation, and evaluation

Whose values? Exploring productively disruptive interventions in tech policy for more inclusive public values

Aviva de Groot

It is a long-standing tradition in law and legal research to respond to perceived technological novelty and (potential) social disruption: to start from technological trouble that threatens a status quo. Not all analyses lead to the conclusion that new rules are needed. Some call attention to technology laws' pre-existing affordances or ability to deal with the perceived challenges; others negate the usefulness of a technology-oriented response to the identified problems. What scholars tend to agree on, however, are the public values that law is there to safeguard, including its own existence and its organisation of several kinds of public institutions such as branches of law-making and adjudication.

However, this agreement also safeguards something else, which is a continuation of law and legal research that does not seriously challenge the status quo in the governance of technologies wherein the values of large groups of people continue to be under-served and marginalised. Although these publics also bear the brunt of technological novelties, for them this does not so much amount to social disruption as to increasingly fine-tuned exacerbations of pre-existing social injustices.

Starting from their experiences of technologies and under regimes that claim to uphold public values amounts to a fundamentally different approach to technology regulation and research. This way of 'starting from the trouble' perceives the roles and histories of law and technological development as intertwined and asks different questions. Not: how are our public values threatened, but whose values, and which legal approaches have functioned in alliance with the disproportionate negative technological experience of some groups over others?
Historical studies of technological and legal fields are productively cross-examined to answer such questions. The next step entails to ask which legal and technological disruptions would be necessary to change the status quo. This contribution introduces three research interventions: three policy-level collaborations in a field of health care, public administration, and technological risk assessment that aim to answer such a question with regard to the transparency related 'public values' of explanation and justification.

From values to valuation, and from public values to common goods: a brief reflection on valuable tech development

Gijs van Maanen

From various angles, disciplines, and theoretical frameworks have scholars been arguing for better, different, and more valuable forms of technology development. Often, references are made to the importance of grounding such better forms of development in public or common values. Often, and simultaneously, the meaning of such claims are far from clear and obvious. In this contribution, four different approaches to the question (or questions) of how to understand valuable tech development are discussed as a means to give some conceptual

clarity with respect to how value-oriented approaches contribute to valuable tech governance.

First, it discusses contributions made within the realm of public administration to so-called 'public value' theory. Historically, public value theory responded to the dominance of New Public Management and the related market and commerce-oriented valuation of public policy. It tried and still tries to do this by identifying specific public values as normative yardstick for policy evaluation.

Second, from the perspective of (institutional) economics, the notions of public and common goods are introduced. While public values and public goods look alike, they are different theoretical constructs invented for different purposes and hence not to be confused with the values put forward in other scholarly disciplines. Rather than a normative aim or goal to strive towards, do economists use the identification of particular goods to determine the type of governance most appropriate for the good in question.

Third, instead of starting with the analysis of the characteristics of economic goods, political and legal theorists use the interests of groups of human beings - e.g. publics and commons - when thinking about how to determine and construct the values that should help govern society. Instead of the careful analysis of the features of e.g. private, public, and common goods, does the identification and delineation of 'publics', 'demos', and 'commons' take center stage in this strand of the literature.

In the last approach discussed, by contrast, the specific problems or issues that force us scholars into thinking about the supposed public or common nature of good tech development take priority. Instead of trying to analyse this question either through grounding it in the supposed existence of a group of (affected) individuals with a particular interests, or through the establishment of the (public) values that are supposed to be important for guiding public policy, researchers in science and technology studies (STS) take the issues and problems technologies present as the starting point of their analysis. The advantage of taking such problems as key in analyses of technology development is that many of the often abstract and almost impossible to answer questions about the status, nature, and value of the publics and their related values, are partly answered through one's careful analysis of specific problems in question. How such a problem or issue-oriented approach to valuable tech development could look like in practice, is exemplified with the help of research done on digital water governance in the province of Brabant.

Realising a blockchain solution without blockchain? Blockchain, solutionism, and trust

Gert Meyers

Blockchain is employed as a technology holding a solutionist promise, while at the same time, it is hard for the promissory blockchain applications to become realised. Not only is the blockchain protocol itself not foolproof, but when we move from "blockchain in general" to "blockchain in particular," we see that new governance structures and ways of collaborating need to be developed to make blockchain applications work/become real. The qualities ascribed to (blockchain) technology in abstracto are not to be taken for granted in blockchain applications in concreto. The problem of trust, therefore, does not become redundant simply through the employment of "trustless" blockchain technology. Rather, on different levels, new trust relations have to be constituted. In this article, we argue that blockchain is a productive force, even if it does not solve the problem of trust, and sometimes regardless of blockchain technology not implemented after all. The values that underpin this seemingly "trustless technology" such as control, efficiency, and privacy and the story that is told

about these values co-shape the actions of stakeholders and, to a certain extent, pre-sort the path of application development. We will illustrate this by presenting a case study on the Red Button (De Rode Knop), a Dutch pilot to develop a blockchain-based solution that enables people who are in debt to communicate to their creditors that they are, together with the municipality, working on improving their situation, thereby requesting a temporary suspension from debt collection.

Explaining the current state of experimentation with automated decision-making (ADS) in Dutch healthcare - an institutional analysis

Jolien van de Sande

In the Netherlands, there has been a shift towards the use of automated decision-making systems (ADS) in the health domain with increasing reliance on born-digital data. Algorithmic technologies are used for tracking practices, inputs, and outcomes in order to predict risk, aid decision-making, and track professionals within the healthcare domain itself to make more efficient use of people and resources. This development has been frequently heralded by politicians and policymakers, as a way to deal with the grand challenge of ensuring future public accessibility of healthcare in light of scarcity of personnel and finances. Despite these promises, scholars also point to possible unintended consequences of the application of ADS which can negatively affect public values such as healthcare quality, equity, and public trust.

Experimentation in specific healthcare practices is perceived as necessary to discover if ADS have added value compared to human intelligence. Also, this experimentation is seen as necessary to develop and improve these self-learning technologies. With this intention, healthcare providers and tech-companies increasingly collaborate to prevent technology-driven innovations that do not fit situational healthcare practices. Although policymakers, practitioners and companies find flexibility to experiment and learn important, they are also careful in applying technologies for which evidence about their usefulness and risks is inconclusive.

This paper therefore aims to explore the possibilities and impossibilities in experimentation with ADS in Dutch healthcare. The paper provides an institutional analysis of developments in politics, policy, and regulation within the healthcare domain in the past ten years to explain current tensions regarding experimentation. Through literature reviewing and interviews with different experts such as healthcare professionals, health policymakers, lawyers, and computer scientists, this paper aims to explain this difference and the current situation regarding experimentation with ADS in healthcare.

This focus is particularly relevant since regulation on ADS in healthcare is lagging behind due to its rapid advancement in the past few years. Different interpretations of what is allowed have resulted in fragmented initiatives across healthcare providers. Problems with the interoperability of systems and financing of innovation are also perceived as barriers to innovation by policymakers. We found that collecting so-called ‘real-world-evidence’ has gradually become common practice as a prerequisite for conditional reimbursement of expensive drugs when health technology assessment (HTA) is difficult. Although similar public values are at stake, we also found that regulation is different (in some cases more and in other cases less restrictive) when it comes to technological innovation in healthcare. We analyse this contradiction in the paper by highlighting distinctive characteristics of ADS compared to drugs and other in-patient and out-patient technologies beyond ADS.

11.05 - 12.20 The philosophy of AI

The impact of fiscal algorithmic governance on the fight against tax fraud: a socio-legal perspective

David Hadwick

Unbeknownst to most, tax administrations have been pioneers of algorithmic governance, exhibiting the highest level of digital maturity among public actors and using AI technology for the longest time. Prior studies show that in the EU, at least 21 Member States make daily use of machine learning in the exercise of fiscal prerogatives. In certain areas of taxation, most notably to combat VAT carousel fraud, machine learning is used by all EU Member States. The use of AI systems catalyzed the most profound structural reform for tax administrations, namely the shift from local selection of taxpayers for audit by field agents to a centralized statistical selection. In that regard, tax administrations as a case study offer a uniquely advanced perspective on the balance of risks and benefits associated with the use of AI systems by public actors. Counterintuitively, despite scandals such as the *toeslagenaffaire*, taxpayers perceive the use of data-driven algorithms as fairer because of its uniformity, and its ability to reduce corruption and human cognitive bias. On the other hand, field agents view the use of AI rather negatively, fearing human replacement and lower agency or discretion for individual tax officials. Following qualitative interviews with tax officials in the EU, this paper shows that the individuals impacted by algorithmic governance extend beyond the subjects of an algorithm, but also include controllers who must now follow the output of predictive models. In doing so, the author hopes to spark a discussion on whether more digitalization is always desirable. Studies and scandals such as the Panama and Pandora Papers, show that the largest bulks of tax frauds is the result of profit shifted to non-cooperative jurisdictions, over which data is by definition purposefully not available. In a data-driven paradigm, these types of fraudulent schemes are likely to continue to escape the scope of tax administrations. These schemes were systematically discovered through traditional forensics accounting by investigative journalists and human tax officials. Making parallels with Popper and Deustch's views on AI and *Bayesiansism*, in tax enforcement only human discretion has been capable of generating new predictive knowledge. Accordingly, as opposed to public perception of fiscal AI systems, a data-driven paradigm may exacerbate unfair taxation by continuing to enable the ability of certain taxpayers to perpetuate international tax evasion.

The question guiding this research is: *"how has the digital transformation of the tax administrations impacted tax officials in the fight against tax fraud?"* Section 1 outlines the historical evolution of the state of use of AI by tax administrations, the typology of functions leveraged and their impacts on taxpayer selection for audit. Section 2 presents the internal perspective of tax officials and whether they perceive AI as the most appropriate means to combat tax evasion. The paper concludes by showing the rather unique balance of risks and benefits of the use of AI by tax administrations, to spark further discussion on its legitimacy as digital governance tool.

Problems in AI, their roots in philosophy, and implications for science and society

Eric Marcus & Max Velthoven

Artificial Intelligence (AI) is one of the hottest topics of the moment. Specialized applications of AI continue to expand and improve, making AI also increasingly relevant as an emergent technology for public governance. Forms of AI are already being used by public entities such as tax authorities and the police. Whilst the fruits of AI are warmly received, there needs to

be more attention to the philosophical foundations of current AI technology. This deficit is combined with philosophical misconceptions about the growth of knowledge. Unfortunately, this is not merely a philosophical problem. In this paper, the authors outline why these deficits in knowledge form a real problem with implications for science and society (including public governance).

This paper refers to the work of the philosopher of science Karl Popper and physicist/computer scientist David Deutsch. Part of their work is aimed against mistaken theories of knowledge such as inductivism, empiricism, and instrumentalism, or in today's more fashionable term: Bayesianism. This paper shows that these ideas are still very much alive in current AI technologies and the (public) discourse on these technologies. With reference to Popper/Deutsch, this paper argues that these views are based on a mistaken philosophy. This paper, therefore, concludes that current AI research/philosophy is based on outdated and refuted theories of knowledge. Identifying such deficits is an important task of philosophy: pointing out what we do not know and why this results in problems.

Despite the philosophical problems underlying AI, authors recognize the potential of AI to bring significant contributions in many areas, including public governance. This potential makes it even more important to have sufficient awareness of how current AI works and what it can and cannot do. Consequently, more efforts should be made to inform stakeholders involved in AI (including the public) of the philosophical deficits of current AI technology. A failure to do so could result in various adverse consequences, such as a wrong use of technology, lack of accountability/transparency, discrimination, and a mismanagement of expectations. Specifically, a misunderstanding of the underlying mechanism of knowledge creation can result in poor regulation and governance strategies.

In the authors' view, the following three propositions should be considered when AI is brought into the context of public governance:
1. Information created by current AI is not new 'knowledge' as created by humans: humans remain at the 'creative steering wheel'. AI is an instrument, not a source of wisdom.
2. From the first point it follows that current AI cannot generate truly new explanations, whereas humans can. An important implication hereof is that human actors should continue to bear the ultimate responsibility to explain the application of AI. This will include cases in which AI is successfully used as an instrument even though its operation itself cannot be explained.
3. Progress in current AI may result in specialized applications of AI that bring great benefits to society. However, there is no reason to believe that further development of current AI technologies will result in the creation of an AI that is truly on par with human intelligence (also called Artificial General Intelligence (AGI)). In fact, current AI is actively moving away from realizing AGI.

14.05-15.20 (Un)Biased AI in public governance

Developing a Workable AI Ethics Process at the Netherlands Police

Merijn Bruijnes

The Netherlands Police is adapting to the developments in our digital society, and the resulting digitization of criminal activity, by "acquiring the right people, resources and innovations" (van der Plas, 2022). These "right people" tend to be data scientists or software developers who have the technical expertise to create and apply algorithms to handle digital data. For instance, they secure and analyze (big) digital datasets to find those data points that are related to potential criminal activity. Building and using the tools for data analyses comes with potential ethical challenges when conflicts of values are observed. A prime example is the tension between privacy and security that exists with algorithms and artificial intelligence (AI) in the policing domain. Dealing with ethics is not the core expertise of a data scientist or developer, yet their (technical) choices are pivotal for the outcome and impact of their work. In this paper, we present the perspective of these technologically minded screen-level bureaucrats on AI ethics, their experiences in dealing with value conflicts, and their view on the governance of AI ethics. We share insights from semi-structured interviews with these "right people" and place their experiences in the context of the Police's efforts to codify and (in)formalize the process of ethical considerations (e.g., OM and Politie, 2020; Gerards et al., 2021). Our insights will be used in the development of AI ethics procedures and resources for the Police, where we aim for practical and workable ethics procedures for data scientists and developers, and as such hope to contribute to the ethical development and use of AI at the Netherlands Police. As such, this recommendation points towards governing the development of technology where values, trust and compliance are by design secured in the process of the organization.

