The Ninth European Multidisciplinary Conference on Global Internet Governance Actors, Regulations, Transactions and Strategies

ABSTRACT COLLECTION

GIG-ARTS 2025

The Rise of Digital Sovereignty: Ambiguities and Challenges

University of Salerno, Italy

26, 27, 28 May 2025

PRIN 2022KTTSBC - CUP Master D53D23007300006
Digital Sovereignty in Comparative Perspective: State Authority, Corporate Power and Fundamental Rights in Cyberspace

PRIN 2020X5LAK7 - CUP Master D43C20000080001
Cybersecurity (As A) Public Policy The Institutionalization Of Platform And Network Security In The Eu And Italy

ABSTRACT COLLECTION

DAY 1 - Monday, 26 May

Paper Panel Session 1 - Conceptualizing Digital Sovereignty

Chair: Dennis Redeker (Bremen University - ZeMKI)

From Sovereignty to Relational Autonomy: a Conceptual Contribution from the Southern Cone

Lucia Bosoer (Universitat Pompeu Fabra/European University Institute)

Abstract

For decades, both political and academic debates suggested that the state was losing relevance as the primary unit in the international order. However, recent global developments have reignited discussions on sovereignty, and the digital realm is no exception. Digital sovereignty has become a central policy priority for many nations, with governments seeking to assert control over digital content and infrastructure to protect their values and interests. These concerns arise not only in relation to other states but also in response to the growing power of a few dominant technology companies.

Despite its prominence, digital sovereignty remains an ambiguous and contested concept. While it broadly implies some level of control over digital technologies, there is no consensus on its precise meaning and implications. Additionally, sovereignty and autonomy are often used interchangeably, further complicating discussions. This lack of conceptual clarity raises a critical question: To what extent does digital sovereignty provide an adequate framework for understanding and fostering self-determination in the digital sphere across diverse contexts?

In Latin America, and particularly in the Southern Cone, the concept of sovereignty has played a less prominent role in academic and political debates compared to autonomy. The notions of dependence and autonomy not only shaped the region's intellectual tradition, but also guided the political action of most Latin American social forces throughout the last century. Within international relations, the School of Autonomy brought together scholars exploring strategies to expand Latin America's autonomy amid longstanding economic and political dependence on the United States. In the 21st century, Russell and Tokatlian (2003) revisited this debate, proposing "relational autonomy" as a normative theory for Latin American countries to approach diverse policy areas and strengthen their self-determination on the international stage.

This paper explores how relational autonomy serves as a more valuable conceptual framework for understanding and advancing digital autonomy in Latin America. While the prevailing literature on digital sovereignty focuses on the narratives and practices of the traditional power centers, relational autonomy provides an alternative perspective that aligns

more closely with Latin America's historical struggles and geopolitical position. By drawing on the theoretical foundations of relational autonomy, this paper discusses its potential implications for the digital domain. Rather than treating autonomy as a rigid assertion of control, relational autonomy invites a more nuanced approach that goes beyond the state as the subject of autonomy and acknowledges interdependence.

In an evolving, non-hegemonic international order, the space for Latin American countries to pursue digital autonomy is likely to expand. However, developing effective policies for digital self-determination requires an analytical framework grounded in the region's specificities and real capabilities. By introducing relational autonomy as a normative theory oriented to political action, this paper not only contributes to the debate on digital sovereignty but also provides a conceptual basis for policies and strategies that meaningfully advance Latin America's empowerment in the digital sphere.

Theorizing Rogue Digital Sovereignty

Marwan Kraidy (Northwestern University)

Abstract

The scope of the growing debate on digital sovereignty has been restricted to states, corporations, social movements, even cyberspace itself, that operate under an umbrella of legitimacy—they are legally and socially recognized as legitimate actors, notwithstanding disagreements about their agendas, practices, and impacts (see Couture & Toupin, 2019)

In contrast, I examine "rogue digital sovereignty." If digital sovereignty is "the exercise of agency, power, and control in shaping digital infrastructure, data, services, and protocolos" (Jiang & Belli, 2025) by legitimate actors, "rogue digital sovereignty" refers to sovereign claims or actions over technology, infrastructure, access, and content by groups that are in violation of global legal, political, and ethical norms.

Like their legitimate counterparts, rogue players assert sovereignty over digital infrastructure and content in two realms. The first, inward-focused is sovereign monopoly control over a territory—physical or virtual—and the population therein. The second, outward-focused is the professed need to protect territory under sovereign claims from external influence, intervention, or threat.

Theorizing "rogue digital sovereignty" lays bare the ongoing ambiguities and unresolved tensions at the heart of "digital sovereignty," which include: interaction between sovereign dominions and the international system; tension between the ideal of sovereignty and its frequent violation by digital superpowers like the United States and China; cybersecurity and cyberterrorism; platform and cyberspace sovereignty, and most importantly, the extension of sovereignty by digital networks beyond territory and infrastructure all the way to the human body. To theorize "rogue digital sovereignty" is to get a better grasp of processes of what Bratton (2015) called "[d]ebordering and overbordering" manifest in the "delinking [of]sovereignty and geography" that lead to an "indeterminacy of outcomes."

To accomplish the above, I focus on digital sovereign claims by "Islamic State" and Western far right groups as case-studies of rogue digital sovereignty, examining a corpus of multi-lingual primary sources (mostly Arabic, English, and French)—manifestos, counterfactual maps, digital currencies, "psychogeographic" drone footage, infographics, videos that make sovereignty claims. I articulate rogue digital sovereignty with affect, elememal media, and infrastructure studies, arguing for a new kind of digital sovereignty that is produced through rogue commandeerings of infrastructure and digitally mediated affective manipulation. This broadens the debate on digital sovereignty to rhetorical claims and media forms that are mobilized in affective and digitally mediated performances of digital sovereignty, and more broadly, sovereignty tout court in the digital age.

Teaching Digital Sovereignty: How Many Bridges to Cross?

Jamal Shahin (BSoG-VUB/UvA/UNU-CRIS)

Abstract

Research Question: Digital sovereignty (DS) emerged as an umbrella term describing the evolving relationship between (state) actors and new technologies. It is marked by questions around control, coordination, and competition in the digital sphere. As discourse and practice, DS profoundly impacts our societies. However, political and technical action in this area requires a blend of policy and technical knowledge: a mixture rarely seen in contemporary educational offerings. Assuming universities aim to support the development of digitally-aware citizens capable of dealing with the technological challenges of the 21st Century, this paper focuses on the interdisciplinary challenge underlying courses that deal with DS. The research question driving this paper is: "What challenges exist when teaching DS, and how can we overcome them?"

(Theoretical) framework: Drawing inspiration from Snow's seminal work, "The Two Cultures," I argue that the distinction between 'hard' and 'soft' sciences is replicated in the contemporary era by those who comprehend technology and those who grasp (technology) policy. Building on Brown's insights (Science in Democracy) and Haas/Williams/Babai's analysis (Scientists and World Order), I emphasise academia's responsibility to 'normalise' interdisciplinary teaching to address pressing policy challenges of the digital age. This framework guides my research approach, which explores how we leverage research (and policy) to inform our teaching practices.

Approach: DS is blooming as a research field, with a richness and diversity in ongoing debates. It provides new insights on Internet Governance (IG) studies, and has helped bridge IG to mainstream Politics and International Relations scholarship. Similarly in the policy field: diplomats now mingle increasingly with IG actors. DS therefore builds bridges, but due to its conceptual heterogeneity, also leads to talking at cross purposes. Whilst richness is suited to research, I argue that teaching DS requires clarity.

Precisely for these reasons, teaching DS is moving more slowly, with only a handful of courses and programmes addressing the topic. It remains difficult to encapsulate the academic debates and the multiple meanings of DS into one (Master-level) course; this paper sets out to inquire whether it is possible and desirable to do so.

Methodology: This paper addresses this topic in a four-stage process.

1. It reflects on conceptual and methodological challenges inherent in teaching DS, drawing upon the theoretical framework described above.

2. It (briefly) provides an overview of the various debates ongoing in the field of DS research, to show how scholars are approaching the topic (which influences education).

3. It surveys a number of instances of courses and university-level programmes that cover DS as a central theme, gathering best practices. Due to the nature of the research at this stage, this will be limited to Dutch and Belgian universities.

4. Finally, it will draw out a number of suggestions for areas where educators can enhance educational offerings in DS.

The paper will conclude with some reflections on how DS can collapse persistent divides in university curricula, including the science-policy nexus and the need for truly interdisciplinary educational offerings.

Digital Sovereignty and Central and Eastern Europe: Thinking Digital Politics from a Semi-Periphery

Jakub Eberle; Linda Monsees (Institute of International Relations Prague)

Abstract

This paper is a draft of a conceptual introduction to a Special Issue on Digital Sovereignty and Central and Eastern Europe (currently under review). Despite the relative abundance of studies, the existing research on digital sovereignty has focused almost exclusively on policies and discourses at the EU level, or the role of big states, particularly Germany and France (Rone 2024, 6). This dovetails with the biases of broader literatures on digitalisation, which also tend to research above all 'wealthy democracies of the European Union's (EU) core', ending up with only 'a particular, and particularly limited, understanding of digital transformation' (Rothstein 2024, 229). In contrast, there is virtually no published academic research on the adoption, formulation or contestation of the digital sovereignty agenda in Central and Eastern Europe (CEE), and very little research conducted by scholars located in or originating from the region (exceptions include Kaloudis 2021; Csernatoni 2022; Monsees and Lambach 2022; Lambach and Monsees 2024; Ivi? and Troitiño 2022). The absence of CEE from the scholarly debates on digital sovereignty are neither surprising, nor unfamiliar to scholars working on the region, as this closely reflects prevailing trends in geopolitics of knowledge production. Over the last few years, and with a renewed vigour since Russia's full-scale aggression against Ukraine in 2022, these trends have been increasingly highlighted and criticised. A growing amount of literature is now pointing out the 'relative ignorance of Eastern European insights and their validity' (Mälksoo 2022, 471) in multiple disciplines. This is both an academic and a political problem, as it not only impoverishes our understanding of European politics, including digital politics, but also reinforces existing hierarchies, in which the condition of large Western European countries is considered more important by default. Yet, without the inclusion of CEE perspectives (or, indeed, those from Southern Europe, which is similarly overlooked in the literature, see Rothstein 2024), the broader academic debate cannot arrive at a more nuanced and complete understanding of European politics, and fails to gain a reflexive image of its own blind spots. In the paper, we will discuss the position of CEE countries in Europe in relation to two existing literatures that conceptualise the structural disadvantages that CEE states struggle with: (a) small states in world politics and (b) the hierarchical structure of transnational capitalism, as shown in

dependency research. We use these literatures to craft our argument concerning the dual disadvantage of (most) CEE states, and discuss how it relates to digital politics.

Paper Panel Session 2 - Geopolitics of Digital Sovereignty

Chair: Carlos Fonseca (Ghent University/UNU-CRIS)

Informational Sovereignty: Website Infrastructure Dependency and Geopolitical Risk in Latin America

Juan Ortiz-Freuler (Annenberg/USC)

Abstract

This paper explores the boundaries of sovereignty by showing the infrastructural dependency of Latin American newspaper websites on dominant global players, and how it can compromise journalistic autonomy and the ability of a public to make informed decisions. The paper places itself at the intersection of three bodies of literature: the increasing centralization of the internet and its impact on sovereignty (Aguerre et al,, 2024; Pohle & Santaniello, 2024); the ongoing crisis in the media sector and its effects on democratic systems (Ananny, 2018; Pickard, 2023); and the decades-old demands for a New World Information and Communication Order (NWICO), which sought to rebalance power dynamics in global information flow (Masmoudi, 1979; UNESCO, 1988). By dissecting the role of infrastructural consolidation in shaping media practices in Latin America, this paper contributes to the broader conversation on sovereignty by specifying how control over key infrastructure (DeNardis, 2013; Musiani et al., 2016) can limit autonomy.

