(Virtual) T02P10 / Public Policies for Digital Risks: A Comparative Policy Analysis

Topic : T02 / COMPARATIVE PUBLIC POLICY

Chair : Sivan-Sevilla Ido (University of Maryland)

Second Chair : Shawn Janzen (University of Maryland)

GENERAL OBJECTIVES, RESEARCH QUESTIONS AND SCIENTIFIC RELEVANCE

This panel proposes to comparatively investigate and explain the way public policies are designed and enforced for governing societal problems associated with digital technologies. We seek to develop a comparative understanding on the extent to which traditional public policy theories can explain the policy gaps and failures witnessed in this space. We are also interested in understanding whether digital risks require new forms of governance or should we acknowledge that empirical observations point to the same-old public policy challenges.

The exponential creation, flow, storage, and use of digital information is rapidly affecting individuals, nations, and societies. They face increased risks to cybersecurity, privacy, discrimination, bias, and manipulation aspects, that undermine individual rights, risk our infrastructures, alter democratic principles, and can sway social order. These pressing issues, however, have been mostly studied by sociologists, law scholars, computer scientists, business researchers, and media experts. These problems have received only little attention from public policy & administration scholars, or from political scientists interested in public policy. Consequently, we are curious if this attention deficit allows for a lack in theoretical models that can explain some of the alarming public policy failures of our time. Puzzles include, but are not limited to, questions such as:

Why do very few corporations control most of the digital space (Hill, 2020)? Why has the tech industry's self-regulation culture persisted? Why do cyber threats and data breaches keep expanding without an effective public policy response (Siboni and Sivan-Sevilla, 2018)? How can we explain the narrow framing of privacy vis-à-vis other policy objectives in the policy process (Regan, 1995; Sivan-Sevilla, 2018)? How come platforms have nearly no liabilities for the content they facilitate (Lee, 2020)? Why have the blunt violations of European data protection laws by the digital advertising industry are not leading to significant enforcement (ICO, 2019; Sivan-Sevilla, 2020b)?

On one hand, creating public policies for digital risks may seem like a unique governance challenge. The fact that data is an increasingly important commodity (e.g. Cohen, 2016), the argument goes, changes the way traditional policymaking should work in this space. For instance, digital policy issues can cut across various institutional policy settings, with a wide variety of regulatory ideologies, in ways that are threatening traditional administrative boundaries (Sivan-Sevilla, 2018; Zanfir-Fortuna & Ianc, 2018). Expertise is almost exclusively in the hands of the regulated instead of the bureaucracy and political institutions. Regulated entities hold intimate knowledge about their networks and services, with certain private intermediaries (e.g. cloud services, vendor-controlled platforms) becoming increasingly important governance actors. This requires government officials to find the delicate balance between relying on market forces and intervening for the public interest. Jurisdictional boundaries are also barriers to national policymaking. Governing problems that arise from technologies that are global in nature requires a response that is sometimes beyond the reach of the regulator. This creates tension and introduces friction in governance efforts (e.g. EU-US data transfers, GDPR implementation in the EU, the inability to address global cyber threats).

On the other hand, empirical observations on the creation of public policies for digital risks show that traditional mechanisms are in fact in play, such as the politics of harmonization in the EU (Sivan-Sevilla, 2020a), path-dependency in policymaking (Sivan-Sevilla, 2018), significant private lobbying impact (Atikcan and Chalmers, 2019), or ideational institutionalism (Seidl, 2020). So perhaps the same old traditional drivers for public policy can still sufficiently explain policy outcomes in this space?

CALL FOR PAPERS

We invite papers seeking to advance research on the drivers of public policy outcomes (or non-outcomes) to govern digital risks, focusing on the political dynamics, interest groups, institutional dynamics, and ideational

theories. We encourage papers that adopt a comparative approach to policy analysis (Peters and Fontaine, 2020) and seek to explain any kind of policy variation over time, across nations, or among sectors. We specifically do not want to limit papers to investigate a certain policy level and welcome research on the municipal, state, federal, or supra-national levels of policymaking.

Despite our desire to promote public policy theorization for issues of digital risk, we are open to papers from various disciplines (law, sociology, anthropology, business), as long as their unit of analysis is some aspect of a public policy ecosystem. Papers can adopt a wide variety of theoretical perspectives and methodological approaches to explain what leads to certain outcomes over others.