Values? Camera? Action!

Isabelle C. Fest

Police departments around the world implement algorithmic systems to enhance various policing tasks. Ensuring such innovations take place responsibly – with public values safeguarded – is essential for public organizations. This paper analyzes how public values are safeguarded in the case of MONOcam, an algorithmic camera system designed and used by the Netherlands police. The system employs artificial intelligence to detect whether car drivers are holding a mobile device. MONOcam can be considered a good practice when it comes to value-sensitive design; many measures were taken to safeguard public values in this algorithmic system. In pursuit of responsible implementation of algorithms, most calls and literature focus on such value-sensitive design. Much less attention is paid to what happens beyond design. Building on 120+ hours of ethnographic observations as well as informal conversations and three semi-structured interviews, this research shows that public values deemed safeguarded in design are re-negotiated as the system is implemented and used in practice. This paper thus highlights that algorithmic system design is often based on an ideal world, but it is in the complexities and fuzzy realities of everyday professional routines and sociomaterial reality that these systems are enacted, and public values are renegotiated in the use of 'algorithms'. While value-sensitive design is important, this paper shows that it offers no guarantees for safeguarding public values in practice.

Ensuring accountability and reliability in the implementation of AI in the decision-making processes of public administrations

Corso Tozzi Martelli

Artificial Intelligence (AI) has transformed various aspects of our lives, enabling algorithm and computer to perform tasks traditionally carried out by humans. So, the public sector has also been affected by this transformation.
AI can enhance decision-making by analyzing big data and identifying patterns and trends that might go unnoticed by humans. This empowers policymakers with valuable insights for informed decision-making. Moreover, AI can personalize public services by utilizing large quantities of data to tailor services to the specific needs of individuals, thus strengthening administrative action.

While the benefits of AI in public administration are significant, it is essential to address the challenges and risks associated with its implementation. Data privacy is a major concern, as the use of AI involves processing large amounts of personal data. Safeguarding individuals' privacy and ensuring compliance with relevant regulations is crucial. Algorithmic bias is another challenge, as AI systems can only reflect the data on which they are trained. Care must be taken to prevent biased outcomes that could perpetuate discrimination or disadvantage certain groups. Additionally, the need for human oversight and interpretability of AI decisions is paramount, particularly when these decisions have a direct impact on the lives of citizens.

Transparency plays a pivotal role in implementing AI in public administration. Public administrations must disclose their use of AI systems, both in the preliminary and decision-making phases of procedures. Adequate justification for administrative decisions based on algorithmic systems is necessary to ensure transparency and clarity of responsibility.

The "black box" challenge, which arises from the difficulty in tracing the decision-making process of an algorithm, must be addressed. Providing clear and comprehensive motivations for automated decisions helps build trust and accountability.
While AI can automate various administrative tasks, it is important to recognize that discretionary activities, where human judgment and interpretation are required, cannot be fully delegated to AI systems. Human decision-makers play a crucial role in ensuring the validity and accountability of the decision. The principle of non-exclusivity of algorithmic decisions emphasizes the need for human involvement in validating, rejecting, or checking automated decisions. This preserves the imputability of the decision and promotes a fair and ethical decision-making process.

In conclusion, the implementation of AI in public administration offers tremendous potential to enhance efficiency, decision-making, and public service delivery. However, it is crucial to address the challenges and risks associated with AI, such as the need for transparency and human oversight. By prioritizing transparency, accountability, and responsible data governance, public administrations can harness the benefits of AI while ensuring the protection of individuals' rights and maintaining public trust.

Notes on the juridical regulation of predictive policing algorithms: disruptive technology vs. emerging rights risk

Stefano Rossa

In Beck's current risk society, characterised by uncertainty, the State is faced with a dilemma. To fail before the risk but to keep the sphere of citizens' rights intact; or not to fail before the risk but to restrict fundamental rights? This payoff turns out to be the main issue that juridical reflections on the use of predictive technology tools in the public sector must consider.

Policing is an administrative function exercised by the State to protect public safety and citizens' rights, through the maintenance of public order. This activity is mainly composed of acts of a preventive nature, which disregard the commission of the criminal fact and are aimed at identifying social dangerousness for the commission of future criminal conduct.

By using ICT, it is possible to optimise the exercise of administrative functions, especially the policing one. It is possible to employ AI systems capable of preventing the occurrence of the fact with a very high rate of certainty that can "predict" the future: software of predictive policing, capable of identifying the possible future crime scene as well as, in some cases, the possible future criminal actors.

The reasons why predictive policing software could harm individuals' fundamental rights can be basically traced to: false perception of the algorithm's neutrality; black box problem; presence of bias in the algorithm's operating data; risk of the algorithm's non-accuracy resulting from the non-accuracy in the dataset; possibility of the algorithm being used in a biased manner with respect to the purpose set; improper functioning of administrative power.

Beyond these critical aspects, it is undeniable that the high level of digital processing of big data could bring enormous advantages in terms of functionality and effectiveness of the analysis activity. Which conducts to the conclusion that the use of predictive policing tools is as effective on a technical level (with the limitations just underlined) as it is dangerous for the guarantee of the individual fundamental rights.

But is it possible to combine the use of such predictive systems with the protection of fundamental rights? One answer could be to argue the need for the software algorithm to be transparent, allowing the right of access to the source code and the learning dataset. This aspect, however, could frustrate the rationale of predictive policing to ensure public safety.

Although the Proposal for an EU Regulation on AI prohibits the use of algorithms to carry out pre-crime remote biometric identification, Article 27 of Directive (EU) 2016/680 allows it, requiring, however, that the predictive policing system be subject to an impact assessment concerning the approach of the specific risk of the processing of personal data on the fundamental rights of the individuals concerned.

Notwithstanding this, the paper will investigate possible juridical principles, some of which are expressed in leading cases (f.i. Supreme Court of Wisconsin, State of Wisconsin v. Eric Loomis, 2016; Bundesverfassungsgericht, decision, 16 February 2023) that can enable the use of such instruments, enjoying the positive effects, reducing the risk of fundamental rights infringement.

15.40-16.55 Public Values under pressure

Remote voting and elective assemblies: the functioning of Parliaments during the emergency

Tony Giorgio

Technological evolution, which is making great strides in a large part of the world, has inevitably invested the political field as well, where "anytime, anywhere" voting is finding fertile ground even in the States with the oldest democratic tradition.

Nowadays, the classic voting methods, which have taken root over time, no longer represent the only "viable ways". The electronic vote, favored by the strong technological progress still underway, acquires an ever-increasing importance; like the traditional vote, the digital one, in order to be considered democratic, has to necessarily take place within a perimeter of certain principles and international standards (such as, above all, transparency, control, responsibility, reliability and security).

Particularly lively, in the last few years, is the international political debate about the opportunity to increase the use of electronic instruments to give expression to the popular will, also fueled by the recent accessibility to systems that make possible the "simultaneous presence" in different places and situations. The dispute, which at first was restricted solely to the question of "elective" electronic voting, currently includes "deliberative" e-voting as well.

The discussion in question, long relegated to the academic environment, has undergone a sharp acceleration with the outbreak of the Covid-19 pandemic, also involving the parliamentary institutions, whose normal functioning has been upset by the health crisis.

The paper focuses on the analysis of e-voting and its use at the systemic level, conducted through the comparison between the Italian reality and the most significant European experiences which, to date, have developed (or effectively started) or not virtualization processes of internal procedures, both as regards the conduct of online debates and for the more complex implementation of remote voting.

One must be aware technology will take on an increasingly important function in the daily lives of every individual, especially because of the virus. The state of emergency proclaimed in most countries, following the spread of the contagion, has heavily influenced the performance of public activities. If citizens were bound to comply the containment measures against Coronavirus, with the obligation to remain in their homes, the Parliaments, in turn, have had to modify the ordinary modes of operation and carrying out their work in order to adapt them to a new and unprecedented scenario, finding themselves forced, however, at the same time, to cede to the Governments considerably extended spaces of intervention.

Together with the study of the respective legal cases, the opportunities and criticalities of home voting are also highlighted, a tool that represents one of the meeting points of an increasingly topical and treated binomial: law and technology.

This comparison allows to investigate how the various solutions adopted have affected, on the one hand, the operativeness of the body as a whole and, on the other hand, the exercise of the prerogatives of single representatives, and to reflect on the legitimacy, as well as on

the usefulness, of introducing or not modalities of remote participation, now and in the future.

The public value of local energy systems

Laurens Gijsbers

In the future energy system, according to the national energy system plan, but also scenario studies from the living environment planning agency (PBL), there will be an important role for decentralized solutions and local energy systems where generation from sustainable energy sources and energy use are more directly linked in terms of time and place.

Smart energy hubs, smart grids, smart solutions, and the smart sharing of energy sources and energy carriers are presented as tools to contribute to the development of the energy system of the future The development of so-called energy hubs and energy communities is currently taking place on industrial estates and within residential areas. Energy hubs and energy communities are geographically defined and are mainly independent and one-off projects on an industrial estate and/or residential area. At the same time, an energy hub or energy community cannot be viewed in isolation and develops among various actors and institutions at various scales. It requires cooperation between the government, public and private parties and the collective of citizens and companies. This collaboration presents an opportunity for social and political changes with regard to the energy system and the development of decentralized solutions.

The public values regarding energy such as availability, accessibility and affordability are a public good, motivating forms of publicly organized governance. At the same time is the generation, transport and use of energy through physical and virtual components a private good, requiring more private forms of governance. These differences with respect to both the kinds of values are present in local energy solutions, and the goods with which they are related, complicate the governance mechanisms to be put in place for the just and democratic governance of the Dutch energy system. What kind of rules are appropriate for what kind of solutions, to be developed at which level? How decentralized or independent are and can local smart energy hubs be? How do energy communities relate themselves to the Dutch energy system in general? And how to make sure that the smart solutions invented on a privately owned industrial estate, do not infringe upon the quality of energy services delivered elsewhere?

This PhD project investigates how the desired situation, a robust energy system with mostly local systems, can be achieved. Based on four case-studies, it does research on governance of these systems, the interaction between local systems with a polycentric character and national structures and public values. This makes it an exploratory study and will methodologically at its core consist of empirical research into actors, public values and the institutional design of managing a local energy system within national structures.

Ethical Evaluation of Risk-Benefit Analysis Approaches to AI by Different Stakeholders

Banu Buruk

There exist various potential sources of harm attributable to artificial intelligence (AI) that have implications for the entities engaged in its development, the individuals who utilize this technology, and the regulatory bodies authorizing its deployment. To elucidate, the perspectives of users and companies concerning the comprehension of concepts like risk-benefit inherently diverge. Companies primarily scrutinize the advantages conferred, asking whether these benefits can be monetized. In contrast, users appraise these benefits in the context of personal gain, pondering what utility they stand to derive. This divergence emanates from the distinct vantage points occupied by the company (often viewing users as data sources) and the position assumed by users themselves. Companies developing AI often convey to users that they are collectively shaping these benefits. Nevertheless, it would be imprecise to assert that users engage in data altruism consciously; they are cognizant of data sharing but lack comprehensive awareness of the specific data being divulged.

In the interview titled "Risks and How AI Will Reshape Society" conducted by Rebecca Jarvis of ABC News with OpenAI CEO Sam Altman, he remarked, *"I think people should be happy that we are a little bit scared of this."* This statement underscores the inability of AI developers to fully apprehend the ethical quandary that underlies the benefit-risk analysis. This deterministic approach among AI technology developers signifies their inclination to regard AI as an autonomous entity advancing independently. Furthermore, instances such as the seven-month collaboration between the CEO and CTO with the government prior to the introduction of ChatGPT seem to reflect a strategic maneuver for self-preservation rather than a genuine ethical concern. Consequently, users who encounter this information and peruse the aforementioned interview come to a realization regarding the necessity to safeguard their interests.

Our individual stances on existential issues linked to AI closely mirror our positions on analogous life-altering problems. For example, in mitigating environmental crises, we adopt precautionary measures that we believe possess significant personal and collective impact, such as curtailing or discontinuing the use of plastic straws. Concerning existential AI-related issues, users tend to take precautions to safeguard their personal data. However, the intricate task of ascertaining reasonable harm inflicted by AI presents considerable challenges. Establishing the precise magnitude and nature of harm in an AI utilization context may prove elusive. Therefore, the delineation of what constitutes reasonable harm for AI users remains multifaceted, with each user embodying a unique perspective. The vast diversity in the definition of reasonable harm compels companies and collaborating regulatory bodies to primarily rely on the deterministic paradigms upheld by these enterprises.

This research aims to expound upon the distinctions, origins, and ramifications of risk-benefit assessments related to AI as perceived by different stakeholders. The potential harms stemming from AI, as perceived by each stakeholder, will be categorized into two principal domains: personal harms and paradigm shift harms, with an overarching ethical evaluation within the framework of public values, trust, and compliance parameters.

The Malabo Convention and Public-Private Partnerships – A New Route to Due Diligence?