Through an empirically grounded analysis of 18 media outlets from six Latin American countries, this paper highlights the vulnerability of these newspapers to external coercion stemming from the concentration of the underlying digital infrastructure. Drawing on a newly constructed database of over 400 data points, the study analyzes 11 critical elements of the media stack essential for online newspaper operations. The results reveal that dominant technology providers such as Alphabet (Google) and Meta (Facebook) pose significant commercial risks to media outlets. For example, reliance on these providers for analytics, advertising, and content delivery centralizes control, leaving newspapers financially and operationally dependent. Geopolitical risks are also acute: 50-100% of providers in each of the 11 infrastructure segments analyzed operate under US jurisdiction, making them subject to US law. This dependency introduces vulnerabilities, as evidenced by cases where the US government leveraged its jurisdiction over such companies to pressure adversaries, such as Venezuela, Iran, and Russia. The findings suggest that similar mechanisms could be weaponized against Latin American countries, particularly as countries within the region deepen ties with China. Beyond the direct risk to media companies, the dependencies might offer a good proxy to understand the degree of geopolitical risk a nation's economy is subject to.

Two conclusions emerge from the analysis. First, there are tangible points of control within digital infrastructure that enable the exertion of commercial and geopolitical pressure on Latin American newspapers, thereby raising concerns about editorial independence and informational sovereignty. Second, addressing these vulnerabilities requires a normative shift in media policy. The paper draws parallels to the Non-Aligned Movement (NAM) and its strategies for decolonizing global communication networks in the 1970s and 1980s, suggesting that these approaches could inspire contemporary efforts to protect sovereignty in the digital realm. NAM's focus on building independent infrastructures and fostering regional cooperation offers particularly valuable lessons for disentangling choke points in digital infrastructure today.

To address the challenges posed by infrastructural dependency, the paper calls for an observatory to monitor these risks over time. Such an initiative would provide actionable insights into the vulnerabilities of digital infrastructure to researchers and policy-makers.

Processing Digital Sovereignty in Western Balkan States: Sovereignty Deficiencies Amid EU Accession and US-China Digital Technology Rivalry
Ana Bojinović Fenko; Anastas Vangeli; Faris Kočan (University of Ljubljana)

Abstract

This paper explores how technological rivalry between the United States (US) and China impacts digital sovereignty of Western Balkan (WB) states. We grasp the limitations in their own exercise of sovereignty (youth, smallness, post-conflict status, economic dependency) via two clusters of structural conditions, namely their European Union (EU) accession process and position of the region as an interest sphere. Re-articulation of sovereignty through digital technologies is analysed as sovereignty over (development and control over digital infrastructure) and sovereignty through (the use of digital technologies for domestic rule and governance). We explore the impact of alternative (digital) paths in the WB as envisioned by the EU, the US, and China via two case studies: the Chinese "Digital Silk Road" and the US' "Clean Network Initiative". The results show that in effort to achieve competitiveness against China, the US and the EU initiatives are compatible in terms of sovereignty over, yet their impact is not entirely in-sync with regards to sovereignty through since the 'European way of life' sets a more politically demanding digital sovereignty agenda for WB states' governments compared to US' market-based logic. A pivotal insight is that differences between the EU, US and China increase WB states' choice of both aspects of digital sovereignty which they make pragmatic use of and thus establish themselves as anything but passive recipients of external powers' digital policies.

Kings vs Giants: Mapping the Struggle for Sovereignty in the Digital Age
Sara Concetta Santoriello; Giuseppe Borriello (University of Naples "Federico II")

Abstract

The concept of sovereignty, a cornerstone of political science, has gained critical relevance in international and geopolitical digital relations, reshaping power dynamics between States and Corporations. Historically, Corporations have posed significant challenges to State sovereignty, a dynamic rooted in longstanding debates on the modern times. Contemporary analyses emphasize the growing influence of Corporations, particularly in the digital domain, where they emerge as dominant actors.

One key tension lies in the erosion of State authority and its ability to maintain control over internal and external dimensions of governance. This study examines the tools, methods, and actors mobilized by States to defend their sovereignty in the cyber domain. By addressing the digital challenges posed by Corporations, States are attempting to rebalance power dynamics and assert their authority in cyberspace.

Although countermeasures—such as stringent regulations, heavy fines, and digital bans—are still in their infancy, they show promise as deterrents capable of reasserting State control. Corporations headquartered primarily in the USA and China are frequently perceived as

threats due to practices such as data mining, privacy breaches, and the exploitation of strategic assets.

This study seeks to identify which actors are responsible for enforcing measures against corporations—courts, government agencies, or independent authorities—and to evaluate the effectiveness of these measures. It also explores the relationship between Corporations and independent authorities in their home countries, shedding light on the complexities of regulatory frameworks.

Relevant cases were collected using keyword searches (e.g., “State name” vs. “Corporation name”) on search engines such as Google, Ecosia, and Bing. The resulting dataset includes official documents (e.g., rulings, fines, judgments) related to disputes, categorized by type, issuing authority, and outcome. This qualitative approach provides a comprehensive mapping of measures, actors, and results in state efforts to defend digital sovereignty.

Findings reveal that States are increasingly taking action to counter corporate influence, though with varying degrees of success. For example, China’s strategic investments and U.S. policy alignments with major tech companies illustrate how States can leverage corporate dominance to strengthen their sovereignty. Conversely, other States face significant challenges in enforcing regulations or imposing penalties on global corporations. The analysis explores the possibility that bans, whether total or partial prohibitions of activities, are replacing embargoes—strategic economic policy measures restricting or prohibiting trade—as a means to protect national authority.

This study contributes to the broader literature on sovereignty by highlighting the evolving role of digital corporations and offering a systematic framework for analyzing State responses. It provides a comparative analysis of measures adopted by G20 countries, identifying prominent tools, the corporations most affected by sanctions and litigation, and the broader implications for geopolitical power dynamics.

By focusing on the intersection of sovereignty and the digital domain, this research underscores the importance of robust, adaptive strategies for States to navigate the complex and rapidly evolving challenges posed by Digital Corporations in the 21st century.

From Internet Freedom to Digital Sovereignty: the Politics of Global Norm Contestation

Tetyana Lokot (Dublin City University); Mariëlle Wijermars (Maastricht University)

Abstract

Our research examines how and why the norm of internet freedom has changed over time and the global politics of its promotion and contestation. While the global norm of internet freedom has become widely accepted, we analyse how the various subnorms constituting it have been continually contested by actors with changing degrees of power and influence – states and international organizations, civil society, corporations, technological and academic communities – acting as “norm entrepreneurs” (Finnemore & Sikkink, 1998).

While multistakeholderism, rooted in the overall normative acceptance of internet freedom, became a core feature of modern internet governance, the perception of growing threats to

the open internet has precipitated the "return of the state". Today, nation-states are reasserting control over the meaning of a "free internet", but also over the limits to this freedom. Meanwhile, states and non-state actors struggle to exert control over data, digital infrastructures, and technological ecosystems, navigating the challenges posed by the global nature of the internet and the influence of technological corporations.

Many countries are now advocating for increased state power in the digital domain and adopting measures to strengthen their digital sovereignty (Pohle & Santaniello, 2024). From viewing the curtailment of state intervention as a core component of the internet freedom norm, grounded in Western notions of liberty, the global conversation has shifted to accepting that (some) state intervention may be necessary, either to prevent human rights violations or to ensure internet freedom is protected from harmful interference by (other) states and private actors.

While digital sovereignty has become a robust scholarly field, it hasn't been explicitly connected to the norm of internet freedom. Making a unique contribution to this domain, we draw upon the constructivist IR theory of norm contestation (Wiener, 2014; Niemann & Schillinger, 2017) and scholarship on cyber norms (Radu et al., 2021) and consider to what extent uncertainty around the role of state intervention has motivated the shift from conversations about internet freedom as an established norm to debates about digital sovereignty. Using publicly available data, we analyse statements and debates by states and international bodies in key global (ICANN, ITU, IGF) and regional (EU, RCC, ASEAN, BRICS) fora over the past five years to identify relevant narratives about digital sovereignty and internet freedom, and to categorise the various strategies and arguments employed in the process of norm contestation in these spaces. We ask whether digital sovereignty is, in fact, emerging as a new global norm – one that overlaps with, but also co-opts the idea of internet freedom to legitimise potentially problematic practices and policies, while empowering states to exercise national restrictions on content, practices and infrastructures, and to make decisions that may not be for the global good.

We show how the various interpretations and contestations of digital sovereignty proposed by national, regional and global actors may reshape or even undermine the very idea of internet freedom as a global norm, instead proposing a more "promising" normative framework that cements state interventionist power and responds to fears provoked by the perception of the waning democratic potential of the free and open internet.

Paper Panel Session 3 - Digital Sovereignty and Security

Chair: Francesco Amoretti (University of Salerno)

How Emerging Security Communities Moderate Cybersecurity Governance: an EU Case Study

Hannah-Sophie Weber (University of Oxford)

Abstract

In international cybersecurity governance, public-private interaction is daily fare. Despite this, two models of conflicting nature pervade contemporary rhetoric in European Union (EU) cybersecurity governance: the co-regulatory, inclusive allure of multistakeholder governance, on the one hand, and the state-centric model of European digital sovereignty, on the other hand. But what explains puzzling public-private alignment behind these multistakeholderist and sovereignist models in EU cybersecurity governance? Extant

literature sheds surprisingly little light on the link between (often informal) everyday public-private interaction and contested high-level discursive rhetoric. Studies that look beyond well-structured, formal multilateral alliances and towards fuzzy networks and informal coalitions of the willing in security politics exist, but the topic remains too peripheral. This persistent lack of scholarly attention to informal practices – instead of formal policies – stands in the way of a thicker understanding of ordering processes around digital infrastructure.

This article introduces the ESC framework – a practice-theoretical framework of emerging security community (ESC) – for the analysis of informal public-private interaction in cybersecurity governance. Officials at relevant EU institutions and agencies are considered as 'public', while 'private' actors are the representatives of large non-EU technology companies. Drawing on epistemic community theorising in inter-state relations enables a new understanding of everyday interaction among public and private actors. Epitomising informal and operational interplay around digital infrastructure, the selected case of the European Cyber Agora ecosystem helps empirically unpack the interaction black box through a combined case-study approach. This selected crucial case of the Agora ecosystem bears intrinsic value and empirical significance, making it illustrative and useful for exploring new hypotheses. It is a carefully selected case of a key informal venue for interaction in EU cybersecurity governance.

Relying on practices as key units of analysis, the empirical inquiry combines process tracing with a complementary theories congruence analysis. This combined research design helps account for complementary explanations provided by extant theorising of norm entrepreneurship and the 'Brussels Effect'. It pinpoints the strengths and weaknesses of these two key alternative accounts while making more nuanced overall inferences regarding the step-by-step process behind the informal public-private alignment. Expert interviews with a set of public and private practitioners provide access to their ad-hoc, daily work and individual perceptions of it. Drawing on valuable primary data within a practice-theoretical framework, this paper finds that the moderating ESC mechanism helps explain public-private alignment behind the two conflicting governance models.

The proposed ESC framework opens up a range of new avenues for further academic and policy research on how normative governance models are informally constituted through daily practices. Scholarship must consider the host of different actors engaged in cybersecurity governance, as well as their ways of interacting within – and increasingly across – different sectors. Emerging security community is shown as a theoretically grounded, praxeological mechanism that has not yet received sufficient attention. Drawing on rich exploratory empirical insights from this case study, the paper contributes to filling a broader gap in the literature on public-private interaction in international cybersecurity governance.

Digital Sovereignty and European Cybersecurity Policy: Shaping a Unified Future

Giuseppe Borriello; Gaia Fristachi (University of Naples "Federico II")

Abstract

As digital threats and shifting geopolitical tensions redefine global power dynamics, sovereignty is no longer confined to territorial borders but is increasingly measured by a state's capacity to assert control and maintain security in cyberspace.This paper examines the concept of digital sovereignty within the European Union (EU), focusing on its internal and external dimensions in relation to cybersecurity and state autonomy. Situated within the political science literature on sovereignty in the digital age, the study addresses the interplay between cybersecurity, defense, and national governance.