Our goal is to start and build a research network of scholars that are interested in risks associated with digital technologies and aim to understand drivers for public policy outcomes, highlighting different trends and approaches of policymaking over digital issues. We hope to create a culture of fruitful exchange of ideas that would take us one step closer to a more empowering digital world to live in.

References

Atickan E. O., and Chalmers A. W. (2019). “Choosing lobbying sides: The general data protection regulation of the European Union.” Journal of Public Policy 39(4): 543-64

Cohen, J. E. (2016). “The Regulatory State in the Information Age” Theoretical Inquiries in Law 17(2): 369-413

Hill K. (2020). “I tried to live without the tech giants. It was impossible.” The New York Times, July 31. Available here: https://www.nytimes.com/2020/07/31/technology/blocking-the-tech-giants.html

Information Commissioner Office (ICO). (2019). “Update report into adtech and real time bidding.” June 20, available here: https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf

Lee T. B. (2020). “The Internet’s most important – and misunderstood – law, explained.” ArsTechnica, Oct 6, available here: https://arstechnica.com/tech-policy/2020/06/section-230-the-internet-law-politicians-love-to-hate-explained/

Peters G., and Fontaine G. (2020). Handbook of Research Methods and Applications in Comparative Policy Analysis. Edward Edgar Publishing

Regan, P. M. 1995. Legislating Privacy: Technology, Social Values, and Public Policy. Chapel Hill: UNC Press.

Seidl T. (2020). “The politics of platform capitalism: A case study on regulation of Uber in New York.” Regulation & Governance. Early view. DOI: 10.1111/rego.12353

Siboni G. and I. Sivan-Sevilla. (2018). ‘The Role of the State in the Private-Sector Cybersecurity Challenge.’ The Blog of Georgetown Journal of International Affairs. Available here.

Sivan-Sevilla, I. (2018). “Complementaries and Contradictions: National Security and Privacy Risks in U.S. Federal Policy, 1968-2018”, Policy & Internet 11(2): 172-214, DOI: 10.1002/poi3.189

Sivan-Sevilla, I. (2020a) “Europeanization on Demand: The EU Cybersecurity Certification Regime between Market Integration and Core State Powers [1997-2019].” Journal of Public Policy. DOI:10.1017/S0143814X20000173

Sivan-Sevilla, I. (2020b, forthcoming) “Artificial Intelligence without Data Protection? A Comparative Analysis of National Enforcement Styles vis-à-vis AdTech.” Special issue on AI Governance for the Journal of European Public Policy.

Zanfir-Fortuna G., and Ianc S. (2018) “Data Protection and Competition Law: The Dawn of ‘Uberprotection’” In Gloria González Fuster, Rosamunde van Brakel and Paul De Hert (eds.), Research Handbook on Privacy and Data Protection Law: Values, Norms and Global Politics. Edward Elgar Publishing.

(Virtual) T02P10 / Public Policies for Digital Risks: A Comparative Policy Analysis

Chair : Sivan-Sevilla Ido (University of Maryland)

Second Chair : Shawn Janzen (University of Maryland)

Session 1 [afternoon preference]

Tuesday, July 6th 16:30 to 18:30 (Virtual 31)

(Virtual) Multidimensional Preferences for Regulating Self-Driving Cars. Evidence from a Conjoint Experiment conducted in the US, Japan, and Germany

Sebastian Hemesath (Carl von Ossietzky Universität Oldenburg)

Markus Tepe (Carl von Ossietzky Universität Oldenburg)

Effective governance of self-driving cars requires broad public support. Although policy-makers and practitioners agree upon the growing need to regulate the development of self-driving cars and the importance of regulation that is consistent with citizens' moral believes and societies' legal standards, there is little systematic evidence about which type of regulation citizens prefer and whether the public is sensitive to specific features of possible regulation regimes. In a conjoint experiment, we asked respondents to compare two multidimensional hypothetical regimes regulating self-driving cars and to decide which regime they prefer. The regime profiles varied with respect to three substantive dimensions: (1) Safety (Regulatory body for self-driving cars and safety standards compared to conventional cars), (2) legal framework (liability for accidents caused by the autopilot and ethical prioritization) and (3) autonomy vs. human agency (data protection and supervision of autopilot by the driver). The pre-registered conjoint experiment has been conducted on representative online samples for the USA (N=1,188), Japan (N=1,135), and Germany (N=1,174). Besides the automotive industry being a major industry in those nations, the country selection also reflects anticipated cultural differences regarding the subjective evaluation of AI and autonomous vehicles. However, across all samples, we find that citizens strongly prefer regulation that requires permanent human supervision of self-driving cars and stricter safety standards. Cross-country differences emerge on the safety dimension, as respondents from Japan and Germany prefer public authorities overseeing the approval of self-driving cars, while American respondents show the strongest preference for an independent expert body. Furthermore, in-depth sub-group analysis reveals that preferences towards self-driving cars' regulation are weakly affected by respondents' attitudes towards technology (technophobia), while partisan orientation has only a minor effect on regulatory preferences.