Joséphine Sangaré

The information era has brought an ontological fight over information centralisation vs. information freedom. While states have formed opposing interest groups, private actors have risen to unprecedented importance in the determination of international relations. Most cyber capacity is located in the private sector and a focus on infrastructure privatisation over the past decades has left many states with less cyber capacity. Dedicated UN bodies, the European Union, and the African Union have therefore called upon states to engage in public-private partnerships (PPPs) as a means of cyber capacity building. This paper explores opportunities of diligent state cyber capacity building applying implementing the institutional measures of the 2014 Malabo Convention. PPPs are characterised by a long-term contractual relationship between the procuring authority and a private entity and fall within the regulatory framework of public procurement procedures. PPPs are subject to risk-assessment aimed at transparency and fiscal efficiency. However, these risk-assessment frameworks do not entail assessment towards the protection of infrastructure integrity. Infrastructure integrity in this context is defined as the operation of a state's public cyber infrastructure in accordance with that state's position on information protection, i.e., information security or information freedom. Particularly, where a state procures information and communication technology from a private actor originating from a third state, and where this private actor is a state-owned or state-affiliated company of that third state, there is a substantial risk for transboundary harm through foreign interference.

The African Union Convention on Cybersecurity and Personal Data Protection (2014 – Malabo Convention) offers a starting point by emphasising the necessity of government leadership in public- private partnership procurement in Chapter III. Previous examples of ICTs procurement in the case of AI-based technology for law enforcement purposes in African states have raised concerns towards potential espionage and a recognisable shift in ICTs law-making processes in favour of the private actor's origin state's position on access to information. Starting from due diligence and the obligation to prevent harm, I aim to explore to how due diligence obligations can or cannot create accountability for harm caused by unsolicited intervention into ICTs infrastructure by a foreign private actor in a public-private partnership. Connecting the scholarly discourse on due diligence in cyberspace with the debate on adequate risk assessment in public procurement of information and communication technologies, I ask about the potential of the Malabo Convention to mitigate the risk of foreign interference and the risk of limiting information freedom through public-private partnerships.

Trust in chatbots and AI on Swiss government platforms -are the current terms of use sufficient?

Marc-Olivier Busslinger

Chatbots are a relatively new technology that use artificial intelligence (AI) to best answer questions and provide answers to the public. If chatbots aren't newin the private sector, their use isn't widespread in public services. These systems are being used to answer questions from the public, facilitate access to official information or even provide personalised advice.
Private websites and platformspublish their termsof use online. These documents, of a contractual nature, govern the relationship between the usersand the websites. Theircontent includesthe responsibilities of the different actors, data protection informationor norms, and procedures forsettlingdisputesbetween the parties. Some argue that these texts contribute to building and maintaining of trust fromthe public.
Trust is often presented as necessary for the public acceptance of e-government1 systems. The same type of terms and conditionsare present on the public platforms and websites that usechatbot systems. Asthese websites are governed by public law and perform official governmentfunctions, these texts shouldn'tbe of a contractual origin.Moreover, they arenotpublished in the same way as other public law instruments.
This contribution has three objectives. First,it will analyse the use of chatbotsand AI public services on government platforms open to the public, focusingon the legal implications of their use andimplementation. Second, it will explorethe place of the public terms and conditions implemented around these chatbots in the legal system and to analyse their legal status. Third, it will question the influence that these texts, as currently drafted, have on trust and on the acceptance of public chatbots and AI,and more broadly in digitised government systems.
In order to provide a practice-oriented analysis, we decided to limit the scope of this case study toterms and conditions on Swiss government websites only. Indeed, most Swiss public websites generally contain broad disclaimers, the legality of which we wish to question.More specifically, this paper analysesthe terms and conditions of selected public chatbots and AI systems. Most of thetextspresent on administrative or specialised websites and e-government platforms oftenexclude any responsibility of the authorities for the information they publish onlineand for the use of these systems.

This paper argues that Swiss governmentauthoritiesdon't meet the requirements of Swiss public lawin the 'terms of use'of their chatbots and public AI systems.More worryingly,from an ethical point of view, by refusing accountability for the use of these systems, they participate in a climate of mistrust that couldhinder society'sacceptanceofthe state'sdigitisation effortsand e-government services.

2. REGULATORY COMPLIANCE TRACK

('S JACOBZAAL)

9.20-10.45 Regulating emerging technologies

Engineering the fiduciary

Bao Chau

This Commentary seeks to expand on current legal proposals attempting to regulate BigTech. American scholars and politicians of all stripes, for example, have called for a revision of Section 230 of the Communications Decency Act of 1996 (CDA) and/or for the implementation of some sort of must-carry provision to protect the American conception of freedom of speech. Similarly, the EU has now passed two landmark legislations – the Digital Markets Act (DMA) and the Digital Services Act (DSA) – which aim to protect "fundamental rights of users and ensures a level playing field for businesses."

At the heart of these proposed and enacted regulations is an attempt to regulate the integration of algorithmic systems into our everyday lives. Because these regulations primarily focus on machine learning (ML) algorithms like ChatGPT's deep learning algorithms, however, they often fail to consider the impact of rule-based, non-ML computer code. The American Equal Employment Opportunity Commission (EEOC), for example, have issued guidelines to ensure compliance with the Americans with Disability Act (ADA) in algorithmic decision-making systems. Unfortunately, these guidelines mostly focus on a particular subset of algorithms that use ML to make employment decisions (e.g., using chatbot to filter out users with disability-related employment gaps). Ordinary digital tools and algorithms remain an afterthought. This is problematic because algorithmic bias in the software scaffolding — non-ML code responsible for collecting and supplying data to the ML models — could contaminate the entire system and produce discriminatory results even if the data and ML models were fair and equitable.

To address this regulatory blind spot, this Commentary discusses the scope of current algorithmic governance frameworks such as the Biden's Blueprint for an AI Bill of Rights, the EU AI Act, and the Chinese Algorithm Recommendation for Internet Information Services. It recommends expanding the regulatory purview to include both rule-based and machine learning algorithms. The Commentary suggests that this expansion will help to further dispel the myth of algorithmic idealism and address the issue of algorithmic bias. In particular, the Commentary contends that the Agile Software Development process does not produce algorithmically neutral code, and top-down proposals of external regulation do not fully address the harm of rule-based algorithms. Therefore, it is beneficial to explore bottom-up regulatory solutions, such as the promulgation and enforcement of a code of ethics for the software engineering profession.

The Regulatory Sandbox and the Cybersecurity Challenge: from the Artificial Intelligence Act to the Cyber Resilience Act

Filippo Bagni

The article carries out an analysis of the innovative tool known as "regulatory sandbox", investigating its specific features in both abstract and concrete terms through the investigation of relevant European use cases. Through the analysis of the application of the regulatory sandbox in the specific field of the regulation of artificial intelligence, with

particular reference to the discipline envisaged by the European regulation proposal called "Artificial Intelligence Act", the article aims to verify the possible applications and implications of this instrument also in the field of cybersecurity, with a specific focus on the recent European regulation proposal still under negotiation called "Cyber Resilience Act".

Apparent decentralization and trust in blockchain based organizations

Benedetta Venturato

The paper builds on the scholars' reflection on trust and confidence in distributed ledger technologies to further develop it by defining and analysing the phenomenon of apparent decentralization in blockchain-based organizations, through the analysis of cases emerged (and in some instances recently prosecuted) in the United States. It is, in fact, claimed that blockchain technology should be regarded not so much as a "trustless technology" but rather as a "confidence machine", because it creates shared expectations with regard to the manner in which it operates, and the procedural correctness of its operations (De Filippi). However, as noted by the same authoritative scholars, even public and permissionless blockchains rely on a particular type of "distributed trust". The paper identifies and analyses three main factors posing significant challenges to the reliability of DLT as a source of confidence and a basis for "distributed trust" in blockchain-based organizations and highlights the importance of addressing these challenges through regulation specifically tailored on these factors. The first threat to actual decentralization is identified in the significant and widespread information asymmetries that often characterise the participants to decentralized organizations (such as developers on the one hand and simple users having invested in utility tokens on the other hand), making it hard – or concretely impossible – for some of them to identify actual risks entailed in such participation and resulting in different levels of awareness in these participants. The second threat identified is the existence of loopholes in the current regulation, which makes most of the rules aimed at preventing conflicts of interest and abuse of powers provided for corporate law not applicable to decentralized organizations. The third threat identified is the lack of consideration – n the part of authorities and the current regulation –to the importance of ensuring compliance through protocol design in decentralized systems and to set rules on protocol design transparency to ensure adequate preventive measures are embedded in the technological infrastructure that regulated governance. The paper then suggests possible solutions to mitigate the impact of such threats through compliance y design and regulation.

Exploring the Operational Framework and Feasibility of Integrating Blockchain Technology with Legal Services for an Intellectual Property Management Platform in the Audiovisual Industry

Emily Li

The emergence of digital technology, music streaming platforms, and social media has brought revolutionary changes to the audiovisual market, disrupting traditional distribution channels and giving rise to various copyright issues. Additionally, the impact of the Covid-19 pandemic has accelerated the development of online community platforms and the ecosystem of audiovisual creators, prompting creators to offer a wide range of audiovisual works and leading to new forms of work, such as YouTubers and live streamers. This has significantly influenced the original landscape of the audiovisual industry.

Simultaneously, long-standing issues in the music industry, such as unclear authorization and revenue sharing and delayed royalty payments, remain unresolved. The evolving ecosystem of the audiovisual industry has introduced further challenges, including the inadequacy of existing agency and marketing methods for new- generation creators and studios, the need for creators to leverage secondary rights from their original content, unfair streaming platform contracts, and complex rights management organization systems. These issues underscore the structural problems in the current audiovisual industry.

This paper aims to plan an intellectual property audiovisual management platform by leveraging blockchain technology and legal service design, while incorporating rights protection and marketing elements. It takes a problem-oriented approach to explore a practical and feasible audiovisual intellectual property management platform.

11.05 - 12.20 Freedom of expression

The suspension of freedom of information and new digital technologies during the emergency

Emma A. Imparato

The principle of transparency of information is a cornerstone of accountable and democratic governance in a constitutional state. It ensures that government actions and decisions are open to public scrutiny, fostering trust and holding authorities responsible for their actions. However, in times of emergency, especially in the digital age, there is a delicate balance to be struck between transparency and safeguarding national security, public safety, and individual rights. Potential abuses of the transparency principle can emerge in several ways during emergencies in the digital age. Government overreach can lead to unwarranted surveillance, data collection, or censorship under the guise of protecting national security.

Information suppression can curtail free expression and stifle public discourse, hindering citizens' ability to access crucial information.

Moreover, the spread of disinformation and misinformation can be weaponized, causing panic and confusion. In response, governments may enact policies restricting the dissemination of information, potentially overreaching and infringing on freedom of the press and expression.

Thus, the challenge lies in maintaining the delicate equilibrium between transparency and security in the digital age during emergencies. Striking the right balance is vital to preserve the core democratic values and individual liberties that democratic constitutional states hold dear while addressing the genuine threats that crises may pose.

There is no doubt that the exponential spread of information in the recent few years has been facilitated by new digital technologies. The internet plays a crucial role in the dissemination of information. Also, during the Covid-19 pandemic, access to internet has proved how important they are for disseminating measures on how to be protected from the disease and to get the most up-to-date information about the current situation. The same Council of Europe in its document adopted on the 7 April 2020 entitled "Respecting democracy, rule of law and human rights in the framework of the COVID-19 sanitary crisis", remember to Member States that the "public's access to official information must be managed on the basis of the existing principles set down in the Court's case-law".

However, several countries interfered with the right to access to information by amending freedom of information laws or suspending the obligations of public entities to allow the public to access information in their power. Several European countries, including Spain and Italy, cited the pandemic when they relaxed or suspend deadlines for responding to freedom of information requests through a state of emergency that suspended deadlines for procedures of public sector entities.

New technologies and online public discourse: what form of control by public and private actors in emergency contexts?

Claudia Marchese

Freedom of expression, as stated by the Italian Constitutional Court in sentence no. 84 of 1969, constitutes the "cornerstone of the democratic order"" Indeed, the realization of the democratic principle is possible only through the recognition of the freedom of expression

to each individual. Freedom of expression helps to realize the democratic principle not only when the speech expresses support of the institutions, but also when it translates into the expression of criticism, political dissent and opinions that do not conform to dominant thought. This reconstruction of the freedom of expression is supported by the jurisprudence of the European Court of Human Rights, which since the Handyside v. United Kingdom decision has affirmed a duty of neutrality on the part of the State «towards the opinions expressed, both those that find consensus and those that shock, shock or disturb all or part of the population». Given this connection between freedom of expression and the democratic principle, it seems appropriate to point out how the advent of the Internet has significantly expanded the possibilities of expressing one's thoughts and contributing to the political debate. Free speech on the Internet, compared to traditional ways of expressing thoughts, presents a greater attitude for diffusion due to the attitude to reach an indeterminate audience of users and to the possibility of sharing contents published online. These characteristics could lead us to affirm that free speech on the Internet has contributed to strengthen the democracy by determining new spaces for discussion, however such a conclusion appears simplistic.

Before reaching such a conclusion, it is necessary to consider the different and numerous forms of control exercised by public and private actors over the online public discourse. These forms of control are characterized by being even more stringent in emergency contexts. Just think of the pandemic emergency or the terrorist risk. In this presentation we intend to offer a brief overview of the legislation that in the European area regulates the forms of public and private control over public discourse on the Internet and, above all, on social platforms, focusing the attention on the most stringent forms of control provided by public actors and applied by the online platform in emergency contexts in order to prevent the Internet from transforming itself into a further vector of risk for public order, security, public health and, ultimately, the State itself. Similar limitations, although based on interests of primary importance, appear likely to generate a paradox: if it is true that the Internet constitutes a very powerful tool for expressing one's thoughts, it is also true that ideas expressed online are susceptible to run into more stringent limitations implemented by both public and private actors. It is therefore necessary to identify the limits within which similar restrictions are legitimate and how far the control carried out by public and private actors can go.