The theoretical framework is built on three key assumptions. First, national cybersecurity, as part of broader defense and security efforts, is indispensable for safeguarding state sovereignty, particularly in the digital realm. With cyberspace playing an ever-greater role, protecting critical national infrastructures and information systems is essential for governments to maintain control and independence. Second, the EU continues to face a sovereignty deficit, particularly in its defense and security policies. Although various proposals for a unified European defense have been made, NATO membership has historically impeded significant reforms. However, recent geopolitical shifts, notably the 2022 Russian invasion of Ukraine, have reignited interest in strengthening European defense, with cybersecurity becoming a central concern. Third, the paper applies institutional isomorphism theory, particularly its technological variant, to argue that the adoption of common technologies across EU member states fosters shared organisational structures, practices, and institutions, thereby enhancing digital sovereignty and contributing to a more unified European political and economic framework.

This study hypothesizes that a coordinated EU cybersecurity policy can bolster European digital sovereignty while accelerating political unification. It posits that establishing national cybersecurity agencies under EU-level coordination, harmonizing regulations across member states, adopting shared defense technologies, and standardizing monitoring practices can strengthen digital sovereignty. These measures would also advance the integration of European defense and security policies, promoting greater cohesion among EU member states.

The central research question guiding this analysis is: How are EU member states coordinating their digital cybersecurity policies? To address this, the paper develops a dataset encompassing all 27 EU member states, analyzing critical variables such as: (1) the existence of national cybersecurity agencies; (2) the alignment of national cybersecurity strategies with EU directives; (3) the publication of national cybersecurity reports; (4) the enactment of cybersecurity legislation consistent with EU regulations; and (5) the adoption of shared cybersecurity technologies across member states.

Preliminary findings indicate a growing trend toward the harmonization of organisational and procedural practices among EU member states, although NATO directives continue to dominate the defense landscape, limiting the EU's cybersecurity autonomy. Nonetheless,

significant progress is evident in strengthening European digital sovereignty. Enhanced policy coordination, the gradual standardization of technologies, and the reinforcement of EU-wide legal frameworks are paving the way for a more integrated European defense and security system. These advancements provide a foundation for greater cohesion and sovereignty within the EU. This study contributes to academic debates on European integration and offers actionable insights for policymakers seeking to navigate the challenges and opportunities of digital sovereignty in an evolving geopolitical context.

Private Actors in Law Enforcement and Digital Sovereignty in the EU

Ryoko Arakawa (KU Leuven)

Abstract

The rapid advancement of biometric technologies results in the acceleration of the partnership between Law Enforcement Agencies (LEAs) and private actors across the European Union (EU). Development and operation of facial recognition, fingerprint databases, and iris-scanning systems are heavily relying on the technologies provided by third parties. Although these technological developments contribute to public order, they also raise critical concerns about digital sovereignty. The purpose of this paper is to answer the question: Who owns these sensitive data when private actors are involved in biometric data processing for law enforcement operations, and how does it undermine digital sovereignty in the EU?

This study investigates the relationship between LEAs, private actors, and citizens from the perspective of digital sovereignty, focusing on biometric data processing by third-party technologies. It examines whether state dependence on private biometric technologies compromises digital sovereignty and law enforcement autonomy while also considering the risks of state-controlled biometric systems lacking transparency and accountability, which may threaten democratic values. Although EU legal frameworks such as the General Data Protection Regulation (GDPR) and the Law Enforcement Directive (LED) (Directive (EU) 2016/680) provide stringent data protection guidelines, challenges emerge when biometric data are processed under exemptions.

In order to address these issues, this study first examined the technological development of biometric data processing and its implications for law enforcement in the EU. After the examination of technological aspects, it conducts a legal analysis of key EU frameworks. This includes the GDPR, LED, and the EU Charter of Fundamental Rights in order to assess how current legal frameworks regulate private sector involvement in law enforcement operations.

Accordingly, this paper conducts a case law analysis of the key Court of Justice of the European Union (CJEU) rulings, including Schrems II, which invalidated the EU-U.S. Privacy Shield due to insufficient safeguards for EU citizens' data and Ligue des droits humains v. Belgium case, which emphasised the need for adequate legal protection when processing law enforcement data. It also examines practical examples, including IDEMIA, a French company that collaborates with the French government on law enforcement, and Clearview AI, a U.S.-based facial recognition company that was fined by multiple EU member states for the infringement of the GDPR.

The expected results imply that, although LEAs retain de jure ownership of biometric data, private actors frequently exercise de facto control over these sensitive data, especially through cloud infrastructure, software, and algorithmic processing systems. This raises serious concerns in regard to digital sovereignty in the EU. Finally, this study highlights the significance of accountability in law enforcement to tackle such concerns and promote digital sovereignty.

DAY 2 - Tuesday, 27 May

Paper Panel Session 4 - Platform Sovereignty

Chair: Fortunato Musella (University of Naples "Federico II")

Digital Sovereignty and Local Governance: Social Media, Public Order, and the Challenge of Platform Content Regulation

Willem Bantema; Laura Postma; Denise de Boer (NHL Stenden University of Applied Sciences)

Abstract

This paper explores how Dutch municipalities, particularly mayors, maintain public order in an era where social media fuels offline disturbances. Examining digital sovereignty and local governance, we highlight challenges posed by extraterritorial social media influence and outdated legal frameworks. Using Alkmaar and municipality X as case studies, we analyse how online incitement escalated into public order crises, exposing municipal vulnerabilities.

Key challenges include jurisdictional constraints, lack of predefined protocols, and limited platform cooperation. Strengthening online information positions, integrating digital crisis management, and fostering cross-sectoral cooperation emerge as critical solutions. The Alkmaar and municipality X cases, involving online-fuelled public unrest, underscore the need for proactive strategies, such as real-time sentiment monitoring and targeted communication. However, barriers in platform cooperation and jurisdictional ambiguity remain hurdles.

The Alkmaar case illustrates the complexity of online-incited disturbances during the AZ-Legia Warszawa football match, where misinformation and digital mobilization escalated into security threats. Municipality X faced a crisis following viral misinformation about a local criminal case, highlighting the role of influential figures in escalation. Both cases emphasize early intervention, digital literacy, and collaboration between municipalities, law enforcement, and community stakeholders.

We propose a hybrid governance model combining legal and communicative strategies to enhance digital sovereignty while safeguarding rights. Insights from these cases demonstrate how municipalities can balance digital interventions with constitutional safeguards.

This research contributes to public order enforcement in digital spaces, offering recommendations for policymakers and scholars navigating platform power. It engages key questions on:
• Digital sovereignty: How can fundamental rights be protected while local governments intervene online?

• Platform regulation: What role do municipal interventions play in shaping broader platform policies?
• The governance paradox: How can authorities act without overreaching digital freedoms?

Research Question: To what extent do local governments contribute to the broader governance of digital spaces while addressing online-incited disturbances and navigating platform power asymmetries?

A mixed-method approach includes a literature review on legal and ethical municipal powers and empirical research in Alkmaar and municipality X. Semi-structured interviews with policymakers, legal experts, and stakeholders (N=20) provide key insights.

Dutch municipalities struggle with the extraterritorial nature of social media platforms and outdated legal structures. The Alkmaar and municipality X cases highlight intervention barriers, including platform cooperation and jurisdictional conflicts. While real-time sentiment monitoring and proactive platform collaboration are effective, privacy, proportionality, and freedom of expression concerns persist. Strengthening alternative strategies, such as improved and proactive social media communication, is crucial.

This paper advocates for a hybrid governance model that blends legal and proactive communicative strategies to enhance municipal digital sovereignty while safeguarding rights. Updated legislation, improved cross-border platform cooperation, and clearer local authority roles are essential. Lessons from Alkmaar and municipality X highlight the urgency of proactive digital governance, offering valuable insights for municipalities managing online public order threats.

Decentralised Social Media Initiatives within European Public Service Media. Towards a Public Service Social Media?

Joan Pla (Østfold University College)

Abstract

Several European Public Service Media (PSM) organisations have, in the last two years, initiated accounts on Mastodon, a decentralised microblogging service that uses the W3C's open standard social networking protocol ActivityPub. Decentralised social media (DSM) services like Mastodon provide a socio-technological countermodel to corporate social media (CSM) platforms such as X, Facebook, or TikTok.

By distributing the ownership and governance of servers on a federated network (the so-called Fediverse), these emerging social media services are posited as alternatives to tackle adverse societal issues associated with the centralised model of CSM: appropriation and commodification of users' data, proliferation of misinformation and hate speech, manipulation of public opinion through tailored algorithms, fragmentation of audiences, and political disengagement.

This paper aims to explore this hypothesis both theoretically and empirically through a multi-case study of PSM organisations in Europe, focusing on an interdisciplinary analysis of social media platforms' economic, journalistic, and political impact. By taking PSM as the unit of analysis, we seek to determine whether their motivations for using DSM align with their public values and legal remits. The primary method of empirical data collection involved interviews with members of PSM organisations such as ARD in Germany, NPO in the Netherlands, and BBC in the UK. Their responses were supplemented with secondary sources and a review of national and European-level public media policies. Additionally, we investigated the operational challenges they faced.

Our preliminary findings reveal that most Mastodon accounts initiated by PSM organisations were started by innovation departments, interested in the technological implications and potential of alternative social media platforms. Thus, the individual and ad hoc origin of these initiatives, rather than an institutional commitment, has so far constrained their success as measured by the number of followers and user engagement. The limited audience reach has led to the suspension of some of these trials, despite requiring minimal additional resources and providing greater congruence with PSM mission compared to CSM.

In the future, it will be crucial for these organisations to develop an institution-based strategy to use social media effectively, achieving engagement goals without sacrificing the public values embedded in PSM. Such a strategy will ultimately contribute to effectively fulfilling their counterweight role in the media ecosystem.

Towards a "Federated Sovereignty"? Mobilizations of Decentralized Platforms for (European) Digital Autonomy

Ksenia Ermoshina; Francesca Musiani (CNRS)

Abstract

Federated or decentralized social networks and messaging services are often perceived by the general public (and even analyzed by some specialists) as technological utopias used by audiences with very specific characteristics, relatively marginal and sparse in number. However, the Fediverse is currently experiencing a rise in popularity (La Cava et al., 2021; Rozenshtein, 2023) which coincides with a number of spectacular and problematic developments in the ownership and moderation policies of platforms such as X and Facebook, and in parallel, with the development of digital sovereignty strategies by many States in Europe, and of the European institutions themselves (Roberts et al., 2021). Indeed, faced with the domination of the secure messaging market by services hosted in the United States (e.g. WhatsApp, Signal), Europe is seeking to deploy alternatives.

This contribution aims to explore how the different technical properties of federated solutions (such as interoperability, self-hosting, portability, modularity, etc.) are currently invoked and mobilized by specific Internet regulators in order to serve the objectives of digital and infrastructural autonomy. The more general question raised by this article concerns the controversy surrounding the reuse, or even the co-optation, by different institutional and regulatory actors, of alternative tools and protocols developed by free software communities, often carrying libertarian and/or anti-authoritarian values.

The article is based on research conducted by the authors since 2016 (see in particular Authors, 2022; Authors, forthcoming 2025), which explores the promises and limits of the "alternative Internet", in particular, so-called "federated" communication tools. This multi-site and interdisciplinary study is based on interviews with tool developers, with administrators of the servers or "instances" that maintain and develop the Fediverse ecosystem, or with specific experienced users (in particular, digital security trainers). It also mobilizes interviews with representatives of public administrations and international Internet governance organizations.