(Virtual) The privacy vs security dilemma: government access comparative policy analysis

Takanobu Sato (Waseda University)

Meryam Azar (Tokyo University of Foreign Studies)

Balancing between protecting personal data and handling security threats have been a major challenge to national security policy makings. After 9/11 in 2001, governments around the world started to perceive the growing threat of terrorism and expand counter terrorism strategies which, consequently, led to more emphasis on security as a first priority.

However, this “national security outweigh privacy” approach became questionable, especially, after the NSA mass surveillance incidence. According to an annual report issued by Director of National Intelligence, the NSA gathered over 151 million records of Americans’ phone calls in 2016, even after the US Congress imposed limitations on its ability to do so. It was also revealed that they examined information related to finance, trade and energy sector without clear justifiable reasons. This incidence raised more concerns about prioritizing national security over protecting privacy in the world. With regard to Japan, the media says that one of those surveillance tools were secretly provided to Japan.

Recently, after the spread of COVID-19 many countries again started compromising privacy and allowing the utilization of personal data in order to contain the pandemic. Moreover, the increasing dependency on digitalization and cyberspace after the pandemic, made it easier for governments to get more access to

personal data and utilize it. This new digitalized era pushed back the questions of “where a boundary should be drawn between privacy and national security” and “how much access governments should have over personal data”.

This article will tackle the problem of how this boundary varies from one country to another, considering the definitions of national security threats and personal data. And it will present a comparative policy analysis of how different governments approach “national security outweigh privacy” vs “privacy outweigh national security” issue in countries with different political environments, such as Japan, the US, China, and the EU. In order to understand the political elements which determine countries’ approach to privacy and security dilemma, it will examine the legislations which authorize governments to access personal data, such as, the US Foreign Intelligence Surveillance Act of 1978 (FISA), and equivalent ones in other countries. Then it will explain how the recognition of national security threats transitioned with the development of these legislations and government accessible range of privacy.

(Virtual) Politicization of Artificial Intelligence: Who drives the Political Debate?

Nicole Lemke (University of Geneva)

Philipp Trein (University of Lausanne)

Frédéric Varone (University of Geneva)

There is a consensus in the literature that usage of Artificial Intelligence (AI) in the public sector will have impacts in many policy fields, such as public health (Sun and Medaglia 2019), defense (Ku and Leroy 2014) and transportation policy (Kouziokas 2017). A fast growing body of literature assesses the technological possibilities of AI applications in different policy fields (Sousa et al. 2019). The potential consequences of this development, both positive and negative, are widespread: Scholars have for example underlined important ethical risks and challenges, such as discrimination, bias, privacy violations or responsibility (Wachter and Mittelstadt, 2019; Mittelstadt et al., 2016; Floridi et al., 2018).

Nevertheless, recent research has also pointed out that there is an urgent need for further investigation into the political and administrative challenges of implementing AI in the public sector (Sharma, Yadav, and Chopra 2020; Sousa et al. 2019). We argue, that in order to understand those challenges, it is necessary to understand the political actors and dynamics aiming to shape the development as well as the use of AI. This article therefore contributes to research on digital risks and digital policy issues by providing an analysis of the politicization of AI. Specifically, we examine which policy issues get attention in the public debate and which actors are driving that debate.

The empirical part of the paper uses quantitative text analysis and discourse network analysis based on novel data from three different arenas of German public discourse on AI, the newspaper discourse, parliamentary debates and a government consultation of interest groups. This allows us to compare which policy issues are salient in the context of AI, which actors such as government, parties, firms or interest groups mobilize, and how actors and issues relate to each other in different arenas. Furthermore, we are able to shed light on dynamics among actors and identify actors central to the debate.

More generally, this article will contribute to understanding the political dynamics behind AI as well as challenges, barriers, and drivers of AI adoption and implementation.

References:

Floridi, Luciano et al. 2018. “AI4People—An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations.” Minds and Machines 28(4): 689–707.