Freedom of Expression, Technology, and Anti-Hate Speech Laws in Times of Emergencies: A Comparative Constitutional Law Analysis of Hungary and Romania

Giacomo Giorgini Pignatiello

The contribution investigates the intricate interplay between freedom of expression, technology, and anti-hate speech laws in the context of emergencies, with a specific focus on Hungary and Romania. Employing a comparative constitutional law perspective, this research seeks to unravel how these Eastern European countries address the complex challenges of safeguarding fundamental rights in the digital age during crisis situations.

The initial section of this study provides an in-depth analysis of the legal frameworks pertaining to freedom of expression and hate speech in Hungary and Romania. While both nations share a commitment to European values and human rights, they exhibit notable variations in their legal structures and cultural contexts. Hungary has faced significant criticism for its restrictive media laws, whereas Romania’s approach has leaned more

towards a liberal interpretation of these rights. This divergence reflects a confluence of historical legacies, political developments, and contemporary democratic norms.

The second section of this paper delves into the profound impact of technology on the dynamics of freedom of expression and hate speech. The advent of digital platforms and social media has drastically expanded the scope of public discourse, offering a dual opportunity for constructive dialogue and the propagation of virulent hate speech. This section scrutinizes how Hungary and Romania have adapted their legal frameworks to address these challenges and the extent to which they have been successful in maintaining a balance in the digital age.

The third section of this research focuses on the impact of emergencies, such as public health crises or security threats, on the preservation of freedom of expression and the enforcement of anti-hate speech measures. Emergencies often necessitate extraordinary measures, raising questions about the potential infringement on civil liberties. This paper investigates how Hungary and Romania have responded to emergencies and examines the legal mechanisms in place to protect freedom of expression while mitigating the spread of hate speech during crisis situations.

A comparative case study approach is employed in the fourth section to illustrate the distinct responses of Hungary and Romania to these challenges. For example, during the COVID-19 pandemic, Hungary's "COVID-19 Act" granted the government extensive powers to control information and restrict freedom of expression, leading to international concern. In contrast, Romania maintained a more open and transparent discourse, emphasizing the importance of unfettered communication. These cases underscore the tension between public health imperatives and the preservation of democratic values.

In conclusion, this research underscores the intricate balance between freedom of expression, technology, and anti-hate speech laws in the digital age during emergencies, emphasizing the need for nuanced legal approaches. Hungary and Romania, with their distinct historical backgrounds and cultural contexts, serve as vivid examples of diverse legal responses to these multifaceted challenges. The study highlights the potential for shared best practices and a harmonized legal framework to ensure the protection of fundamental rights while addressing the complexities of the digital era and emergency situations in Eastern Europe.

Platform Democracy or Return to Patrimonialism?

Giulio Santini

The paper intends to address, from a theoretical point of view, the issue of the growing relevance, for the system of contemporary democracy, of the forms of private governance that are characteristic of digital platforms, and that appear akin to the ancient schemes of the Patrimonialism. This analogy emerges by the investigation of the participation methods, which are characterized by a considerable contractual disparity. This is accentuated by the networked goods nature of platforms, which determines the physiological concentration of members. It is up to the strongest party in the synallagma to define not only the access possibilities to the platform, but also the moderation and censorship of unwelcome and excluded content according to the conditions of use. Similarly, the model of the Ancient Regime Patrimonialism seems to be mirrored in the regulation of content hosted by platforms, since, by contract, it is not in the domain of those who produced or shared it but comes under that of the platform itself. The increasingly central nature of digital platforms

obviously has a very incisive impact on the concrete exercise of civil and political rights in the democratic sphere. The conditioning comes from a private subject and based on private law rules, by reason of the control over the platform, which derives from the corporate structures and the contractual terms of the relationship with subscribers. Due to the transnational nature of the services and the usual contractual exclusion of domestic jurisdiction as far as the relationship between platform and users is concerned, the possibilities of resistance on the part of members are very limited, and there are few safeguards that can be offered by the public authorities, which should also guarantee rights and interests that are fundamental for the maintenance of the democratic state. To the synallagma between platforms and users therefore seem to belong not the characteristics of the social contract, but those of the *pactum subiectionis*. It is not surprising, then, how, with respect to it, the greatest mistrust is shown by liberal democracies: of course, they repudiate the principles of the Patrimonalism, but can tolerate limitations on their own *auctoritas*. That is not true for authoritarian regimes, which see in the digital sphere an unacceptable limitation of the monopoly of force and the capacity to govern, which they unconditionally claim. Having outlined the most salient features of Patrimonialism, which are also characteristic of the model of private governance of digital platforms, the paper will turn to an examination of the problems for democracy based on pluralism and participation that this model poses, then reflecting on the possible interventions with which the public authorities can attack it, to protect the interests of users or their own jurisdictional primacy, and on the compatibility of the latter with the paradigms of liberal democracy.

Decentralized online social networks: A taxonomy of technological and organizational choices to embed public values

Mathilde Sanders & José van Dijck

Decentralized online social networks (DOSN's), such as Mastodon or PeerTube, are the refuge for those who want to flee highly autocratic and centralized platforms, such as Twitter or Facebook. In this paper we explain what DOSN's are and how they are presented in public debates. We argue that the choice between decentralized and centralized is not as binary as it may appear, but that platforms can contain elements of both.

'Decentralization' is not only about technical aspects (protocols, software, data servers), but also concerns organizational aspects (moderation, ownership, business model). To embed public values, such as privacy, security or inclusion, a platform can combine centralization and decentralization choices for each of these aspects. In this paper we plot these options. To embed public values in a platform, a combination of both centralized and decentralized technological and organizational elements may be preferable over a static category. We propose a taxonomic model of several decentralization choices that can be linked to underlying (conflicting) public values.

The development of decentralized platforms erupted from numerous points of resistance against centralization—from grass roots movements, and tech nerds to regulators, local communities, politicians, and small entrepreneurs. What unites them is a profound dissatisfaction with Silicon Valley companies' hegemonic power over centralized platform architectures. Their common denominator expresses what they are *against* (centralized, closed walled gardens, proprietary, for-profit) but not exactly what they stand *for* in terms of safeguarding public values. Our taxonomy introduces the public value balancing act as a general way of looking at both technical and organizational platform governance.

14.05-15.20 Global perspectives on regulation

Who controls data rules All under Heaven": Chinese dataregulation between State interventionism and Shanghai Data Exchange model

Davide Clementi

In recent times, attention surrounding the Chinese data governance model has grown, both among those who wish to take it as an example and adapt it to their national and often undemocratic characteristics, and among those who genuinely seek to distance themselves from it, lamenting the authoritarian (when not dystopian) traits of Chinese regulation. China, as «a late entrant to the field of personal information protection and privacy law», has demonstrated both a strong state interventionism and initiatives aimed at the rapid development of digital productive forces, including the creation of a flourishing data market. These recent initiatives have played a pivotal role in shaping the nation's data regulation landscape. These two approaches have often been juxtaposed. In contrast, as is customary in the Chinese way of 'holding opposites together', the Chinese legislator-decision maker has managed to combine both state interventionism and a market-driven approach. Through State interventionism the Chinese legislator has adopted a firm stance on data sovereignty, emphasizing the need to protect national security while maintaining political stability and social harmony. With the coming into force of the Cybersecurity Law (2017), the Personal Information Protection Law (2021), and the Data Security Law (2021), regulations on data collection, storage, and cross-border transfer have become tougher. European and foreign companies have perceived these measures as barriers to the free flow of data, but they align with the government's overarching goal of asserting control over critical information resources. Conversely, the Shanghai Data Exchange sets a model of unique experiment in data governance. Since 2021, Shanghai, as a global financial hub, has been pioneering a data exchange platform that encourages data sharing and monetization while respecting (at least theoretically) users' privacy, striking a balance between data utilization and protection, government and businesses interests, aiming to boost economic development and innovation. Issues concerning privacy, data security, and market's ability to leverage data-driven innovation have arisen because of the coexistence between State interventionism and market-driven approaches, not only among Chinese companies but also on the international level, as China's data governance practices have far-reaching implications. In this paper, the legal implications of this coexistence in Chinese data regulation are analyzed. Advantages and drawbacks of state interventionism and data exchange are discussed and compared, emphasizing their role in safeguarding national interests but also highlighting the challenges of reconciling them with global data flow requirements. In summary, the paper offers an in-depth analysis of Chinese data regulation through the lens of the intricate interplay between state interventionism and the pioneering Shanghai Data Exchange model. By illustrating this multifaceted dynamic, the paper tries to enhance a better comprehension of China's influence in shaping the landscape of global data governance, both domestically and on the global stage, as well illuminated by the phrase «Who controls data rules All under Heaven» (*dé shùjù zhe˙dé tiān*xià 得数据者得天下).

Navigating the Crossroads: Data Privacy, Security, and Responsible AI Implementation in Indonesia

Virga Dwi Efendi & Haryo Putro Dirgantoro

In recent years, Indonesia, like other countries around the world, is at a crossroads in its digital transformation journey by witnessing a rapidly growing internet population and a booming digital economy. Consequently, this growth has also raised concerns about data privacy, security, and the responsible implementation of artificial intelligence (AI) along

with the negative impacts that it can have. One prominent example is a surge in the use of AI technology called ‘deepfake’. Deepfakes are manipulated videos or audio recordings that use AI to make it appear as if someone is saying or doing something that they never actually said or did. From the circulation of manipulated pornographic videos featuring well-known Indonesian public figures to the incendiary hate speech videos using the likeness of famous political figures, deepfake cases serve as a wake-up call, raising prominent concerns of a serious challenge to data privacy, security, and responsible AI implementation in Indonesia. The paper begins by discussing the importance of data privacy and security in the digital age. It then examines the current state of data privacy and security regulation in Indonesia, highlighting the strengths and weaknesses of the recent Personal Data Protection Law legal framework and questioning whether it is sufficient to regulate the ever-changing landscape of new emerging technologies. Furthermore, the paper looks at the dynamic cybersecurity landscape in Indonesia and emphasizes the importance of having strong security measures in place to defend against increasingly sophisticated cyber-attacks. The paper highlights the importance of being proactive about cybersecurity and how this can help to protect both personal data and national security interests. Furthermore, this paper explores the complex issues posed by AI from an Indonesian perspective. The absence of specific laws directly addressing AI in Indonesia leaves law enforcement and the judiciary struggling to apply existing laws to this multifaceted issue. Consequently, this paper offers insights into potential legal reforms and recommendations for the field of AI in Indonesia, specifically. Legislation that prioritizes a human rights approach to AI challenges can guide responses to these threats, emphasizing the importance of protecting the rights of all individuals, both ordinary people and public figures. This approach is essential to safeguarding individuals' rights and preserving a democratic society in the face of modern challenges. Finally, the paper emphasizes the urgent need for Indonesia to collaborate with other countries and international organizations to develop global standards for responsible AI development and implementation, based on the principles of transparency, accountability, and fairness, to ensure that AI is used ethically.

Incorporating Human Centric Design into Algorithmic Governance: Lessons From Past Experiences

Madhav Shankar

The exponential growth in emerging technologies and their applications especially in the field of artificial intelligence (AI) has created a requirement for proactive regulation of such technology in order to safeguard public values, trust, and legal norms. While such regulation has manifested in various forms in different jurisdictions, the European Union has adopted the Artificial Intelligence Act (AI Act). The AI Act among its various objectives, seeks to achieve human values such as trust, accountability and privacy as well as promote innovation and adoption of emerging technologies for a better human experience. The horizontal regulation of algorithmic governance in form of the AI Act for achieving the double aim of innovation and protection of human values would require adoption of standards and technical requirements by sectoral regulators and member states. Such segmented adoption of regulatory standards may suffer from an over-reliance on the industry’s priorities and its understanding of the aims of algorithmic governance leading to weakened standards. The fears of weak regulatory oversight, especially in the context of artificial intelligence are aggravated in light of the ‘black-box’ nature of artificial intelligence in its operation. Due to the complex nature and lack of epistemological insights into the decision making process of AI, only subject matter experts may be able to understand the process. They may therefore be seen as having an informational upper hand in the standard setting process. This may lead to adverse implications for both the ‘legitimacy’ and ‘trust’ aspects of the regulation as well as the effectiveness of such

standards. This paper argues that one of the aims of the Artificial Intelligence Act is to incorporate human centric design process and human values into the development cycle of algorithmic governance systems. In order to achieve this, the paper examines some of the criticisms related to legitimacy and effectiveness of standard setting processes marked by disproportionate industry influence. Such analysis brings forth the problems of standard setting process when it comes to regulation of algorithmic governance systems. The paper then looks at previous regulatory experiences in regulating high-risk technologies which were marked by high levels of uncertainty and want of technical knowledge at the regulators' end. For this purpose, the paper specifically focuses on the European Union's Taxonomy Regulation and United States Food and Drug Administration's regulation for gene editing. This analysis draws insights from the standard setting process adopted in previous regulatory exercises which can now be adopted by regulatory bodies as well as industry experts in developing the required technical standards. These lessons may go on to assist regulators in charting pathways to incorporate human centric design processes in the development cycle of algorithmic governance systems by way of standard setting thus advancing the goals of European Union's AI regulation strategy.