Following an approach informed by science & technology studies – more particularly infrastructure studies and critical code studies –, part of the analysis is devoted to source code repositories, "white papers", documentation, project websites and user forums. We have conducted numerous observations at the major offline and hybrid gatherings of the free software communities such as FOSDEM and Chaos Communication Congress. In addition, we conducted several years of participant observation within the development team of the encrypted messaging service Delta Chat. This long-term observation allowed us to closely

follow internal discussions around questions of collaboration with public entities and better understand the technical decisions taken by the team, in particular those leading towards a certain form of recentralization, a paradox of federated tools that we described in previous work (Authors, 2022).

A Case of 'Strategic Hedging'? Contestation and Adoption of Norms in Social Media Governance in Indonesia

Treviliana Eka Putri (University of Groningen)

Abstract

Social media platforms have established a form of global governance manifesting through their platform design. This is visible, for instance, through the practice of content moderation implementing a universal values (DeNardis, 2015; Griffin, 2023), which best described as a "one-size fits all" approach . It is often argued that these universal values are merely a facade, allowing western big tech companies to impose values on the majority of the global population. Scholars such as Gillespie (2018)critically assessed the power of platforms in shaping public discourse through such content moderation. If users outside the West wish to use social media, they have virtually no choice but to accept practices established. This raises the question how countries in the Global South, where most users come from, situate themselves among the competing norms and values?

Analysis of social media governance is often focused on the United States, Western Europe, and more recently, China. This should come as no surprise. The 'innovation power' of the United States created a path dependency for others using and adopting technologies developed there. The European Union's 'regulatory power' has undoubtedly shaped the global regulatory governance of social media. Furthermore, China challenges the existing order by establishing new platforms. These examples sketch how national and regional governance have a significant extraterritorial impact.

This study examines how norms are contested and adopted, highlighting the factors that influence this process. It focuses particularly on social media governance in Indonesia, as a representative of the Global South countries. Indonesia's landscape of digital technologies and social media platforms serves as a canvas portraying the competition between the US and China as technology exporters. In addition, Indonesia adopts regulations influenced by the EU, such as the newly enacted (2024) Personal Data Protection (PDP) Law.

The research employs a case study approach with process tracing by collecting data from legal texts, existing policies, academic reviews, and public discourse around social media governance in Indonesia. It utilizes a constructivist approach to international norm diffusion (Finnemore and Sikkink, 1998) exploring how "norm entrepreneurs" such as the US, EU, and China influence and convince the government to adopt their norms. It will also operationalize strategic hedging (Kuik, 2021) as a concept where a small state manifests a mixed element of selective engagement, limited resistance, and partial deference against the great powers.

This study argues that Indonesia applies a selective norm adoption. Moreover, in maneuvering the competition, it applies a hedging strategy to leverage its position. The strategy seems to be to benefit from the US-China tech rivalry, while selectively endorsing some of the EU's regulations to project the image of a good international actor.

Paper Panel Session 5 - Decolonial and Indigenous Perspectives on Digital Sovereignty

Chair: Jan Aart Scholte (Leiden University)

Can We Decolonize the Internet?

Henna Zamurd Butt (University of Chicago) and Marianne Franklin (University of Groningen)

Abstract

The past decade has seen scholars grapple with enduring injustices that persist - even as they are reshaped - through the internet's expansion and development across then globe. Scholars, and politicians, who critique the legacies of imperialism and colonialism have illuminated the myriad ongoing continuities from a range of theoretical positions on the relationship between technological transformations, society and politics. The central research question of this project and its main output - a forthcoming edited volume - asks: can we decolonize the internet? If so, how? And if not, what then? Internet Decolonized (Oxford University Press, forthcoming) presents the outcome of two years of dialogues and collaborations amongst activists and researchers.

This project brings together internet governance scholarship in the Global South (Oppermann 2018) and theory and research interrogating Global North dominance in policy and scholarly domains. The collective output throws into relief synergies, and differences, amongst approaches that draw from Indigenous, decolonial, postcolonial, and anticolonial schools of thought and action. Another inspiration, and primary motivation for this project, is to bridge gaps in existing scholarship on internet - media, platform, AI - governance with groundbreaking work on the role of colonialism and coloniality in early internet developments; Miryam Aouragh's Palestine Online (2012), which examines Palestinian resistance in digital spaces, Lisa Nakamura's Cybertypes: Race, Ethnicity, and Identity on the Internet (2002) and Ziauddin Sardar's Cyberfutures (1996, co-written with Jerome Ravetz). These foundational works provide a critical lens and an entry-point for empirical research addressing more recent debates around how the role of digital colonialism (Nyabola, 2018), surveillance capitalism (Zuboff, 2019), and data colonialism (Coleman, 2019; Couldry and Mejias, 2019) perpetuate the relationship between Empire (slavery, extractive processes, and environmental degradation) and the 'short history of the internet', in the words of Steve Jones (2002).

The interdisciplinary nature of this project is reflected in a methodology that positions the politics of knowledge production, ownership and control, and terms of reference as core parameters. Some of our key methodological decisions in curating the research, advocacy and policy insights that participate in the volume include: (1) collaborative authorship, engaging contributors whose expertise spans theoretical intervention, historical inquiry, engaged policy work, and activist organizing; (2) facilitated workshops hosted at the University of Groningen in 2023 enabling authors to present their ideas, collaborate with each other, and refine their contributions in conversation with one another and the editors; and (3) welcoming a range of topics, approaches and styles, acknowledging epistemic plurality.

The output features eleven original chapters that address the findings along the following themes: undersea cables and legacies of enslavement; the implications of community networks on governance; internet governance and its histories; Pan-Africanism and digital constitutionalism; internet access management; experiences of youth organizing; how to

bridge Indigenous epistemologies with digital technologies; language justice online; the metamorphosis of human rights into 'digital rights'; the weaponization of internet decolonization by autocratic leaders; methodological dystopianism and decolonial computing; and hopeful speculation on whether another internet is possible.

Reclaiming Sovereignty or Reinforcing Marginalisation? Anti-Gender Movements, Digital Sovereignty, and the Framing of 'Gender Ideology' as Neocolonial Imposition

Karolin Rippich (Dublin City University)

Abstract

The rise in digital sovereignty has ignited debates about its dual role as a tool for national autonomy and a mechanism for authoritarian control. Against this background, Hungary's 2021 "anti-LGBTQ+ law" exemplifies how digital sovereignty is increasingly weaponised to justify censorship and marginalisation, in this case, under the guise of child protection. By framing LGBTQ+ content as harmful to children, Hungary aligns with broader anti-gender movements that depict 'gender ideology' as a harmful neocolonial imposition by "leftist forces" in Brussels.

The Commission contending that Hungary's "anti-LGBTQ+ law" is violating the EU Charter of Fundamental Rights, as noted in European Commission v. Hungary (C-769/22), not only underscores how the growing tension between the two entities now plays out in the digital sphere, but also raises questions about how the EU can maintain its commitment to the EU Declaration on Digital Rights and Principles amid growing ideologically infused digital sovereignty claims. This paper explores how these competing forces influence EU digital policy, with Hungary as a microcosm of broader trends.

While digital sovereignty has been studied in the context of state control and digital governance, little attention has been paid to its strategic use by anti-gender movements, particularly in the context of children's online safety. This paper addresses this gap by asking: How do anti-gender movements invoke children's online safety to counter EU norms? Has framing 'gender ideology' as cultural imperialism become a digital sovereignty strategy? What are the implications of these dynamics for EU digital policy? These questions are essential to understanding how digital sovereignty operates within broader socio-political conflicts.

To answer them, the paper combines feminist and critical legal theory. This approach explores how digital sovereignty and narratives of cultural imperialism are employed to criminalise LGBTQI+ content, amplifying digital oppression. Specifically, feminist intersectionality highlights the compounded vulnerabilities of LGBTQI+ youth, while critical legal perspectives reveal how Hungary's digital sovereignty claims obscure an exclusionary political agenda.

Methodologically, the paper uses Hungary's "anti-LGBTQ+ law" as a case study, combining socio-legal analysis of the European Commission's infringement proceedings with critical discourse analysis of public narratives by Hungarian leaders and anti-gender movements.

Hungary's actions are situated within anti-gender tactics, showing how digital sovereignty is used to resist "EU-mandated inclusivity" while reinforcing exclusionary digital policies under the pretence of children's online safety.

The findings will demonstrate how anti-gender movements use digital sovereignty to frame LGBTQ+ rights as cultural imperialism, justifying digital policies that criminalise these groups and challenge the EU's vision for rights-based digital governance. Hungary's "anti-LGBTQ+ law", framed domestically as a child protection measure, exemplifies a broader strategy that complicates efforts to create inclusive digital spaces by merging narratives of (digital) sovereignty with those resisting progressive policies.

By linking Hungary's case to EU digital governance challenges, this paper deepens understanding of digital sovereignty's complexities, particularly regarding ideological influences on digital policymaking. It underscores the need for inclusive approaches to digital governance that counter the risks posed by the nexus of digital sovereignty and anti-gender ideology, fostering equitable and rights-based digital futures for LGBTQI+ youth.

Digital Pan-Africanism: an Alternative to Digital Sovereignty?

Dennis Redeker; Adio-Adet Dinika (Universität Bremen - ZeMKI)

Abstract

Digital sovereignty has become a defining issue in global digital governance, yet prevailing frameworks remain shaped by the political and economic paradigms of the Global North. African nations continue to face digital neo-colonialism, where external actors control digital infrastructure, platforms, and data governance. This paper asks: How can Digital Pan-Africanism serve as an alternative framework to digital sovereignty in Africa, addressing digital neo-colonialism while balancing collective governance and individual rights? Grounded in Kwame Nkrumah's philosophy of Pan-African solidarity and anti-colonial resistance, Digital Pan-Africanism presents a context-specific, rights-based, and collective vision for reclaiming Africa's digital future.

While formal sovereignty has been achieved across the continent, Africa's digital landscape remains structurally dependent on foreign technology providers, platform governance models, and policy frameworks, reinforcing economic and infrastructural vulnerabilities. Existing digital sovereignty models, primarily focused on state-centric control, fail to account for Africa's unique historical and geopolitical realities, necessitating a Pan-African approach to digital governance. This paper critically engages with Nkrumah's theory of neo-colonialism, which highlights the ways former colonial powers maintain control through economic and technological dependencies. It argues that reclaiming African digital autonomy requires a unified, regional approach that prioritizes collective governance over fragmented national strategies.

Methodologically, this research employs a critical analysis of African digital governance policies, supplemented by a comparative review of existing digital sovereignty models in Europe, China, and Latin America. The paper explores how digital constitutionalism—a framework advocating rights-based digital governance—intersects with Pan-African ideals to

shape policies that safeguard against authoritarian tendencies while ensuring inclusive and democratic digital futures. Empirical data on Africa's technological dependencies, regulatory frameworks, and emerging digital collaborations will be analyzed to assess the feasibility of implementing a Pan-African digital sovereignty model.

Based on an analysis of African postcolonial thought since the 1960s, this paper makes several key arguments. First, it argues that digital sovereignty cannot be reduced to state control alone but must incorporate multistakeholder governance, including civil society, regional bodies, and the private sector. While Nkrumah's vision emphasized state-led unity, contemporary governance models must adapt to decentralized, participatory frameworks that ensure digital rights are upheld alongside sovereignty. Second, it examines the tensions within Digital Pan-Africanism, particularly the risk of reproducing centralized governance structures that exclude grassroots digital actors and sideline fundamental rights. Finally, the study proposes actionable steps for building a resilient African digital ecosystem, focusing on infrastructure development, data governance, and regional cooperation through Pan-African institutions.

By advancing Digital Pan-Africanism as a transformative alternative to Global North-centric models of digital sovereignty, this paper contributes to critical debates on digital governance, neo-colonialism, and technological autonomy in Africa. It argues that an African-centered, rights-based, and decolonial approach is essential for addressing power asymmetries in the digital age. In doing so, it offers a framework for reimagining digital sovereignty not as a tool of state control but as a means of collective empowerment, self-determination, and digital justice.