Kouziokas, Georgios N. 2017. “The Application of Artificial Intelligence in Public Administration for Forecasting High Crime Risk Transportation Areas in Urban Environment.” Transportation Research Procedia 24: 467–73.

Ku, Chih-Hao, and Gondy Leroy. 2014. “A Decision Support System: Automated Crime Report Analysis and Classification for e-Government.” Government Information Quarterly 31(4): 534–44.

Mittelstadt, Brent et al. (2016). The ethics of algorithms: mapping the debate. Big Data & Society, 3(2), pp. 1-21.

Sharma, Gagan Deep, Anshita Yadav, and Ritika Chopra. 2020. “Artificial Intelligence and Effective Governance: A Review, Critique and Research Agenda.” Sustainable Futures 2: 100004.

Sousa, Weslei Gomes de et al. 2019. “How and Where Is Artificial Intelligence in the Public Sector Going? A Literature Review and Research Agenda.” Government Information Quarterly 36(4): 101392.

Sun, Tara Qian, and Rony Medaglia. 2019. “Mapping the Challenges of Artificial Intelligence in the Public Sector: Evidence from Public Healthcare.” Government Information Quarterly 36(2): 368–83.

Wachter, Sandra, and Mittelstadt, Brent (2019). A right to reasonable inferences: re-thinking data protection

law in the age of Big Data and AI. Columbia Business Law Review, 2, pp. 443–493.

(Virtual) INTERNATIONAL GOVERNANCE OF TRANSBORDER DATA TRANSFERS: TOWARDS A COHESIVE SYSTEM?

Tatiana Heim (University of Twente)

There is a fragmentation of norms and institutions in the cybersecurity space that could lead to a less consistent legal system that may result in loss of effectiveness, efficiency, and legitimacy of the cybersecurity regime. The fragmentation can raise problems of coordination between the instruments at the international and domestic level. In the context of a fragmented system, the exchange of information and data becomes a major asset to improve cooperation, coordinate responses, develop trust, among others. The free flow of information can promote economic and social development and limit it can be a potential threat in the field of cybersecurity. However, the free flow of information can collide with the right of protection of personal data and bring risks to the individuals. Different international norms try to solve this problem by creating different regulations that deal with the transborder flow of personal data across the national border. However, there has been little attempt by the literature to understand if the international norms are cohesive or conflicting. The article considers only international legal norms that focus on personal data protection and cybersecurity. The conclusion of the article shows that there are conflicting approaches to the transborder flow of data. The conflicts were found regarding the free flow of personal data between the Member States but mostly in the transference of personal data to third countries and organizations. The European Union norms didn´t present any restriction regarding the free flow between the Member States but have a great limitation in the transfer of personal data to third countries. The agreement developed by Shanghai Cooperation Organization is the opposite, they don't regulate the transfer of personal data to third countries but present restrictions about the free flow between the Member States. At last, the article believes that the conflict of norms causes a more complicated and less transparent system, and consequently less understandable for individuals.

(Virtual) Beyond risk regulation regimes: varieties in governing automation and algorithmic risks in the public sector

Regine Paul (Max-Planck-Institute for the Study of Societies, Köln, Germany)

Emma Carmel (University of Bath)

Emma Carmel and Regine Paul

Over the last decade, the use of automated decision-making (ADM) systems in public policymaking and administration – including predictive policing, biometric borders, health care 'optimization', automated 'detection' of social security fraud, or dialect recognition and genetic coding in asylum decisions – has increased in scale and depth. While concern over the social, economic and political risks of ADM applications by the state is well documented, we lack comparative accounts of how and why countries regulate these applications differently. This paper develops a comparative framework for exploring respective policy variety by expanding the perspective of risk regulation regimes with its triple explanatory focus on market failure, public opinion and interest politics (Hood, Rothstein, and Baldwin 2001). We discuss the value and limitations of this classic comparative lens for the regulation of ADM systems in the public realm. We identify three characteristics of ADMs that require an expansion of the risk regulation regime lens: (1) apparent indeterminacy of agency in complex human-machine interactions; (2) the fusion of data, decision rules and enforcement in ADM systems; (3) the highly context-specific interaction of policy, design and practice in real world applications of ADM. Taken together, these collapse the hegemonic conceptual distinctions between policy design/delivery, and between public/private accountability of the last half-century. We discuss how the institutionalist perspective of risk regulation regimes can be adapted to theorize variation in countries' efforts and struggles to address the political, policy and conceptual challenges of these systems.