Necessity - an underutilized tool in the regulation of new technologies

Katarzyna Łakomiec

Regulating new technologies is one of the most substantial challenges for public authorities. The first reason is the cross-border nature of operations enabled by technological advancements and the need to harmonize instruments based on different legal traditions. The second is the need to adjust legislation to rapid changes in the realities of network society. Thirdly, this process is hindered by the length and rigidity of court procedures, which impact the effectiveness of enforcement of adopted regulations. The answers to these challenges are, among others, European Union legislative initiatives aimed at regulating the digital space, such as GDPR, DSA, and DMA. An interesting aspect of these initiatives is utilizing the proportionality test, previously associated mainly with public law (I refer to a three-step proportionality test derived from German constitutional law). Of course, proportionality still shapes the activities of public authorities, but what is new is the incorporation of its elements in the obligations imposed on private entities (e.g., very large online platforms). Examples of solutions that refer to proportionality include data protection impact assessment (GDPR) and systemic risk management tools (DSA). Considering that the proportionality test is applied in new contexts and used by new actors, it is essential to analyse changes in its application. I want to focus on the use of the necessity test as an underutilized tool in assessing proportionality. Public authorities assessing proportionality in Europe tend to focus on the last stage of the test – i.e., balancing (da Silva), by direct reference to legally protected values and their importance for individuals and society. However, if the proportionality test is applied in the context of new technologies, the complexity of possible solutions to a given social problem increases. I aim to answer whether the necessity test can serve as an effective analytical tool, preparing the ground for balancing. In short, the necessity sub-test aims to determine whether there are less restrictive means to accomplish the same goal. It must be assumed that the public and private actors choosing the least restrictive means must comprehensively analyse the available solutions. In the case of new technologies, combining the selected measures with possible means to eliminate interference with individual rights is particularly important. Only when possible measures are supplemented with tools that reduce the risk to rights and freedoms (e.g., procedural guarantees, appropriate technical safeguards) is it possible to find the least harmful solutions. An example of such an analysis is the obligation of very large online platforms to use mitigation measures tailored to the specific systemic risks addressed by DSA. In my paper, I look at the application of the necessity test by both public authorities

and private entities. I draw attention to the critical role of this stage of proportionality testing in addressing the risks to rights and freedoms created by new technologies.

Rethinking public acceptance mechanisms for emerging technologies and regulatory efficiency in the EU

Manuel Protasio

This paper provides a comprehensive examination of the EU mechanisms designed to evaluate public acceptance of emerging technologies, with a specific focus on the application of emerging technologies that may pose ethical challenges to society. The study pertains an analysis of the effectiveness and transparency of existing EU models for impact and risk assessment when applied to emerging technologies. The analysis commences by exploring how the EU gauges public acceptance on various aspects of these technologies, including whether these assessments involve active participation from the public and other stakeholders, and in what manner such assessments influence the regulatory process. The paper further argues that the current mechanisms in the EU are insufficient for addressing potential ethical concerns raised by the public, thereby hindering the regulatory procedures undertaken by EU institutions and Member States concerning emerging technologies. To illustrate this analysis, the paper reflects on the Web3 and the metaverse developments and uses as an example virtual reality and its convergence with other technologies to assess its potential impact on mental health, education, consumers. Furthermore, given the rapid pace of technological advancements, the present research underscores the pivotal role that alternative mechanisms for assessing public acceptance can play in shaping future technology regulations. It emphasizes the necessity of aligning expectations between the tech industry and the rest of the stakeholders, revealing that such alignment cannot be achieved without higher levels of transparency and increased participation within the existing EU mechanisms. In conclusion, this study proposes the adoption of new approaches to assess the public acceptance of emerging technologies impacts and, ultimately, to reinforce regulatory efficiency, particularly in light of the ethical complexities inherent to these innovations and the resources available in our contemporary digital age.

15.40-16.55 Ex ante approaches to regulation

Artificial Intelligence and Compliance by Design in Healthcare

Éric Pardoux & Angeliki Kerasidou

Artificial Intelligence (AI), amongst other emerging technologies, is gradually transforming healthcare. From AI models used in medical imaging and diagnosis, to the use of AI and big data in the optimisation of hospital management, as well as its integration in the delivery of care, it is becoming ubiquitous in healthcare. Nonetheless, the extended agency AI-based systems are supposed to provide is not without raising ethical, legal and social concerns. The way AI-based systems are employed may disrupt our understanding of informed consent, the (re)uses of our private data, and the social organisation of healthcare, among other problems. Furthermore, the architecture of some AI systems based on online learning makes them dynamical by design, which is a problem for product approval. Their partly opaque nature is also raising concerns regarding liability. All of these are partly stakes of public governance. In order to limit potential negative impacts, one could thus intend to regulate emerging AI technologies *ab initio*, so to produce technological systems which would be compliant by design – as it is illustrated by the advocates of ethics or privacy by design for instance. However, regulating emerging technologies is easier said than done, as the ethical and legal frameworks are also dynamical. Thus, the yet unknown nature and extent of the impacts of AI technologies are not the only design problems. Envisioning the construction of AI-based systems for public healthcare which would be compliant by design raises several questions. What or who should be compliant with which frameworks during the development and integration of AI-based systems in the public healthcare sector? Is it even possible for a sociotechnical system (based on AI) to be intrinsically compliant? If yes, should we demand it and how? Such questions call for an inquiry about how the compliance by design paradigm may be understood and applied in the case of emerging technologies in healthcare. Compliance in this context does not only mean adherence to the law, but also to medical guidelines for physicians and nurses, or to treatment regimens for patients. It can be understood as following financial guidelines for hospital managers. AI-based systems are progressively integrated in all these layers of healthcare, which questions how compliance can be attained in their presence. Hereby, we propose and defend a vision of the development of AI-based systems in healthcare through the lens of compliance. This implies taking greater account of the dynamics of the sociotechnical systems, acknowledging the co-evolvement of problems and solutions, the openness of the design process, along with a cultural change regarding both the design process and the normative frameworks it should comply with. Compliance would not be only with regards to the law and static frameworks but rather it would be an explicitly dynamical process of constant readjustments, thus fostering trust in the integration of AI in healthcare.

Rethinking regulation by design

Kostina Prifti, Claudio Novelli, Jessica Morley, Luciano Floridi

In recent years, the functional value of design has gained increasing relevance in regulation theory. The trend has been facilitated by a transition in the conceptual treatment of regulation from an essentialist view, which casts regulation as a set of rules that are enacted and enforced by the state (Baldwin et al., 1998; Hood, 1983), to a functionalist one, whereby the scope of regulation is expanded to include additional mechanisms and actors (Black, 2001; Murray & Scott, 2002). Law, markets, and community norms have always affected regulation. At present, the role of design is also coming to be acknowledged, leading to what is generally referred to as "regulation by design" (Lessig, 1996; 1998; Leenes, 2011;

Brownsword, 2016). Given the outlined evolution, regulation by design has become not only a widespread practice – for example it informs the General Data Protection Regulation (GDPR) and the AI Act – but also a research field, with an increasing number of scholarly works, addressing various aspects and levels of analysis. A careful study and analysis of such literature is currently missing. In this paper, we aim to fill this gap by conducting a systematic review of regulation by design in the context of digital technologies.

To fulfil this goal, we develop a conceptual map of regulation by design, identify its conceptual tenets, and distinguish between three types of regulative practices, namely *compliance by design*, *optimisation by design*, and *value creation by design*. This refined approach to regulation by design enables more granular analyses of the concept and more nuanced distinctions between its different applications and related criticisms. Next, we review various technical solutions and identify the latest innovations in the field. Finally, we highlight the challenges that regulators and policymakers must approach carefully and precisely. This review hopes to guide further research that focuses on specific practices, modes, and features of regulation by design. Additionally, we hope to guide policymakers to account for and steer the practice of regulation by design. In that regard, we foresee three possible directions in which the research field can advance. First, we anticipate regulation by design practices to transition from compliance and optimisation by design towards value creation by design. Second, we may expect and aim for a closer alignment between the technical and normative disciplines that characterise the field. While authors of these two types of disciplines reference each other's work, they tend to operate independently. Third, more space is required for the role of public institutions in overseeing and steering the practice of regulation by design, which may potentially contribute to the two aforementioned developments.

A Fundamental Rights Impact Assessment for DLT-programmes targeted at the public sphere

Georgios Bouchagiar

Distributed Ledger Technologies (DLTs) can be seen as kids playing basketball: every kid can know and check validity of the rules and the score, as well as their history; every child may call each other with a pseudonym; any kid can join (or leave) the game, insofar as she/he complies with the rules and accepts the score; in case of foul, they reach consensus and keep on playing; and they all agree upon the rules and the scoring, making referees and score-keepers unnecessary. Born in the crypto-anarchist underground of the Internet, after the 'Crypto Anarchist Manifesto', the 'Declaration of the Independence of Cyberspace' and The Wealth of Networks, DLTs have enjoyed widespread use by various entities.With numerous DLT- programmes in the EU agenda, targeted at the public sphere (ranging from voting to establishing digital identities), one may reasonably question whether and the degree to which we are, from a scientific and regulatory point of view, ready to introduce DLTs in public areas that demand enhanced checks and balances.This contribution discusses DLTs' features and design options, with a view to identifying key challenges in particular relation to DLT-uses in the public sphere. Finding that certain intrinsic and emerging features of DLTs may contradict fundamental principles that need be respected in certain public areas (like secrecy of voting or anonymity of citizens), it recommends a Fundamental Rights Impact Assessment that can be applied by an independent authority ex ante, before the actual use of DLTs in a given public field.

Networked algorithmic administrative decision-making

Charlotte van Oirsouw

Analyzing networked algorithmic administrative decision-making: A conceptualization

Administrative authorities continuously have to adapt their decision-making processes to meet the demands of our changing world and to address complex societal challenges. From a public law perspective, two interesting developments can be identified. First, traditionally the task of government has been to apply administrative law top-down to those it regulates. However, complex societal issues, such as poverty or climate change, require the collaboration from administrative authorities with multiple stakeholders, such as other administrative authorities, private organizations, NGOs and citizens, resulting in governance networks where multiple actors jointly contribute to addressing the complex societal issue. While such network governance is characterized by the benefits of collaboration and flexibility, it is also characterized by opacity, unclear responsibilities and a lack of accountability. Second, technological developments such as the proliferation of the use of AI and the emergence of blockchain technology have increased the range of technological possibilities for administrative authorities to (partially) automate their administrative decision-making processes. The use of these technologies has already resulted in several "scandals", think for instance of RoboDebt, the SyRI-case or the Dutch childcare benefit scandal. In particular, these scandals raised concerns about the transparency of the administrative decision-making process and the accountability of government.

These developments go hand in hand where algorithmic systems are used to (partially) automate administrative decision-making processes within an already existing governance network, or where a governance network emerges in the course of its development. This paper argues that this leads to "networked algorithmic administrative decision-making", or for short, NAADM. A clear conceptual understanding of NAADM is currently lacking in public law scholarship. The aim of this paper is therefore to conceptualize NAADM based on a multidisciplinary literature review, drawing on literature from legal scholarship, governance studies and Science and Technology Studies (STS). A conceptual foundation provides analytical tools for future research to conduct systematic (empirical) legal research on NAADM and allows for further theory building.

In short, NAADM occurs where administrative decision-making process involves the use of an algorithmic system within a network governance context. NAADM is understood as a socio- technical concept: it has technical elements (hardware, software and data) and social elements (actors, relationships between them). Due to the socio-technical nature of NAADM, a NAADM- process embodies norms and values, and is contingent upon changes in the social context in which it is situated. During the development phases of an NAADM-process, developers may seek compliance with legal norms by adopting "by design" approaches, thereby embedding legal norms into the (technological) design of NAADM. NAADM challenges the values of transparency and accountability because of the opacity and accountability issues that arise from the technical and social complexities of NAADM. Addressing these challenges is vital, as transparency and accountability are two important contributors to the legitimacy and acceptance of the exercise of public authority in constitutional democracies.

The need for responsible use of artificial intelligence by the Public Administration: Algorithmic Impact Assessments (AIA) as instruments for accountability and social control

Julia Lunes

The public administration of several countries is increasingly applying artificial intelligence (AI) to assist various activities, such as public services provision, decision-making processes and law enforcement. Although the use of algorithms by the states is still in its inception compared with the private sector, it has been provoking wide-ranging impacts on fundamental rights. Automated systems are influencing people´s access to social benefits without proper accuracy and due process guarantees, as is the case of the SiRI (*"system risk indication"*) deployed by the Dutch government, and systems for social security provision implemented by the federal government of Brazil. Moreover, algorithms are also used for criminal prosecution activities, through facial recognition and predictive policing technologies, introduced in several cities around the world. It is expected that the government´s use of AI will increase the efficiency of public management. Nonetheless, its indiscriminate use is causing damage to society as a whole and to the principles of legality, equality and public justification that should underpin state acts (Smuha, 2021). There is overwhelming evidence of the discriminatory potential of algorithms, especially for groups that are already marginalised in society (Eubanks, 2017; O´Neil, 2016). Furthermore, its lack of transparency and explainability often undermines citizens' ability to understand, challenge and scrutinise public decisions that affect their lives (Danaher, 2016). Despite the systemic impacts that algorithms can have on society, they are being widely implemented by the public sector from the Global North and South, without a proper assessment of their risks. There is a lack of accountability mechanisms so that states can publicly justify the adoption of these technologies, explain how they work, attest to their benefits and take responsibility for eventual damages they may cause (Brandusescu, 2022; Reismann et al., 2018). An increasingly necessary question in this scenario is how to guarantee accountability for algorithmic policies implemented by the state. What duties should the public administration assume when deciding to implement algorithmic technologies that impact fundamental rights? As shown by recent research, regulatory frameworks for public accountability are still in their infancy and governments in general are struggling to establish processes to implement AI responsibly (Ada Lovelace et al., 2021; Moss et al., 2021). Although the regulatory efforts and policy initiatives are still at an early stage, algorithmic impact assessments (AIA) are gaining prominence among academics and policymakers as one of the main accountability mechanisms that should be applied before introducing an algorithmic system in a given context. AIA has its origins in impact assessment processes already developed in other fields, such as Data Protection Impact Assessment (DPIA) and Environmental Impact Assessment. Inspired by these existing models, AIA aims to enable a prior and participatory study of the risks, costs, benefits and societal implications of algorithmic systems deployment. It is recommended that AIA´s processes count with meaningful participation of civil society and it is hoped that, when properly institutionalised, AIAs may inform public agencies´decision on whether or not to adopt the system, as well as on how to mitigate its potential future harms. Given the importance that AIAs can have for the preservation of trust in government, the rule of law and fundamental rights, the general aim of the article is to explore the fundamentals of AIA, indicating the challenges and requirements for it to become an effective mechanism for algorithmic accountability by the public sector.