Indigenous Data Sovereignty (movement): Connecting Visions and Digital Futures.

Claudia Padovani; Enes Abanoz (University of Padua)

Abstract

Our proposal contributes to the reflection of reconceptualize digital sovereignty by focusing on non-state actors, and particularly indigenous people. Indigenous sovereignty has been discussed by different authors since the adoption of the UN Declaration on the Rights of Indigenous Peoples (Keal 2008; Moreton-Robinson 2020; Shrinkal 2021; Bauder & Muller 2023), most often in relation to the management of natural resources (Enyew 2017; Alam & Faruque 2019; Ibrahim 2023). Interestingly over the past ten years there has been an increasing mobilization of the term in relation to 'data'; while "indigenous data sovereignty" (IDS) has come to be appreciated as a strategic area of concern for indigenous populations (Kukutai & Taylor 2016; Carroll et al 2019, 2022), starting from a radical critique of Indigenous policies that have used, managed and governed Indigenous data to sustain/within a framework of disadvantage and developmental disparity (Walter et al 2021).

Adopting a decolonial perspective on digital research (Couldry & Meijas 2021; Avila Pinto 2018; Lehuede 2024) that accounts for historical legacies of domination, asymmetric power relations, and epistemic silencing, this paper focuses on an emerging transnational IDS movement, that is connecting indigenous networks across different countries (specifically

English speaking former colonies, United States, Aotearoa New Zealand, Canada and Australia, referred to as CANZUS countries). We investigate the ways in which such dynamic has fostered collective framing of IDS, by analyzing the concepts, values, claims and challenges that are articulated across CANZUS Indigenous networks.

The analysis is inspired by an analytical framework for the study of digital sovereignty that includes attributes pertaining to the actors involved, their relations, policy orientations, contextual constrains (Santaniello 2023, 2024). The framework has been integrated so as to include further attributes that emerge as relevant to IDS discourse. It has been applied to the analysis of a corpus of ten IDS documents - Charters, Declarations and policy briefs - elaborated by national IDS networks between 2016 and 2023, alongside online content available IDS networks websites. Content analysis has been carried out through a coding scheme aimed at identifying constellations of terms that characterize Indigenous use and understanding of sovereignty in relation to data and its governance; semantic network analysis has been conducted to identify connections between docs and words so as to explore both the discursive consistency of the IDS movement and specific geo-local concerns; online issue network, starting from IDS networks websites and their documents, have been traced to see how the discursive space of IDS shapes up online. Main findings from the analysis and elements for a prospective research agenda are discussed in our concluding remarks.

This study offered an opportunity to test the heuristic potential of a theoretical framework to investigate digital sovereignty, while gaining better understanding of how the concept is framed in IDS discourse, and what may be learned from IDS visions that could nurture principled and planetary care-centered visions of digital sovereignty. We trust the initial findings and emerging new research questions, may spark and contribute to a broader conversation whereby decolonial perspectives and practices could indicate (path)ways in which sovereignty – a Western concept loaded with colonial values and histories of domination – can be re-conceptualized in due consideration of individual and collective values - of equality and justice, but also relationality, respect, reciprocity and responsibility - for the digital age.

Paper Panel Session 6 - Digital Sovereignty and EU Regulation

Chair: Julia Pohle (WZB)

Governance Mechanisms for EU Digital Sovereignty: the Case of the Artificial Intelligence Act

Evangelia Psychogiopoulou (University of the Peloponnese)

Abstract

Digital sovereignty has recently emerged as a concept that is keenly used by the EU institutions with reference to EU digital policies. It is associated with the development of policies that assert (or seek to ensure) the EU's independence and autonomy in the digital world, and it is generally used to denote authority over the digital realm and leadership in the digital field in line with the Union's values and strategic interests. The term is not defined in the EU Treaties or EU secondary law. Scholars have thus sought to reach a clearer understanding of it. They have mostly focused on how the term is employed by the EU

institutions, the ways it connects to specific EU policy areas and measures, existing policy gaps in the Union's efforts to secure digital sovereignty and ways to address them. When studying digital sovereignty, the emphasis has usually been on areas such as data protection and innovation, cybersecurity, the regulation of platforms and digital services, artificial intelligence and digital infrastructure. However, less attention has been given to governance structures and their role in the digital realm. Building a genuinely sovereign EU digital environment has a lot to do with the governance mechanisms operating in the digital field - horizontally (with the establishment of regulators in specific sectors that operate in parallel) and vertically (with the establishment of regulators at Member State and EU levels). Such mechanisms can play a key role in ensuring coherence and consistency in EU digital sovereign approaches and practices.

This paper studies digital sovereignty from the perspective of its governance structure implications. It focuses on the Artificial Intelligence Act (AIA, Regulation 2024/1689). The AIA aspires to foster responsible and trustworthy AI development and use in line with the Union's values. It also establishes an intricate governance model for the implementation and enforcement of the rules enacted. Besides requiring the Member States to designate distinct national authorities for supervising the application of the rules introduced, it creates a European AI Office within the European Commission to oversee implementation, with a focus on specific issue areas such as general-level AI models and systems, AI regulatory sandboxes, joint enforcement and global AI governance; it provides for a European AI Board to ensure coordination and consistency in implementation; and it sets up an Advisory Forum for the provision of technical expertise, together with a Scientific Panel tasked with offering scientific advice. The analysis delves into the governance mechanisms employed by the AIA. It explores the nature and composition of the bodies involved, their mission, tasks, and safeguards for independence and impartiality. It also examines their interaction and coordination with a broader set of regulators, agencies and standardisation entities, and avenues for collaboration with stakeholders at national and European levels. In doing so, the paper aspires to shed light on the ability of the AIA governance framework to genuinely uphold the Union's digital sovereignty claim.

The Digital Services Act in Action: Platform Governance, Regulatory Adaptation, and the Future of EU Digital Sovereignty

Thi Ngoc Anh Nguyen (University of Padua)

Abstract

The EU Digital Services Act (DSA) represents a significant change in platform governance, transforming voluntary self-regulation into a legally binding framework of mandatory responsibilities. As part of the EU's broader strategy to assert digital sovereignty, the DSA imposes strict obligations on Very Large Online Platforms (VLOPs), reshaping how major digital intermediaries govern content, algorithmic transparency, and systemic risk mitigation. This paper examines how VLOPs are adapting to the DSA's enforcement, focussing on differences in compliance strategies between Meta, TikTok, and X (Twitter). By comparing their regulatory adaptations, the study assesses whether the DSA reinforces the sovereign control over digital platforms or whether platforms continue to assert dominance through selective compliance and regulatory arbitrage. The research seeks to understand how

Meta, TikTok, and Twitter/X differ in their responses to the DSA enforcement mechanisms. It also examines the extent to which the DSA enhances the EU's regulatory authority or whether platforms retain significant leverage in shaping compliance outcomes.

This study draws from digital constitutionalism and platform governance scholarship to analyse the evolving nature of state-platform relations. Digital constitutionalism theory argues that legal frameworks are essential to safeguard fundamental rights and democratic oversight in the digital realm, preventing platforms from exercising unchecked private governance (Celeste, 2019; Suzor, 2018). In light of this perspective, the DSA serves as a regulatory instrument that embeds transparency, accountability, and systemic risk mitigation into platform governance, reinforcing user rights and public interest protections (Heldt, 2022; De Gregorio, 2021). Meanwhile, the platform governance literature highlights the negotiated nature of compliance, where digital intermediaries strategically respond to regulatory pressures while maintaining their business interests. By combining these perspectives, the study examines whether the DSA marks a fundamental shift toward state-led digital governance or merely a recalibration of corporate power under legal scrutiny. The study employs a comparative case study approach, analysing Meta, TikTok, and Twitter/X as test cases to evaluate variation in regulatory adaptation. The study looks at (1) transparency and compliance reports published by each platform before and after the DSA; (2) policy adjustments in content moderation, algorithmic transparency, and systemic risk management; and (3) public statements and corporate discourse on regulatory adaptation.

The expected findings suggest that platform responses vary significantly, reflecting differences in corporate governance structures, geopolitical affiliations, and historical regulatory engagements. Meta, with its established compliance infrastructure under GDPR, is likely to adopt a proactive alignment strategy. TikTok, facing geopolitical scrutiny over data governance, may demonstrate strategic overcompliance in certain areas to gain regulatory legitimacy. Twitter/X, under its new ownership and deregulatory stance, may engage in minimal compliance or legal challenges, testing the EU's enforcement mechanisms. These differences highlight tensions between EU regulatory sovereignty and platform self-preservation tactics, questioning whether the DSA can enforce a truly coordinated governance model.

By investigating how different platforms navigate the shift from voluntary to mandatory responsibility, this study contributes to debates on digital sovereignty, platform power, and regulatory effectiveness. It provides a critical assessment of the EU's capacity to enforce its digital governance model, offering insights into the broader global implications of regulatory interventions in platform governance.

Norms of Digital Sovereignty and Altercasting: The European Union and Artificial Intelligence Governance

Sophie Hoogenboom (UNU-CRIS)

Abstract

Sovereignty has always been shaped by underlying norms that define the locus and nature of legitimate authority. Floridi (2020) has referred to ''fights'' for digital sovereignty, in which state and non-state actors are fighting for 'control over the digital'. Roberts (2024) has rightly

pointed to the lack of focus on legitimacy in this understanding, as sovereignty ultimately deals with the notion of 'legitimate authority' instead of control. Both point to a social process in which norms of digital sovereignty are being formed.

This paper wants to bring attention to insights about the nexus between sovereignty and roles found in Symbolic Interactionist Role Theory literature. It argues that these fights for digital sovereignty could be approached as being a social process in which actors are trying to claim a desired role for their Selves and (actively) engage with norms of (digital)- sovereignty. This, as the existing literature on 'analogue' sovereignty, points to the importance of norms of sovereignty as it impacts the availability, legitimacy, and nature of roles which state and non-state actors can play. Given their significance, norms of sovereignty are subject to active contestation, particularly when existing norms are challenged or when actors enter a new space.

Symbolic Interactionist Role Theory highlights three key processes in role dynamics: role-taking, role-making, and altercasting. However, the concept of altercasting, where actors seek to shape others' roles to align with their own objectives, remains underexplored. A notable exception is Opperman (2024), who offers a framework for analysing ego altercasting. This paper builds on this work to further explore the concept of altercasting in relation to digital sovereignty.

The paper is structured into three main parts. First, it explores the theoretical connections between altercasting and the development of digital sovereignty norms. Second, it examines suitable methodologies for capturing the altercasting process. Third, it applies Opperman's framework to analyze the European Union's role in artificial intelligence governance as a case study. By doing so, this paper hopes to contribute to ongoing efforts to integrate insights from Symbolic Interactionist Role Theory into the study of digital sovereignty, refine our understanding of altercasting processes and methodologies, and enhance our comprehension of AI governance.

DAY 3 - Wednesday, 28 May

Paper Panel Session 7 - Data Governance and Data Sovereignty

Chair: Marianne Franklin (University of Groningen)

Practices of Ordering and Bordering in Sovereign Cloud Projects

Andreas Baur (Universities of Amsterdam and Tübingen)

Abstract

Cloud computing changed the idea of place and placelessness of IT infrastructures. Although cloud computing is made of brick-and-mortar data centres, the idea, the metaphor but also its technicalities promise and entail placelessness.