3. GOVERNANCE TRACK

(SOETESALON)

9.30 – 10.45 The governance of cybersecurity

The Implementation of Directive NIS2 between Public and Private Governance: The Role of CSIRTs

Erik Longo and Elia Cremona

On the 16th of January, 2023, Directive (EU) 2022/2555—commonly referred to as NIS2—officially entered into legal force, superseding its predecessor, Directive (EU) 2016/1148 (NIS). The NIS2 Directive aims to augment the extant cybersecurity infrastructure across the European Union through a variety of mechanisms. One such strategy for bolstering cybersecurity within the EU involves the cultivation of Public-Private Partnerships (PPPs). Entities such as Computer Security Incident Response Teams (CSIRTs) play a pivotal role in sense-making during cyber crises and epitomize this policy of collaborative endeavours between the public and private sectors.

To harmonise practices across the European Union, the "NIS Directive" mandated that each member state designate a single point of contact responsible for coordinating issues pertaining to network and information security as well as international cooperation. The NIS2 Directive amplifies this role, expediting collaborative efforts in this particular domain.

However, the evolution of these partnerships encounters challenges - both at an EU and National level - that extend beyond merely technical or political dimensions; they also present substantial legal complexities. One such issue pertains to the operational guidelines that CSIRTs are mandated to adhere to and the scope of their competencies. Within this framework, public administrations are transitioning towards a model wherein they no longer merely contract for specific tasks and oversee their execution. Instead, they are actively shaping the conditions that facilitate the self-organization of these networks. This approach posits a middle ground between the extremes of interventionist and laissez-faire policies.

Additionally, a further issue of import arises in the context of cyber crisis management, particularly regarding the role that CSIRTs are to play in cyber warfare scenarios. This necessitates a thorough examination of the implications for domestic and international legal frameworks and strategic policy considerations.

Toward a Charter of Fundamental Rights in Cyberspace

Gianmario Demuro

In 1996, John Perry Barlow opened his Declaration of Independence in Cyberspace by stating, "Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather". This libertarian vision to the point of anarchy, in addition to being belied in everyday life, is directly conflated with the claim of states of law to extend their sovereignty, within the limits and in the forms provided by their constitutions, to cyberspace as well. Precisely with the

aim of making cyberspace permeable to the traditional prerogatives of states to control any form of power (be it public or private) and to protect national security and fundamental rights, an extended Partnership called "Security and Rights in the CyberSpace" (SERICS) has begun in Italy. This is an impressive form of collaboration between universities, private and public research organizations, and businesses under which the University of Cagliari will address the protection of fundamental rights within cyberspace.

On the merits, assuming that the research will be conducted through the prism of constitutional law and in light of a multilevel governance perspective, which involves public and private actors from the European to the national level, the University of Cagliari research team considered it essential to answer three research questions: which new technologies create new conflicts between rights? Which rights are being violated by the use of new technologies? Are there new problems arising from the use of new technologies for which rights do not yet exist? The clarification of these three issues will be crucial in order to arrive at the drafting of a Charter of Fundamental Rights in Cyberspace, which will have the function, not only to represent a clear political commitment on the part of European and national authorities to the respect of rights in cyberspace, but also to facilitate the European process of digital transition.

What role for Italian regions in the cybersecurity governance

Giovanni Coinu

In a multilevel perspective, the complex system of cybersecurity governance that synergistically involves public actors from the European to the national level through the system of agencies-European Union Agency for Cybersecurity and the Italian Agency for National Cybersecurity (ACN)-cannot ignore the role regions play in delivering key public services.

While it is true that under Article 117(r) of the Italian Constitution, the national Government retains legislative and regulatory authority over the "statistical and information coordination of state, regional and local government data", the regions are at the very least entitled to the organizational competence for the territorial delivery of public services such as health, education and active labor policies. In such a context, the regions must also deploy appropriate cultures and tools to respond effectively to cyber threats because each public actor must develop, even at the local level, its own specific capacity for prevention, early detection and response to cyber threats.

If, therefore, the national legislative assembly or executive must be properly involved in the policy formation process on cybersecurity, the counterparts in regional government cannot be excluded from these same circuits. Regions must be especially sensitized on strengthening cyber security incident detection, analysis and response activities, as well as cyber risk prevention and mitigation.

Studies at the international level say that 85 percent of data breaches depend on human error, so building training paths for regional administrative staff can also become an effective cyber-attack defense tool, as well as easy to implement.

In this regard, at least two elements are worth exploring.

On the one hand, the positions expressed by the Conference of the Regions on the need for their involvement to clarify the intersections between the different regulations that have been stratified in cybersecurity in recent years and the relative transitions of competence,

with a shared path that is synergistic with the systematic and sustainable activation over time of "business impact analysis (BIA)" and "risk assessment" activities, to be financed with structural funds.

On the other hand, the funding through PNRR resources of a program proposed by the National Cybersecurity Agency for the activation of Computer Security Incident Response Teams (CSIRTs) in each Region, including through an extraordinary emergency recruitment in the regional systems of IT professional profiles specialized in cybersecurity and digital transformation, providing for specific national funding rules and/or exceptions to existing constraints for the recruitment of such personnel.

The complicated governance of cybersecurity between technology and policy

Lorenzo Moroni

Cybersecurity requires the preparation of an institutional organization suitable for dealing with the challenges and threats that are increasingly coming from the digital world. Just think, by way of example, of the very rapid spread in the last year of artificial intelligence systems, such as chatbots (e.g., ChatGPT, Google Bard, etc.), or of the ever-increasing cyber-attacks, which, according to the most recent studies, are expected to increase by 21 percent worldwide in 2022.

The need to navigate such a complex environment has led the European Union, through EU Directives 2016/1148 and EU 2022/2555 (so-called Network and Information System - NIS - I and II, respectively), to require member states to establish national cybersecurity authorities. However, it is interesting to note that, aided by the physiological cross-cutting nature of cybersecurity policies and the wide margin of discretion that the directives themselves grant to member states in fulfilling their European obligations, the implementation of the two NIS I and NIS II directives has been particularly heterogeneous. In fact, a first group of states decided to entrust the role of "national NIS authorities" to independent administrative authorities or, at any rate, technical regulatory bodies. These include, for example, Luxembourg, which has assigned cybersecurity functions to the Financial Markets Authority and the Telecommunications Authority, depending on their area of responsibility. A second group, on the other hand, has grafted powers arising from the NIS directive directly onto ministerial apparatuses or dependent on them. This is the largest group, and the concrete choice of the competent body depends on how cybersecurity policies are interpreted, with the result, then, that in some countries the Ministry of Communications (e.g., Malta and Ireland) is entrusted with the functions, in others the Ministry of the Interior (Germany), and in still others the Ministry of Justice (e.g., the Netherlands). Third and finally, other countries have decided to directly or indirectly confer the functions of "national NIS authority" to the government (e.g., Italy, Belgium, France).

In light of this uneven context, it is crucial to ask what is the best form of organization of European cybersecurity governance: is it an issue that due to its particular complexity should be released to technical entities, or is the nature of the issue primarily political and, therefore, its "governance" should be entrusted to political authorities? Again, should cybersecurity policymaking remain the sole preserve of governments, or should it involve national parliaments? These are just some of the many questions that are intended to be answered in order to shed light on the contentious issue of multilevel governance of cybersecurity.

The Digital Constitutionalism

Marco Betzu

If the purpose of constitutionalism is the limitation of power, "none of its forms can logically escape containment." Against the pervasive power of the giants of the digital world, therefore, it is necessary to rediscover and apply the traditional categories of constitutionalism, without the need to theorize new as well as labile formulations of them. In this sense, theories of "digital constitutionalism" end up conveying a warped version of it.

The points of attack are numerous.

Among them, for example, there are certainly those that affect the use of data, in order to build a far more effective protection of privacy than that provided by the GDPR Regulation, based on consent , and which, above all, dissolves the normative contradiction whereby "the protection of privacy as a personality right must be combined with the need for the free circo-lation of data" .

Likewise, stricter measures must certainly be put in place to counter the phenomenon of disinformation, hate speech and, more generally, capable of fostering "collective awareness of the risks of those communication circuits" .

But above all, an implementation of the principle of competition declined according to a perspective that goes beyond the reduction of users to consumers is unmissable. In this sense, there is a need to rethink antitrust theory by following trajectories similar to those traced by the new Brandeisian movement, enhancing the virtualities of the principle of competition.

A look at the processes and structures of the digital economy shows that the role of big data in the data-driven economy must be taken into account above all, and it is therefore these that need to be affected in order to shape the market for digital services differently. For example, by opening up digital platforms to third-party providers of middleware services or by providing users and businesses with the necessary tools for data portability to other platforms .

Where necessary, it is then time to make bold decisions like those that guided the dismemberment of Standard Oil over a century ago . Instead, in the future, all acquisition procedures by gatekeepers should be subjected to a double evaluation, ex ante and ex post: a kind of "takeovers on parole," "which should be reviewed after five years for possible dissolution if they prove to be anti-competitive" . After all, when Brandeis spoke of the "curse of greatness" he was referring precisely to the situation in which oversized enterprises end up "damaging democratic self-government" .

This is a challenge that may seem daunting: if humans are not angels , even less so are data barons, who shape and control our lives on a daily basis so pervasively that they have become an integral part of it. But starting from the constitutional principles that represent the irreplaceable tools "of civilizing human relations," it is more necessary than ever to continue "the fight against arbitrariness, limitation, containment, and fragmentation of power" .

11.05 – 12.20 Governance of technology

Designing institutions for Emerging Technologies: Towards a heuristic model

Anieke Kranenburg

In an age with large societal challenges, the pivotal role of emerging technologies has garnered widespread recognition (Mazzucato, 2021; Ulnicane, 2022; Diercks et al., 2019). This recognition is particularly pronounced in the energy transition, driven by the imperative to achieve the 2050 net-zero greenhouse gas target. Emerging technologies constitute a distinct category of new technologies that is characterized by radical novelty, fast growth, prominent impact. However, they also exhibit high levels of ambiguity and uncertainty (Rotolo et al., 2015). For instance, the adoption of emerging large-scale energy storage (LSES) technologies is deemed essential in the Netherlands to better balance energy supply and demand[1], but there are inherent uncertainties stemming from their emergent stage. These uncertainties include questions related to scalability, operational scale, benefits, and ultimately result in challenges to effective accommodation of these technologies.

It is widely acknowledged that emerging technologies necessitate corresponding adjustments in the institutional design to harness their benefits while minimizing potential risks (Mandel, 2009; Chleba & Simmie, 2018; Rip & Kemp, 1998). The institutional design of emerging technologies encompasses the formal and informal 'arrangements between actors that regulate their relations: tasks, responsibilities, allocation of costs, benefits, and risks' (Koppenjan and Groenewegen, 2005: 243). These formal and informal institutional arrangements provide stability, but they may also be inadequately flexible if emerging technologies require adjustments to accelerate their development and deployment. Therefore, the stability offered by the institutional design might be at odds with the dynamic and rapidly evolving nature of emerging technologies. For example, in the case of LSES, concerns have been raised by stakeholders regarding the potential for these technologies to outpace existing Dutch regulations, potentially impeding their development.

While prior research has delved into the institutional design of technologies and proposed models for the process of designing institutions, these studies have predominantly focused on socio-technological systems with established technologies (Koppenjan & Groenewegen, 2005, De Bruijn & Herder, 2009). There is a lack of understanding regarding how to effectively design institutions for emerging technologies despite their growing importance in sectors such as the Dutch energy system. Previous research has shown that emergent technologies pose distinctive challenges to institutional design, particularly concerning risk management, regulatory frameworks, and governance approaches- challenges that diverge from those posed by established technologies (Isigonis, et al., 2020; Linkov et al., 2018; Marchant, 2020; Mandel, 2009; Withford & Anderson, 2021). However, it is insufficiently understood how to manage challenges when designing institutions for emerging technologies. Therefore, the following research question is formulated: How to design institutions to deal with the distinct challenges posed by emerging technologies, in particular large-scale energy storage technologies?

This study leverages data derived from 31 in-depth interviews and 4 focus groups, involving diverse LSES stakeholders in the Netherlands. First, the institutional design emerging LSES technologies is analysed, and the key challenges posed to the institutional design are identified. Subsequently, drawing on insights from the literature on the governance of emerging technologies and institutional design, along with the results of the LSES case

study, a heuristic tool is presented to navigate these challenges in the process of designing institutions for emerging technologies.

This article is structured as follows. Section 2 uses existing literature to delve into the challenges posed by emerging technologies to the institutional design. Additionally, this section presents a framework to analyse the institutional design of LSES and explores the conceptual basis of process design models. Section 3 provides detailed descriptions of the study's methods. Section 4 analyses the institutional design of LSES, particularly focussing on the challenged posed by emerging LSES technologies to the institutional design. Building on these insights, Section 5 proposes a general tool for the process to design institutions for emerging technologies. Lastly, Section 6 concludes the paper, expanding on the research's contributions and limitations, and outlining potential avenues for future research.

Decentralisation as a Design Parameter for a Public Digital Infrastructure

Arno Laeven & Tina van der Linden

The majority of individuals now spend a significant portion of their waking hours online, both for work and leisure purposes.