Increasing political attempts to control and reign in on 'the internet' and its underlying IT infrastructures did also affect cloud computing. Snowden revelations, surveillance capitalism and single regulations such as the US CLOUD Act informed the debate. Europe's focus on challenging Big Tech, protecting privacy and supporting European industry lead became part of strengthening European Digital Sovereignty – also in the cloud.
In this paper, I analyse concrete practices of introducing digital sovereignty in cloud infrastructures. I argue that ideas of data and digital sovereignty in the cloud can and should be understood as practices of bordering the cloud.
The relationship between cloud and bordering practices is defined by tension. Territorialisation and data localisation are core aspects of digital sovereignty strategies in general. Introduced to the cloud, they are contradicting its core characteristics.
While bordering practices have long been part of debates in political science and especially International Relations, bordering as a concept has not been developed in relation to cloud technologies or questions of cloud sovereignty or digital sovereignty.
In this paper, I argue that bordering is used on several levels to achieve different goals: to enforce (1) compliance (data is stored and processed according to the local regulations), to (2) guarantee the privacy of users, and to (3) protect against industrial and government espionage, leaks and attacks for a fair competition.
This paper analyses several sovereign cloud projects and the concept of (federated) data spaces, extracting strategies for digital sovereignty that can be understood as bordering practices. Inspired by STS, the analysis is based on extensive fieldwork including expert interviews, background talks, observations of conferences and business events, as well as documents on the architecture and promotion of sovereign cloud solutions. To support the argument, I distinguish practices and technologies of introducing digital sovereignty into cloud infrastructures and the organisation of providers and ecosystems. The analysis shows, for instance, that these borders are hardly ever absolute and do not entail a complete split of the technology. Yet, "checkpoints" are established and technologies set-up to separate "good" from "bad".

Data Sovereignty in India: Balancing Restriction and Accumulation of Data through Digital Public Infrastructure and Artificial Intelligence

Jyoti Panday (Georgia Institute of Technology)

Abstract

The exponential growth in data generation and the heightened recognition of its intrinsic value have positioned data as a strategic resource, necessitating control by nations, organizations, and individuals. However, the globalized nature of the internet and the concentration of data within a limited number of multinational corporations have created significant challenges for both states and individuals in asserting control over their data. In response, the concept of data sovereignty—the principle that data should be governed by the laws and regulatory frameworks of the nation in which it is collected or stored—has gained traction across various regions and contexts.

Academic scholarship highlights the multifaceted nature of data sovereignty, with its interpretation varying across actors and contexts (Hummel et al., 2021). While territoriality strengthens state control over citizens' data (Chander & Sun, 2023), it can also hinder

governments' ability to address cybersecurity and privacy concerns effectively (Panday & Malcolm, 2018). These tensions reveal the complexities of operationalizing data sovereignty in a globally interconnected digital ecosystem.

Given its contentious nature, it is essential to critically examine how data sovereignty manifests in different contexts. In India, policymakers have framed technological sovereignty as a pathway to drive a new industrial revolution and establish the country as a global technology leader. Initiatives like Make in India and Digital India exemplify India's state-centric approach to achieving self-reliance (Atmanirbharta) in strategic industries and critical technologies. Central to this vision is data sovereignty, which aims to extend the state's authority over the collection, storage, and use of personal and non-personal data.

This paper argues that India's approach to data sovereignty combines two interconnected strategies: (1) restrictive control, involving regulations to limit data flows, and (2) accumulative strategies, aimed at fostering data creation, sharing, and utilization. To illustrate this duality, the analysis focuses on two key initiatives enabling pervasive datafication: digital public infrastructure (DPI) and artificial intelligence (AI). DPI represents state-driven efforts to build interoperable digital systems for governance and service delivery, while AI reflects India's ambition to leverage data for innovation and economic growth.

Using a historical lens, this paper examines the legal, regulatory, technical, and institutional frameworks surrounding DPI and AI, assessing their effectiveness in expanding data control and their implications for power dynamics among stakeholders. The analysis reveals that governments, tech companies, and civil society organizations have varying capacities, priorities, and interests, leading to disparities in their commitment to and influence over data sovereignty initiatives. These findings underscore the contested and uneven nature of data sovereignty in practice.

Converging Frictions: the Unexpected Alignment of Secure Messaging and Digital Sovereignty in Switzerland

Samuele Fratini (University of Padua / Università della Svizzera Italiana)

Abstract

This study examines how digital sovereignty can be non-linearly achieved as a hybrid product of public contestations, non-hegemonic discourses, and alternative technical arrangements. Adopting a Science & Technology Studies theoretical framework, the analysis challenges the traditional institutionalist approach that understands digital sovereignty as a policy and legal achievement. The suitable case study is Threema, a Swiss secure messaging application and the largest European-headquartered messaging app by user base. The case of Threema is interesting because it was born as an alternative messaging app but has evolved into the official messaging application of nearly every Swiss institution and big corporation (Fratini, 2024). From a digital sovereignty perspective, it allowed the Swiss institutions to reduce foreign dependencies. Among many others, Threema is the exclusive means of internal and external communication for the Swiss Federal Administration, some Cantonal Administrations, the Border Police, and the Swiss Army.

The research analyzes 40 official (technical and non-technical) documents published by Threema and German and Swiss institutions and newspapers between October 2016 and June 2024 and 10 semi-structured interviews conducted with Swiss institutional actors between February and May 2024. The data were analyzed using Grounded Theory (Charmaz, 2012).
We show how Threema's privacy-oriented design and discourses result in hybrid forms of friction, a concept borrowed by Lowenhaupt Tsing, indicating "the awkward, unequal, unstable, and creative qualities of interconnection across difference" (2004: 4). Emerging frictions are ordered into three main categories:

1. Privacy as ensemble of sociotechnical forces opposing the free flow of information (Floridi, 2015) advocated by US tech firms;
2. Non-interoperability as a way to safeguard corporate standards on metadata protection and a matter of clash with the EU institutions.
3. Territorialism as the logic that legitimates Threema as a secure messaging channel. Territorialism emerges both infrastructurally (in-home data centers) and discursively (remediation of "Swissness" as a set of values) Messaging technologies are grafted onto jurisdictional (infra)structures, and are in turn re-empowered through themselves.

Threema's construction of privacy underscores the unexpected convergence between hybrid anti-surveillance frictions and strategic national goals, i.e., those of data sovereignty in particular (Fratini et al., 2024). As these privacy-related frictions stabilize, they translate into norms that support a localized, sovereign digital agenda, excluding foreign operators in favor of domestic solutions (Fratini & Musiani, 2024). The analysis reveals how Threema's story can only be understood through a processual and infrastructural model of digital sovereignty (Musiani, 2022), where Swiss authorities have managed to achieve digital sovereignty meant as the reproduction of state material and normative dispositions (Laurent, 2024):
1. Material dispositions: The reduction of dependencies on foreign messaging service providers without resorting to autarchic policies.
2. Normative dispositions: The advancement of a Swiss model of privacy reproducing the state's historically opaque regulatory system (Mazzoni et al., 2024) and financial tradition.

Finally, the work highlights the efficacy of the STS scholarship in analyzing the structuration of sociotechnical assemblages (Slack & Wise, 2015) – such as secure messaging – in a global-local tradeoff.

Towards Substantive Digital Sovereignty in E-Government: Tensions Between Power, Responsibility, and Control as Evident from an Empirical Study on the Perspectives of Citizens, Experts, and Administrative Staff in Germany

Robin Preiß; Christian Herzog (University of Lübeck)

Abstract

The notion of digital sovereignty, which continually buoys as a very current topic, bears various conceptualizations (e.g., Couture & Toupin, 2019; Pohle & Thiel, 2020). Despite its multi-faceted expressions, we argue that the socio-technical complexities in working towards achieving digital sovereignty have not yet been sufficiently considered — a statement we

support by evaluating an empirical study based on citizen interviews and group discussions. We identified tensions arising from a diffusion of responsibilities towards citizens and from a lack of citizens' confident use of digital technologies, the implicit responsibilities incorporated into software applications, and public administration employees' limited power to act in digitalization approaches.

The digitalization of public administration appears conditioned by an interweaving of national and individual sovereignty. For instance, it is challenging for users to exercise autonomy in the digital realm if they lack requisite application skills and are at the same time, due to structural conditions, overburdened by privacy management tasks (Solove, 2020). Citizens face excessive responsibilities to safeguard personal data, understand and use digital tools effectively, and navigate complex interactions in the digital sphere. While these expectations aim to empower citizens, they often result in an overwhelming burden that some are ill-equipped to handle (Ciesielska et al., 2022). We, therefore, argue that substantive digital sovereignty requires more than individual skills, namely structural support and empowerment. The following question is thus analyzed: Which concepts are crucial to promote substantive individual digital sovereignty, and how are they shaped?

This discussion is based on an interview study with ten citizens and two group discussions focusing on fostering digital sovereignty, one with interdisciplinary academics, the other with digitalization experts from public administration. We found a perceived "diffusion of responsibility" (Darley & Latane, 1968) embedded in some public administration digitalization approaches. This responsibility diffusion not only obscures institutional accountability but also amplifies power imbalances between individuals, society, and entities such as the state and Big Tech companies. While Big Tech influences citizens' expectations and thus gains power in the Foucauldian sense (Foucault, 1976), political regulations attempt to recapture power, sometimes at citizens' expense.

Digitalization efforts appear to result in increased delegation of significant responsibilities to citizens systematically. This may refer to managing data privacy and acting self-determined in the digital sphere, despite bureaucratic obstacles. Considering an existing lack of "digital literacy" in many citizens, we expect structural inequalities (Young, 2011) to be exacerbated if current digitalization practices continue. The necessity for these competencies is expected to increase in AI-supported systems as functionality increases in complexity. Moreover, the absence of personalized support and neglect of individual circumstances in digital services lead to frustration and disenfranchisement. These dynamics undermine public trust in e-government systems and the state's ability to act as a protective intermediary in the digital age.

Key principles include accessible and understandable e-government communication, reduced bureaucratic barriers to allow for citizen-centered decision-making, and the integration of analog and digital support systems as needed. Therefore, digital public administration must provide accountability and assume responsibility for maintaining its trustworthiness to foster substantive digital sovereignty.

Paper Panel Session 8 - European Digital Sovereignty: Digital Constitutionalism, Digital Autonomy and Normative Power

Chair: Daniela Piana (University of Bologna)

The European Third Way: the EU's Strategic Narrative of a Value-Based Digital Order and its Global Impact

Julia Pohle; Leo Thüer; Milan Schröder; Christian Rauh (WZB)

Abstract

In recent years, the European Commission has integrated its 'digital sovereignty' strategies into a broader narrative aimed at steering global digital transformation towards a human-centred, value-driven model, distinct from technology and commercial imperatives. This approach reflects a shift from a primarily inward-looking focus to an outward-looking global policy agenda, positioning the EU as a critical actor offering an alternative to the digital models proposed by the US and China, thus articulating a European 'Third Way' (Cancela & Jiménez, 2022; Adler-Nissen & Eggeling, 2023).

A key mechanism for increasing its global influence in digital policy is the EU Global Gateway initiative, launched in 2021. This initiative aims to promote sustainable connectivity worldwide through the development of digital, transport and energy infrastructure, while strengthening international trade and investment partnerships (Daniels et al., 2022; Abels & Bieling, 2023). By promoting digital connectivity projects, the EU seeks to enhance its geopolitical status and solidify its role in the global digital economy. Unlike China's Belt and Road Initiative, the EU's value-based connectivity strategy calls for cooperation based on principles of rationality and reciprocity. However, critics argue that it may create uneven partnerships that limit partners' influence on technology norms, potentially undermining the EU's normative goals (Karjalainen, 2023).

This paper examines the transition from an inward-looking to an outward-looking EU digital sovereignty agenda by analysing the narratives used by the European Commission and the European External Action Service (EEAS) regarding connectivity partnerships. This analysis is part of a broader research project exploring the impact of geopolitical tensions, particularly between China and the US, on the EU Commission's digital policy discourse. Using computational NLP methods together with qualitative discourse analysis, the project examines an original corpus of public communications from the Commission and the EEAS spanning the period from 1985 to 2024. The analysis adopts the strategic narrative framework from Miskimmon, O'Loughlin, and Roselle (2013) to categorize the discursive frames regarding the EU's influence on global digital connectivity: system narratives (how should a global digital order look like), identity narratives (what is the role of the EU and others in shaping this order) and issue narratives (how is the digital transformation actually understood).