For now, we still have physical bodies that live in the physical world where we eat, sleep and move around. The physical infrastructure is typically owned and controlled by public authority; governments on different levels. Based on law, they determine the architecture of the infrastructure, the distinction between the public and the private sphere, the rules that apply, and the enforcement (or not) of such rules. And even if the infrastructure is owned and exploited by private parties, its goal and the rules that apply are determined by law. All, in theory, in the interest of society as a whole and respecting human rights such as laid down in constitutions and international treaties.

Online, the situation is rather different. Grown organically from its military and academic roots, the online world has evolved over the last forty years or so into the plutocracy of what is commonly called Web 2.0. The architecture of the infrastructure, the distinction between accessible to all and restricted access, the rules that apply, and the enforcement (or not) of such rules are determined by privately owned commercial parties, driven by their own commercial interests. Sure, law applies to the online world, but the unlike physical infrastructure this is not linked to its architecture or design principles. The online infrastructure does not and cannot reflect the notion of public space as we know it in the physical world. Moreover, law originates from sovereign nation-states, whose jurisdiction stems from and is limited to their territory. Prescriptive jurisdiction (setting norms) can lead to spill-over effects and conflicts of norms. Enforcement of such norms may lead to conflicts or be simply impossible.

This paper explores decentralisation as a fundamental design parameter for a public digital infrastructure, offering an alternative approach to address the challenges identified earlier. Our central argument is that the choice of decentralised digital technologies should not be viewed solely as a market principle but as a fundamental design choice that reflects the values of a society - and therefore it should be part of the public debate and policy making.

We start by explaining what we mean by decentralisation as a design parameter for public digital infrastructure. Subsequently, we demonstrate how a decentralised digital infrastructure has the potential to address the issues outlined above. Next, we will examine potential implementation strategies and provide an illustrative example. In conclusion, we assert that decentralisation indeed represents a viable alternative to the current online

infrastructure. We encourage further discussion, research, and action in this direction to explore the full potential of decentralised technologies in shaping the digital landscape in the public interest.

Towards a Quantum-Safe Global Encryption Policy: Challenges and Solutions

Alessia Zornetta

Cryptography, an essential art in preserving information integrity through encryption, stands as a cornerstone for ensuring the security of today's information-driven society. The ubiquity of Internet-enabled communication, information acquisition, and commercial transactions underscores the indispensable role encryption plays in enabling these activities securely. Amidst evolving interests in encryption policy among policymakers over the past decades, this paper advocates for a comprehensive reconsideration of the policy discourse aimed at advocating for robust encryption on a global scale.
This argument stems from the rapid advancements in quantum computing and their implications for national security. Quantum computing, distinguished by its unique ability to leverage superposition to perform computations previously impossible, introduces apprehensions about its potential to disrupt current encryption methodologies. In stark contrast to classical computers, quantum computers boast computational capabilities that could conceivably dismantle even the most complex and secure encryption techniques, thereby jeopardizing the security of interconnected systems. The paper sheds light on the risks posed by quantum computing to national security, wherein breached encryption could compromise classified information, military intelligence, sensitive devices, and critical infrastructures.
The argument for a worldwide encryption policy is further substantiated by the looming specter of profound global power asymmetries. As the evolution of quantum technology remains concentrated within a select cohort of nations, those in possession of functional quantum computers could gain unprecedented advantages and exploit such technological supremacy. To buttress this assertion, this paper employs the logic of the "least trusted country problem" to underscore the fragility of global security in the face of such imbalances.
In response, this paper introduces a three-fold strategy designed to pave the path toward a quantum-secure future. The strategy encompasses the pivotal elements of post-quantum cryptography, quantum key distribution, and quantum random number generators. While acknowledging the challenges inherent in implementing these measures, including the projected decade-long timeline for establishing standardized solutions, the paper underscores the urgency of confronting the imminent quantum computing menace in a proactive manner. By adhering to these strategic imperatives, the global community stands poised to reinforce encryption practices against the potent capabilities that quantum computing wields. In so doing, the security and integrity of information exchange can be preserved in an ever more interconnected world.

Digital democracy reimagined: navigating the intersection of innovation, governance, and accountability

Francesca Niola

In the digital age, traditional representative democracy is undergoing a radical transformation, with the integration of emerging technologies such as artificial intelligence and blockchain. The following reflection originates from the Italian case: a parliamentary

democracy, symmetric bicameral, where political parties, traditionally seen as intermediaries between citizens and institutions, are exploring new ways to involve the public and the private sector in political decisions and, potentially, in the legislative process using crowdsourcing platforms (e.g., SkyVote or Zooppa).

These platforms, embodying the pinnacle of technological innovation through the adoption of artificial intelligence and blockchain, are shaping as catalysts for a new governance paradigm. They do not merely act as simple intermediaries but weave a complex network that connects citizens, public entities, and private actors, giving life to a dynamic and interconnected ecosystem.

The public-private collaboration emerging from this ecosystem proves to be a powerful engine for innovation in public services. This synergy, if well-orchestrated, has the potential to transform administrative procedures, making them not only more efficient but also more aligned with the needs and expectations of citizens. A horizon of possibilities opens up for the creation of truly user-centered public services, characterized by a high degree of customization and responsiveness.

However, the enthusiasm for the potential offered by such technologies should not overshadow the inherent challenges and complexities. The intrinsically private nature of crowdsourcing platforms raises crucial questions about the tension between commercial objectives and democratic ideals. In a context where economic interests can influence decision-making dynamics, it is imperative to investigate how to preserve the authenticity of democratic participation and prevent distortions of representation.

The issue of transparency and accountability thus becomes pressing. In an era characterized by incessant information flows and the increasing complexity of digital networks, ensuring the clarity of decision-making processes and the accountability of the involved actors is fundamental. Democratic institutions, subject to mechanisms of control and balance, must face the challenge of integrating private platforms, whose operational logics may remain obscure, without compromising citizens' trust and the legitimacy of the democratic process.

In this intricate scenario, the regulation of crowdsourcing platforms takes on a central role. The theme of digital sovereignty and representation intertwines with the need to define a clear and rigorous regulatory framework. In this regard, the commitment of the Italian parliament to address the issue is noteworthy, with the bill A.S. n. 2495 of March 23, 2022. It represents a concrete example of legislative commitment in this direction, prompting a thorough reflection on representation mechanisms and the ways in which interests are conveyed and represented in a digital context.

Crowdsourcing platforms, especially when integrating cutting-edge technologies, require a regulatory framework that ensures their integrity, transparency, and legitimacy. Only through a holistic and multidisciplinary approach, considering the multiple facets of the phenomenon, will it be possible to navigate the tumultuous waters of digital transformation, preserving democratic values and promoting responsible innovation.

14.05-15.20 Governance by technology

Digitalization in rural municipalities - the role of suppliers

Anja Gjærum

Digitalisation and digital transformation in public sector organisations depend on digital systems and infrastructures from global and national commercial suppliers. Public sector handle complex issues, and constitute a multibillion market. The differences in digital skills and capabilities between smaller municipalities and commercial suppliers are presumably substantial.

The technologies the municipalities use increasingly include elements from emerging technologies. Hence, a better understanding of the relations between public sector organisations and commercial suppliers and vendors is important for development and deployment of emerging technologies in public governance.

Even though relations between commercial suppliers and public actors is a topical and debated concern, existing literature seems scattered. IT and information systems outsourcing in the public sector is understudied (Gantman & Fedorowicz, 2020; Lin et al., 2007; Swar et al., 2012), and existing studies discuss both why, how, which, and outcomes (Gantman & Fedorowicz, 2020).

Collington (2022) discusses how dependency involve welfare state retrenchment, while Mazzucato and Collington (2023) argue that extended use of big consultancy firms outsource competencies from the public sector, and frame solutions to complex problems as simpler than they really are.

Haug et al. (2023) identify suppliers as an inter-relational factor that influence digital development, though referenced studies (Jones et al., 2019; Klopp et al., 2013) do not target relations between private and public actors.

Other related fields and topics are public procurement and innovative procurement, public private partnerships, as well as digital platforms (Fishenden & Thompson, 2013).

I find the relations between commercial suppliers and (smaller) municipalities; including organisational relations, development processes and power structures, among issues that remain elusive.

To address this topic, I conducted a qualitative study comprised of semi-structured interviews with managers and employees in rural municipalities and inter-municipal ICT collaborations in Norway. I plan to interview commercial suppliers of digital public sector systems and services. A document study of government white papers and strategies for digitalisation further informs the study.

I plan for the paper to capture the perceptions and experiences of the different groups of informants, concerning the relations between their organisations, and analyse how these relations influence the digitalisation processes in the municipalities.

Hearing out informants from both the municipal and commercial side and analyse the findings considering existing literature, should provide a relevant basis for discussing the organisational relations, development processes and power structures.

Most Norwegian municipalities have less than 10 000 inhabitants and limited capabilities concerning procurement, development and support of digital systems and solutions. They are also characterised by a large number of digital administrative systems, and quite extensive use of systems and services administered or delivered by commercial suppliers (Schartum et al., 2017).

The municipalities in the study have between 900 and 5400 inhabitants. Insights from the study might highlight topics relevant also to bigger municipalities and other public organisations. The informants from the municipalities communicate reliance and trust, as well as dependence and frustrations concerning their relations with commercial suppliers.

Disentangling digital welfare dystopia: Towards a general understanding of system failures in social security enforcement

Maarten Bouwmeester

Recent government scandals across welfare states, with striking similarities, have demonstrated the potentially destructive impact of digitalized welfare fraud detection and enforcement on vulnerable citizens. These cases are not only alarming because of their dystopian outcomes, but also because they have exposed systemic flaws in government and the relationships between state institutions. The digital welfare state appears to be a hazardous environment for the emergence of 'system failure', comprising a complex interplay of decision-making errors and weaknesses in the control mechanisms of the rule of law system (*Rechtsstaat*). While there is growing awareness of the (micro-level) risks for vulnerable citizens in practices of digitalized service delivery and decision-making, our understanding of this (macro-level) risk of system failure and the significance of rule of law control mechanisms remains rather limited. Therefore, this article explores the general, cross-national risk factors underlying recent instances of system failure in the digital welfare state. It first provides a working definition of system failure and illustrates this definition through a short comparative discussion of cases from multiple countries. It then combines theoretical insights on the intersection of public law, social policy and automated decision-making to systematically outline the risk factors that challenge the efficacy of rule of law control mechanisms in the digital welfare state. The result is an encompassing framework that distinguishes between multiple types of risks and different control mechanisms (from the legislative phase to parliamentary scrutiny and judicial review). Finally, the article illustrates the empirical value of this framework by reflecting on two cases: the Dutch childcare benefits scandal and the Australian Robodebt scandal. All in all, the article contributes to a better understanding of the intersection of digital welfare and rule of law control mechanisms, informing current discussions on institutional reforms beyond specific national contexts.

The Role of Technology in Citizens' Right to Good Administration: Examining the Impact of Smart Governments

Bárbara da Rosa Lazarotto

In a quest for a more effective and cost-efficient public administration, governments have boosted the use of technology throughout the administrative process with the aim to collect and process data on a large scale. This practice has been labeled as "smart government" and is often carried out with the widespread installation of technological apparatus – such as information and communication technologies (ICT) and artificial intelligence (AI) –, which

are applied in multiple tasks such as automated decision-making processes, predicting policing amongst others, with the conviction that they will solve long-lasting problems. However, the adoption of multiple technological tools by governments has impacted the role of the state in its relationship with citizens, creating power imbalances. Citizens are often submitted to processes of surveillance and datafication which remove their autonomy and privacy often in all areas of their lives. These actions place governments in the role of the party that "knows it all" while citizens have their rights diminished by not knowing what data governments have access to and what it does with it. Yet, many governments justify the heavy use of technology on citizen's right to good administration, since it allegedly permits the delivery of more efficient, less costly administrative services, often claiming to be personalized to the citizen's needs and seamless, a practice that differs from the traditional bureaucratic tradition of the state. In this context, this paper explores the concept of "smart governments" as the phenomenon of the heavy reliance on technology and how (and if) these practices, in fact, fulfill citizens' right to good administration. This study proposes to make an analysis of the most common technological practices applied in "smart governments" such as nudging, and sensorization of public environments as a backdrop to the examination of the "smart government" phenomenon, and its practices in the light of the right to good administration but also

propose measures that limit the power of the smart government with the objective of rebalancing the current power imbalances.

Searching for Complementarity: A Comprehensive Literature Review of Human Intervention in (Semi-)Automated Administrative Decision-Making

Lucas Haitsma, Barbara Brink, Elliot Mayhew

Governments have been actively integrating information technology into administrative and public agency tasks. This has resulted in the adoption of sophisticated technologies capable of automating various administrative functions. Algorithmic technologies and AI are playing an increasingly pivotal role in processing and analyzing data, identifying patterns, making forecasts, optimizing outcomes, and executing informed decisions in a (semi-)automated manner. This enables decisions to be automatically generated with limited human involvement, thus promising more prompt, efficient, precise, and less biased decision-making processes. Recent incidents in the Netherlands have demonstrated the potentially devastating consequences associated with the irresponsible use of such technologies. Such incidents undermine trust in the government's ability to use such technologies in a manner that safeguards the fundamental rights of citizens. In an effort to prevent such incidents, there is a growing recognition of the need for a human-in-the-loop safeguard to facilitate comprehension, challenging, and communication of (semi-)automated system outputs. The focus on human intervention, encompassing elements such as human-machine interaction, manual or human review, supervision, human agency, or human oversight, is gaining traction. However, a precise conceptual framework for this human- in-the-loop involvement has yet to be established. This paper seeks to explore the following central research question: *What role is attributed to human intervention in (semi-)automated administrative decision-making, and how is this role conceptualized?* In order to answer this question, we undertake a comprehensive literature review to delve into the notion of human intervention within the realm of (semi-)automated administrative decision-making (AADM). We scrutinize the various forms of involvement (oversight, judgment, intervention), the presumed timing of human participation, the nature of the decision-making process, and the relationship with discretion, along with the rationale behind advocating for human involvement. To this end, and given the interdisciplinary character of the subject of this paper, we will draw on literature from the public administration, legal,

and technical domains. This paper seeks to enhance our comprehension of the role played by human intervention in (semi-)automated administrative decision-making and its potential configuration, thereby contributing to the development of a human-in-the-loop framework.

The legal implications of the use of Artificial intelligence by public actors: The common global challenges related to trust, transparency and accountability

Sajal Sharma

Artificial intelligence (AI) is set to transform human life in all its dimensions. Although this may sound somewhat exaggerated and disturbing, it is a process that has already happened with other disruptive technologies. That is the case with the development and expansion of the internet since the beginning of the century, which has brought about major changes in our economies, societies, politics, and personal lives. In any case, the use of Al in government is still very limited, but it is spreading to new activities and services. It is foreseeable that it can be applied to all government functions. A number of examples of this exist both in the United States and the European Union, which demonstrates the enormous potential of using Al systems in government.

This paper analyses the legal implications of using Al in government from a general perspective, including all three branches of government, but it focuses on administrative activities, from government decisions to service provisions. Although each country faces digital transformation in line with their own constitutional and administrative tradition, there are some common challenges related to the use of Al in the public sector which can be considered as global issues. Therefore, the purpose of this piece of work is to identify these global challenges by carrying out a comparative analysis of the United States (US) and the European Union (EU) and India.

It is urgently needed to promote a new governance for the use of algorithmic Al by administrative bodies to meet the challenges it will pose for government. A first step is to identify what Al consists of and how it is being applied (and can be applied) in government functions. From there, it is necessary to analyse the incipient problems that are arising with respect to the role of humans in administrative Al decisions; the transparency and the possibility of accessing the reasons for Al administrative decisions; the dependence on third parties that provide external Al; and, above all, the difficulties of accountability and oversight of government Al action to ensure that it is lawful and respectful of constitutional values

It is clear that the use of Al in government is changing the rules of the game. A key area for public debate and academic inquiry is how to adapt existing principles of administrative and constitutional law to the new playing field. There is a need to be vigilant to this transformation and adopt the necessary measures in time. Otherwise, humanity may soon find itself trapped in the rationality of algorithms and missing some human arbitrariness.

15.40-16.55 Governance by and of technology

Utopian Visions, Dystopian Concerns, and theLegal Realities of Blockchain and AI

Fulvia Abbondante

This paper seeks to delve into the sufficiency of current legal frameworks in addressing the challenges posed by AI and blockchain technologies. The primary objective is to investigate how these regulations, with a specific emphasis on the European context, are influencing the constitutional principle of the rule of law. In addition to exploring the regulatory aspects of AI and blockchain, this contribution introduces a systematization of the theoretical framework associated with *digital constitutionalism*, a novel approach to the legal complexities brought about by digital technology.

Modern technologies elicit contrasting emotions in individuals. On one hand, they undeniably bestow substantial benefits upon our lives by simplifying various tasks that would otherwise prove exceptionally challenging. This initially fosters an optimistic belief that technology is a *panacea* for all issues and difficulties, ushering in a new era of societal welfare (*Utopian Visions*). Conversely, as technologies advance, they instill a sense of trepidation, particularly when their increasing complexity renders their inner workings inscrutable. Literature and philosophy adeptly delineate these disparate perspectives on human innovations (*Dystopian Concerns*).

The advent of the internet and computational systems has but intensified these divergent viewpoints. In recent years, in fact, the rapid progress of Artificial Intelligence and blockchain has exerted pressure on conventional constitutional law concepts. The crux of the matter lies in how the deployment of these technologies has facilitated the erosion of state sovereignty and the concurrent rise of the economic and technological power of private corporations. Simultaneously, states have delegated decision-making authority to machines, often under the illusion of their infallibility and neutrality. Over time, age-old issues have resurfaced, albeit in novel forms, due to the integration and occasional replacement of technologies in sensitive domains. This integration has engendered potential discrimination, as exemplified by the use of machine learning in judicial decisions, as well as opportunities for the proliferation of illegal activities, and more. The conundrum lies in crafting legal solutions that address these multifaceted issues, compounded by the technical intricacies of tech-related language, which remain incomprehensible to the layperson. The paramount query now pertains to the constitutional balance between the necessity for regulations that do not hinder technological progress (indispensable for contemporary life) but safeguard fundamental rights (*Legal Realities*).

Privatization of criminal investigation

Milana Pisaric

State's ius puniendi encompasses the right of competent authorities to use coercive mechanisms for the purpose of detecting crime, prosecuting and sanctioning the perpetrators. In case of necessary degree of suspicion that a criminal offense, prosecuted ex officio, has been committed, they have the power, but also the duty, to undertake certain measures and actions in order to collect data and evidence, and to bring the accused to justice. In case of necessary degree of suspicion that a serious crime is being prepared, special investigative techniques can be applied proactively, but exceptionally, if strict conditions are met. With such a legal framework for crime prevention and investigation, intensive work is being done on the creation of technological capacities for the prediction and detection of illegal behavior, based on the use of biometrics, AI, and other technologies.

Still, the purpose of modern criminal proceedings is also to ensure that an innocent person is not punished, while international human rights standards serve to secure that state power is not excessively applied and the guaranteed rights are not unjustifiably limited. Therefore, the application of certain actions and measures to prevent, detect, and prove crime is subject to strict procedural conditions.

These actions and measures are traditionally the exclusive competence of state bodies. Nevertheless, some tendencies in recent years, many of which rest in the gray zone, represent a kind of deviation from this paradigm, leading towards the privatization of criminal investigation. That does not mean the state authorities are renouncing their competence in detecting and proving criminal acts; however, they are increasingly partnering with private sector on several tracks. Here are several examples. The enhanced information sharing mechanism between law enforcement authorities and financial institutions is being fostered. Not only does the state already possess a large amount of data on citizens, but entire databases are being bought from data brokers. In addition, states are buying vulnerabilities and paying hackers to obtain evidence for criminal proceedings. In order to gain access to a device within digital forensics examination, LEA use the service of unlocking a mobile phone remotely, from the company's headquarters, sometimes even outside the territory of the state. Also, competent state authorities use the results of cyber investigations and crypto investigations conducted by individual private companies as their regular OSINT activity.

Private companies act differently and under different conditions compared to the state authorities, which are bound by legal requirements for criminal investigation. By using the products of their services, state authorities indirectly obtain knowledge, data, and material that they otherwise could not obtain lawfully if they acted strictly following the letter of the law and within the scope of their powers and duties. Notwithstanding the eventual effectiveness and necessity of public-private partnerships, the question is whether something like this is acceptable and to what extent in accordance with the rules of personal data processing and criminal procedure, and consequently, whether obtained evidence could be considered legal and admissible in a criminal court.

Heading to Resemblance? The Redress Mechanisms in the Personal Data Protection Policies of International Organizations

Zelin Li

As it has been stated in several international legal instruments on personal data protection, redress and oversight mechanisms are of paramount importance in ensuring the fundamental rights of individuals. While the redress mechanisms in domestic jurisdictions have reached a relatively well-developed stage, similar mechanisms in international organizations (IOs) are not at the same level of maturity. Nevertheless, there are increasing academic attention and political efforts dedicated to the design of redress mechanisms in personal data protection policies of IOs. This paper aims to interact with the current discussion on this topic by offering an inter-institutional analysis of the data policies of the World Health Organization (WHO), United Nations High Commissioner for Refugees (UNCHR), and the International Committee of the Red Cross (ICRC).

Three questions will be asked in the paper. First, what is the role of redress mechanisms in IOs data protection policies, and what factors should be taken into account when we evaluate IOs redress mechanisms? This question is noteworthy, because on the one hand, IOs redress mechanisms can hardly have the same enforceability as domestic jurisdictions, which means that domestic mechanisms should not presumedly serve as a reference framework when we

design the redress mechanisms for IOs. On the other hand, IOs face increasing pressure to provide remedies in case of personal data violations, and several special values have to be considered, e.g. trust, legitimacy and compliance, due to the unique nature of IOs. Therefore, there exists a need to reimage the evaluation criteria of the IOs redress mechanisms.

Second, what are the main features of the redress mechanisms in the WHO, the UNCHR and the ICRC? This paper addresses this question by comparing three elements: the subjects of the mechanisms, namely who provide redress; procedures; and remedies. This comparative exercise is useful to understand how redress mechanisms operate in practice, and it will specially enable us to assess whether their practices are up to the values identified from the first research question.

Third, what are the foreseeable developments of the redress mechanisms in IOs? In answering the first two research questions, the gap between the objectives and the reality has already been identified. Thus, the response to the third question provides suggestions on how to bridge this gap.

This paper borrows the analytical framework from Block-Lieb and Halliday, in which social ecology theory is applied to the study of IOs. It considers IOs as rationale actors in an ecology, whose behaviours are influenced by the overall environment. In this sense, IOs' redress mechanisms are driven not only by the purpose of protecting individual rights but also by the standards that conform the values of the IOs ecology. Guided by this framework, this paper argues that the redress mechanisms in IOs data protection policies are subject to environment- sensitive evaluation criteria, which include the principles that are particularly valued by the IOs system, and since most IOs share these principles, it is likely that the IOs redress mechanisms will resemble each other in the future.

From the Denationalisation of Money to the Central Bank Digital Currencies: a comparative analysis of a new monetary instrument

Giuseppe Naglieri

The emergence of blockchain technology and cryptocurrencies has appeared to pose a serious challenge to the state's monetary sovereignty, its monopoly over currency, the extension of its taxing power, as well as its ability to control international trade and combat crime. This moment, which coincided with the surge of Bitcoin, seemed to realize the idea of denationalization of money proposed by von Hayek in the 1970s and advocated, with different ideals, by various groups, including anarchists and cypherpunks.

In response to the potential risks to their roles in modern political and economic systems, governments and central banks have closely monitored the evolution of blockchain technology applied to cryptocurrencies and its potential risks to economic stability. Nevertheless, as numerous studies have shown, even before the advent of cryptocurrencies, the central banks' monopoly over currency issuance was already in crisis due to the substantial increase in digital transactions involving bank money and the growing and pivotal role of the banking system in money creation and transmission.

It then became evident that, rather than a constraint, the technology underpinning cryptocurrencies could offer an opportunity for governments to both reclaim centrality in relation to bank money and reduce the circulation of cryptocurrencies (considered extremely volatile in value and potentially risky for their speculative use and transaction anonymity).

This is the objective of Central Bank Digital Currencies (CBDC), originally arose as an unsuccessful attempt in Venezuela during an unprecedented inflation crisis, and now

evolved into an ambitious, shared objective for numerous central banks. This includes the People's Bank of China (already launching its E- CNY), the European Central Bank (well-advanced in designing a digital euro), the Russian Central Bank (conducting a digital ruble trial), and the Federal Reserve (which commenced a feasibility study). These endeavors aim to regain centrality within the monetary market, modernize currency circulation systems, reduce transaction costs, and, consequently, reclaim the public's trust and those portions of monetary sovereignty gradually eroded since the 2008 financial crisis.

The proposed intervention seeks to investigate, from a comparative perspective, the debates, underlying causes, approval processes, issuance mechanisms, and operational aspects of the principal Central Bank Digital Currency proposals worldwide. The objective is to identify the diverse legal frameworks in the numerous jurisdictions that have either adopted or are planning to embrace this significant innovation within their monetary systems.

Political parties dealing with digitalization: campaigning rules and electoral process as fields of cooperation between public and private actors

Giulia Sulpizi

In our complex contemporary society, public governance has to deal with innovative emerging digital technologies. Nowadays, they shape European democracies, especially thanks to new social media companies. In this context, the role of political parties is vital, since they act as public actors, through internet-based systems, in order to reinforce their connection with citizens. In this way, they often collaborate with private subjects, that develop new technical tools for electoral propaganda and electoral process. After considering these positive goals, we also have to stress that these means of political participation challenge various public values. In particular, privacy and data become more and more central and they have to be preserved. In this perspective, the existing European legal systems have an important task: it is to define a balance between the use of the above mentioned technologies and the guarantee of people's rights. For this reason, we have to take into account two different fields. On one hand, the electoral campaigning through social media. On the other hand, the whole electoral process, especially dealing with the rules for collecting signatures in support of lists. These issues represent a European problem, common to all State members. This is why the European Commission has launched the *2030 Digital Compass* in 2021, in order to ensure online public access to all citizens, which is the only way to assure true participation to public life. This task is up to political parties, that have to face uncertainty and the lack of trustworthiness of algorithmic public governance. It is no surprise that – in a competitive society – both social and ethical problems arise, alongside with legal considerations. Still, there are two important solutions that we could acknowledge. First, we have to act in the public sector, giving shape to innovative pieces of legislation, to secure political propaganda on social media and promote by design approaches for electoral processes. The European Union has acted through the recent approval of the *Digital Services Act* in 2022 and the *Proposal for an Artificial Intelligence Regulation* in 2021. Secondly, it is even more important to reshape the organization of social media companies, thanks to antitrust and pro-competition law. These reforms might restructure how digital advertising operates and they might break up largest companies into smaller ones, that could compete with each other or create a space for new competitors to emerge.

In conclusion, only through cooperation among public and private actors and stakeholders we could guarantee a vibrant democracy and the protection of end-users fundamental values.