Initial findings suggest that the Commission and the EEAS are using the strategic narrative of a "global digital order based on European values" to increase the EU's external influence (spatial aspect), while at the same time assuming that the historical and ongoing struggles associated with (post-)colonialism have given way to more equal, cooperative relationships

(temporal aspect). So-called 'partner countries', which are presumed to be equal, are integrated into the EU's digital policy approach under the umbrella of 'European values'. The current basis for this very specific narrative of progress is a particular, idealistic vision of the 'digital world', and it serves to justify and strengthen the EU's geopolitical influence.

While the global impact of EU digital policy has been discussed under the concept of the 'Brussels effect', this paper contributes to the existing literature by focusing on the strategic framing and potential ramifications of the European Third Way narrative, which remain relatively underexplored. By integrating concepts from the literature on digital sovereignty, global connectivity, and digital colonialism, it also offers insights into how the EU's digital sovereignty initiatives reflect a shifting global digital order amid rising geopolitical pressures.

The Geopolitics of Semiconductors – How digital Sovereignty Helps Legitimize Geoeconomic Measures

Linda Monsees (Institute of International Relations Prague)

Abstract

This paper engages with the theme of digital sovereignty by focusing on one technology that is a focal point for debates on digital sovereignty; namely semiconductors. Semiconductors or computer chips are at the core of the production of all digital technology but also the base for producing ever more powerful machine learning capacities. Their intricate production process and globalized supply chain make it thus a core battlefield for geoeconomic battles. That is why semiconductors are among the most important technologies for the digital society and a core technology of the European Union (EU)'s digital sovereignty agenda.

This paper investigates the question of how the governance of semiconductors in the EU operates. Based on a qualitative analysis of EU-documents and expert statements this paper provides a unique analysis of a pivotal digital technology. This study draws on critical infrastructure literature in order to allow for a better understanding of how narratives and values are inscribed into technology.

The main argument of this article is that the governance of semiconductors is shaped by an inherent tension. On the one hand, this governance is embedded in the agenda of digital sovereignty, suggesting some form of autarky is possible. Not only the EU but also China and the US foster an agenda where the (seemingly) sovereign production of semiconductors is feasible and a declared policy-goal. On the other hand, the production of semiconductors is necessarily globally distributed. A variety of different chemicals, devices and production steps are necessary to produce semiconductors. Its supply chain is highly specialized and spans the whole globe. This apparent tension, however, allows the EU to align a variety of different policies. Ultimately, the paper argues that in the case of semiconductors, digital sovereignty works as a tool for legitimising trade, economic and research policies. The policies all work to legitimize a geoeconomic approach toward tech development. The need for a strong semiconductor industry in the EU and the globalised nature of threats against the supply chain are acknowledged simultaneously. In turn, subsidizing global corporations has turned out to be the natural response. Politically, it becomes difficult to contest these subsidies, as well as the underlying assumption concerning future innovation.

As such the paper contributes to the important critical discussion of the role of the digital sovereignty agenda for legitimizing EU policies and how it is embedded in global geopolitics.

EU Digital Sovereigntism: the Risks of Strategic Autonomy

Edoardo Celeste; Alba Perez Victorio; Victor Henriquez Diaz (Dublin City University)

Abstract

In the digital sector, the EU is heavily dependent on third countries (Mayer and Lu 2022). Recent EU policy strategies no longer merely aim to boost digitalisation, but are guided by a new, at times vague, principle: digital sovereignty (Floridi 2020; Pohle and Thiel 2020; Celeste 2020). The Union is seeking to achieve a status of strategic autonomy across a plurality of areas, including in the digital field, which is also considered to be key to fostering the green transition (Celeste and Perez Victorio 2025). This paper questions the alignment of the effects of EU digital sovereignty strategies with their policy objectives as well as, more broadly, with the Union's constitutional aims and values. The first part of the paper categorises EU digital sovereignty regulatory approaches into 'centripetal' and 'centrifugal' strategies, assessing which types of internal (within the EU) and external (outside of the EU) effects they produce. The second part of the paper examines to what extent these effects misalign with EU strategic objectives, constitutional aims and values. The paper identifies three types of discrepancies and interprets them as potential 'sovereigntist' trends at EU level. The analysis carried out in this paper adopts a doctrinal, hermeneutic and empirical legal approach and builds on a systematic and interdisciplinary literature review of the concept of digital sovereignty and sovereignism.

According to the literature, the regulatory instruments through which EU digital sovereignty strategies are pursued are manifold, ranging from the GDPR to the AI Act or the DSA (Sheikh 2022; Codganone and Weigl 2023; Broeders, Cristiano and Kaminska 2023). In an attempt to systematise and categorise EU regulatory initiatives pursuing digital sovereignty objectives, the paper identifies two main approaches: centripetal –whereby digital assets and services are physically reshored to the EU – and centrifugal – which seeks to extend EU standards outside EU borders (Celeste 2020; 2023).

These strategies generate a series of effects that go beyond their policy objectives and have an impact also on non-EU countries. The paper analyses to what extent these effects are in line with EU constitutional aims and values. EU strategies de facto generate imperialist, protectionist and isolationist effects, respectively from a regulatory, economic and environmental perspective, which are at odds with the multilateral, open and green stance of the EU. Firstly, the EU risks imposing its digital standards to jurisdictions with a different legal culture; secondly, it risks erecting trade barriers, even with potentially trusted partners; thirdly, it exacerbates potential paradoxical conflicts between the benefits of digitalisation and the green transition, with little account of the impact on non-EU countries.

We identify a collision between EU digital sovereignty strategies and digital constitutionalism's aspirations. Such a model of strategic autonomy focuses on the EU at the expense of other countries and is characterised as being EU-centric (Kuner 2019) and 'too

self-interested' (Innerarity 2023, 290). We therefore argue that these strategies are at times impregnated with Europeanism (Ackerman et al. 2022) and risks embodying forms of sovereigntism (Basile and Mazzoleni 2020).

Digital Sovereignty vs. Digital Constitutionalism: between the EU and its Member States

Chiara Spiniello (University of Salerno)

Abstract

The European Union has explicitly acknowledged its pursuit of a «third way» in Internet governance, presenting an alternative to both the United States and Russian-Chinese models. The United States has established a highly protective legal framework for digital enterprises, underpinned by the First Amendment's safeguards on free speech and Section 230 of the Communications Decency Act, enacted by Congress in 1996. This framework grants extensive self-regulatory powers to private entities, thereby significantly restricting the regulatory authority of State Institutions. Conversely, China and Russia regard the Internet, the web, and digital platforms as fundamental national infrastructures, placing the State at the core of digital governance and directly shaping the regulatory framework of the online environment.

In contrast to these two paradigms, the European Union's digital strategy aspires to reconcile digital constitutionalism with digital sovereignty. This approach is predicated on the principle that the development of Europe's digital infrastructure must remain aligned with the Union's foundational values (most notably, solidarity and inclusion, freedom of choice, democratic participation, cybersecurity and sustainability). Such a strategy has been articulated through the adoption of various soft law and, more notably, hard law instruments (including, most recently, the Artificial Intelligence Act - AIA, the Cybersecurity Act, the Digital Services Package - DSP), with active involvement from several EU Member States in their development and promotion.

Given this context, it is crucial to explore whether a similar approach has been reflected in the policies and positions of national governments. Consequently, this contribution aims to examine the central elements of the discourse on, and policy of, digital sovereignty and digital constitutionalism in five specific EU Member States: France, Germany, Italy, Spain and Poland. These countries have been selected due to their distinctive roles in the ongoing Internet governance debate: France and Germany are both leaders in advancing the European digital agenda and have developed a strategic discourse at the national level; in Italy, particularly in recent years, the President of the Republic has emerged as a key figure, seemingly advancing a personal «Digital Agenda» that contrasts with the Government's official stance; Spain has already integrated significant constitutional recognition of digital rights; while Poland, having assumed the presidency of the EU Council since January, has placed digital sovereignty at the core of its agenda and has developed its own national strategy.

The paper aims to conduct a qualitative analysis, employing a comparative method, of legislative acts and key political speeches on the subject. By examining the principal literature on sovereignty and digital constitutionalism, the study formalizes a set of indicators (defined

in terms of key concepts such as digital rights or strategic autonomy) whose recurrence in the analyzed documents allows for their classification within the broader frameworks of constitutionalism and/or digital sovereignty. The goal of the analysis is to address the following research questions: What are the connections, if any, between the concepts of digital sovereignty and digital constitutionalism in the five countries under examination? Do these national approaches align with the European trajectory, or do they diverge from it? The expected outcome is the emergence of conflicting national interests, which may jeopardize the delicate balance the EU has sought to establish by integrating the concepts of constitutionalism and digital sovereignty.

Paper Panel Session 9 - Infrastructural Sovereignty

Chair: Jamal Shahin *(BSoG-VUB/UvA/UNU-CRIS)*

Digital Sovereignty for Industrial Competitiveness – the Case of Manufacturing-X in Germany

Max Münßinger (Friedrich-Alexander-University Erlangen-Nuremberg); Cartus Bo-Xiang You (National Taiwan University; Friedrich-Alexander-University Erlangen-Nuremberg)

Abstract

The past few years witnessed growing "digital sovereignty" initiatives to reclaim governments' control over digital infrastructure, data flows and technological capabilities, especially centering a series of legislation and policy efforts in the European Union. This determination, as many authors argue, is largely driven by both geopolitical and geoeconomics consideration. By establishing regulations and common technical standards, EU's data strategy intended to avoid lock-in effects and dependencies on non-European (i.e. American and Chinese) platforms and ensure greater economic authority. This expansion could be understood as a paradigmatic shift in the relationship between the state and capitalism, emphasizing the intersection of regulatory power and technological dominance. While existing scholarships in political economy have long been concerned about state intervention in economic activities, they did not capture the alternative rationales in the development of digital economy—namely the prioritization of data accumulation instead of money. The centralization of data not only provides essential fuels for technological innovation, but more importantly, consolidates and enhances the structural dominance of leading firms. Moreover, it extends the controlling power of the regulatory entities through economic relationships.

This paper particularly draws attention to the intertwining political and economic interests in Germany's digital sovereignty policies. We examine this interplay with the "Manufacturing-X" (MX) infrastructure and standardization project initiated by Germany's "Plattform Industrie 4.0". The project was launched in 2022 with the explicit aim of ensuring greater digital sovereignty in the global production networks of the manufacturing industry by reducing lock-in effects. It is intended to be a nucleus for both the industrial data space "Datenraum 4.0" in Germany and the "Common European Manufacturing Data Space(s)" and aims to set global standards for industrial data processing. Due to the close intertwining of political and economic interests in the project, it is particularly suitable for investigating political-economic ambiguities and contradictions in the emergence of digital sovereignty in Germany and the EU.

To this end, we draw on political-economic approaches that focus on the close interweaving of economic constraints and demands for sovereignty. Additionally, our analysis is further supplemented with infrastructural approaches that understand digital infrastructures as conflictual instruments to restructure, depoliticize and legitimize political-economic relations. Against the backdrop of this analytical lens, the paper elaborates (1) how the project attempts to break up digital lock-ins, (2) how this attempt is based on extra-territorial power being implemented through supply chains and built on German firms' dominant industrial position, and what role (3) supposedly neutral technical standards and (4) institutional incentives for information exchange and cooperation play in this. On this basis, the article shows that MX as a project to establish German and European digital sovereignty in industrial production networks can be understood as a precarious infrastructural and "apolitical" approach to create a lock-in effect of a German-European capitalist ecosystem. Finally, the article discusses the prospects for success and the frictions of this approach.

The Liverpool Civic Data Cooperative: A Participatory Approach to Building Regional Digital Sovereignty and Data Stewardship

Gary Leeming; Emily Rempel; Iain Buchan (University of Liverpool)

Abstract

The Liverpool Civic Data Cooperative (CDC) was funded in 2020 by the Liverpool City Region Combined Authority in England to help to address the challenges of civic data stewardship and digital innovation. This paper explores how the CDC used principled participatory design and civic engagement, legal frameworks of data protection, and technical capabilities to create a novel approach to supporting regional digital sovereignty. This includes new collaborative infrastructure, connecting organisations across healthcare, local government and other public services that are otherwise disconnected and lacking the clear, common values that are vital to digital sovereignty and capability. The CDC approach prioritises collaboration, engagement and co-design with data rights holders, including the public, to improve data governance through an action-oriented model addressing community needs and aspirations.

The CDC began by building on the theoretical foundations from Elinor Ostrom's work on collective governance, alongside modern software and human-centred design thinking to develop a set of values that could be sustained through practice. Key considerations include local data needs and capabilities, the social license to act, and the complex interplay of legal, commercial and civic obligations. The CDC convenes diverse public organisations, businesses and residents to foster values of collaboration, innovation and mutual trust through cooperative principles.

These core values were developed through several participatory and technical projects, including data-reliant responses to the Covid-19 pandemic, outreach to explore uses of data to improve community wellbeing, integration of care across NHS, social care and third sector agencies through shared data and digital workflows, and the development of a UK-wide community of practice in civic approaches to data and digital sovereignty.

Incorporating public input with organisational collaboration has created a balance of privacy expectations, innovation and ethics while addressing the inherent challenges of incomplete consent and potential biases. Working with partners such as the Ada Lovelace Institute, following their work on creating a spectrum of participation for data stewardship, the CDC has actively included public voices through use of citizen juries, public debates, and hackathons in projects such as Round 'Ere and Greater Data (see https://civicdatacooperative.com/). In March 2025, this approach will be tested through a large-scale Residents Assembly to co-design the CDC governance framework under a Regional Charter for Data and AI. This assembly will produce a declaration of expectations of what digital sovereignty means for the Liverpool City Region, and how it should be implemented in public services.

The paper concludes by considering how the experiences of the CDC can be more widely applied through agile, action-oriented, and theoretically well-founded ways to mobilise data and digital innovation to meet public needs, while being practical and consistent on the specific values that are important to organisations and communities within the region. This civic data/digital pragmatism supports relational working across complex civic systems of public services and service users, creating a patchwork of practice evolved to meet specific expectations of data values, and to support equitable and inclusive digital ecosystems.

Unlocking Digital Sovereignty: Open Source Software in Connectivity Architecture. A Perspective on Chinese Companies in O-RAN

Riccardo Nanni (CNRS)

Abstract

5G infrastructures are being deployed at the time of writing. This infrastructure has been subjected to a stark political debate that underlies protectionist measures in the US and elsewhere, especially when it comes to accepting network manufacturers headquartered in hostile countries (namely China as far as the US is concerned) (Ten Oever, 2023).
An overlooked site in which digital sovereignty plays out in mobile connectivity infrastructure is the elaboration of the open source software-based Open Radio Access Network (O-RAN) at the O-RAN Alliance (O-RAN Alliance, n.d.; Polese et al., 2023).
This article explores China's state-owned Internet Service Providers' participation in the making of O-RAN as an instrument to foster digital sovereignty. This exemplifies the use of free and open source software (FOSS) to break vendor lock-in and foster digital sovereignty.
1) Context
Radio Access Network (RAN) is the mobile connectivity infrastructure component allowing devices to connect to the core network via radio waves. Developing solutions that become part of the global RAN standard is strategic for companies as the way RAN is shaped directly affects the way devices are made, with huge financial implications (Garcia-Saavedra & Costa-Perez, 2021; Nanni, 2021). Furthermore, proprietary interfaces in the infrastructure ensure that countries and actors that rely on a company for infrastructure implementation undergo a vendor lock-in when it comes to maintenance and future development (Baron et al., 2023).
O-RAN is based on open source software and hardware. It promises to make RAN fully open and interoperable, thus breaking infrastructure vendor lock-in (O-RAN Alliance, n.d.).

Among many actors in the O-RAN Alliance, there are China's main Internet service providers: China Telecom, China Unicom, China Mobile.
Observing Chinese actors in this field is key to understanding the dynamics of digital sovereignty and the use of open source technologies to attain it. The Chinese industry - particularly Huawei - has achieved a leading position in Internet and mobile connectivity standardisation on par with European giants such as Ericsson (Pohlmann et al., 2020).
2) Approach and methods
This is an early-stage version of an article that fits into a broader research agenda on China's digital sovereignty vis-a-vis connectivity infrastructures.
This article leverages qualitative methods such as the systematic analysis of O-RAN Alliance documents and interviews with technologists involved first-hand in O-RAN development to reconstruct the engagement and objectives of Chinese state-owned ISPs in the making of O-RAN.
This work is grounded in previous research on Chinese engagement in 5G standardisation and patenting (Baron et al., 2023; Becker et al., 2024; Nanni, 2021; Pohlmann et al., 2020), as well as work on FOSS as instrument for digital sovereignty in that its adoption helps actors disentangling themselves from vendor lock-in and overreliance on a single technological provider (Biström et al., 2024).

3) Results and empirical relevance
This article contributes to an important but understudied niche of the digital sovereignty debate, namely the use and development of FOSS to break the dominance of established business actors.
Empirically, it casts new light on the O-RAN development process, an under-observed aspect of mobile connectivity infrastructure standardisation.

Infrastructural Power: How Governments Are Managing Internet Points of Control

Juan Ortiz-Freuler (Annenberg USC)

Abstract

This article engages with the debate on digital sovereignty by focusing on the strategic reconfiguration of internet infrastructure by nation states (Musiani, 2022). To this end, I introduce a typology of six distinct strategies through which governments are asserting or disrupting control over critical internet infrastructure nodes, or "points of control" (DeNardis, 2012). These strategies show different responses to the geopolitical and economic implications of the internet's centralization under the control of corporate actors that are often perceived as unresponsive.

The six strategies outlined in this article are exemplified by concrete case studies: the European Union and Brazil's joint investment in the EllaLink undersea cable aimed at bypassing the US-controlled landing points; India's Open Network for Digital Commerce, which neutralizes the control of a corporate few players over digital marketplaces; the European Union's Digital Markets Act, compelling Apple to allow sideloading of apps; the US transition of ICANN to a nonprofit structure with a diverse board; the NSA's covert access to AT&T's internet infrastructure; and the global trend of data localization policies, which aim to make global corporations more responsive to local authorities by requiring them to re-root

parts of their infrastructure within the local jurisdiction. These examples, accompanied by visual representations of how each strategy implies a re-design of power relations, with the first three focused on the network topography, while the latter three focus more on the ways in which the existing network architecture is governed. Thus, this paper shows how digital sovereignty is enacted not just through policy but through infrastructure itself.

The discussion section of the article explores how governance is moving from consensus-driven global fora to more localized efforts at infrastructural control. Meanwhile, the way in which these infrastructures are interconnected shapes and afford specific interactions, influencing how power is distributed and exercised across the digital landscape. The internet, as a dynamic network of networks, remains in constant renegotiation, with control points shifting both vertically and horizontally. For example, Brazil's efforts to circumvent undersea cables or the US's devolution of power over ICANN happened while the explosive growth of social media allowed the US government to retain control over information flows by controlling another layer of the internet stack, underscoring the need for dynamic, ongoing analysis. This reconfiguration of power dynamics also challenges the discourse of "internet fragmentation." Rather than framing the issue as a binary, the "re-networking of information infrastructures", offers a more neutral account of how points of control move mirroring shifting power relations. Larger powers, such as the US, EU, and China, often focus their resources on extraterritorial effects, while smaller states are typically relegated to managing local infrastructure defensively, and in the face of coercive interdependence.

The article underlines the complex ways in which internet sovereignty is being sought. It calls for a reconceptualization of internet governance that moves beyond the fragmentation narrative and towards a more dynamic and realist understanding of how control over infrastructure is shaping sovereignty and geopolitics.

Paper Panel Session 10 - Digital Sovereignty in Wartime

Chair: Mauro Santaniello (University of Salerno)

Lessons from Ukraine: Examining the Policy Implications of the Multi-stakeholder Environment Found in Digital Open Source Investigations During Violent Conflicts

Magdalene Karalis (Chatham House - Russia Eurasia Program)

Abstract

Russia's full scale invasion of Ukraine in 2022 saw Open Source Investigations (OSI) and their resulting Intelligence (OSINT) surge in popularity and shape the way social media was used in times of conflict, removing traditional borders to frontline support as all facets of cyber and kinetic warfare continue to become increasingly interconnected. As with many subfields of cyber conflict and internet governance, OSI in Ukraine also marked changing norms in the role of the private sector during global conflict and saw the convergence of diverse actors all using these resources to conduct digital investigations for their own purposes. From government officials and military personnel to civil society, legal experts, tech experts and online sleuths, the stakeholders that now produce, harness and leverage open source data for digital investigations are far more widespread than the old norms of OSI found within traditional intelligence units in governments and militaries. In particular, tech

companies involved in the development of social media and other crucial tools have become key, inextricable players. These companies represent diverse networks, goals and capabilities that can evolve and change alongside any unfolding conflict. As such, they are simultaneously becoming increasingly crucial and harder to regulate.

Using a mixture of fieldwork, relevant literature, semi-structured interviews, open-source investigations and social media analysis, this paper outlines the ways in which the rise of a multi stakeholder environment in digital spaces has shaped the way information and crucial intelligence is mobilized and weaponized in times of violent conflict. It delves into the new precedents set and the new policy needed for the increasing exposure everyday civilians have to the realities of war, the rapid evolution and role of emerging technology in this space and the shift in power dynamics between invested governments and private tech companies that now leverage, influence and shape the online domain of warfare.

Digital and Technological Sovereignty of the Emerging Powers with some Industrial Capabilities. Russia's Cooperation with the Global South since the Beginning of its War Against Ukraine.

Ewa Dabrowska (Freie Universität Berlin)

Abstract

With the extended West and China being in possession of crucial technologies in the digital age, countries dependent on them look for ways to advance technologically in these challenging circumstances. Some of them perceive themselves in this context as "technologically (or digitally) non-aligned", implying a political non-alignment as well. Others, such as Russia, do not have official access to Western technologies due to sanctions. Since the attack on Ukraine and ensuing sanctions, therefore, Russia has been strengthening existing or looking for new alliances in the Global South. The Russian government and business associations regard India as one of the crucial countries for technological cooperation. They sent a digital diplomatic attaché to this country, strengthened other diplomatic efforts to market Russian technologies and products, with some evidence of success, and bought Indian software to replace Western products. At the same time, Russia continues to purchase Western technologies through so-called parallel imports – imports of sanctioned goods through third countries, such as Kazakhstan, China, Turkey, etc. and relies on open-source technologies. These new alliances and the reliance on Western and open-source technologies are aspects of Russia's industrial and technological policy conducted under the label of "technological sovereignty". This paper examines the role of new alliances with the Global South, particularly India, for this policy. It addresses three issues: 1. What strategies does Russia use to become an attractive partner for technological cooperation, and how do they relate to the strategy of establishing its own value chains? 2. How are these strategies received by the countries addressed? 3. What are the consequences of these new alliances for the constellation of (technological) power in the international political order?

We study official documents, newspapers, think tank publications and business association reports from Russia and India, as well as expert interviews, to examine these questions. The paper relates to technological and digital sovereignty debates and innovation diplomacy studies. It argues that technological sovereignty is necessarily relational despite its association with autarky. Even in the case of Russia, it would be wrong to equate

"technological sovereignty" with isolationism, even if it is imposed by the West through technological and financial blockades.

Digital Sovereignty Wartime: 'Infrastructure Power' and post-2022 Ukraine Dealing with a Twofold Digital Dependency

Julien Nocetti (University Paris 8)

Abstract

Over the past decade and a half, digital sovereignty has gradually become a fait accompli as well in Internet governance debates as in international political and economic lives. Most of the academic publications have focused on the intertwining between domestic and international-related sovereignty challenges (Thumfart 2024; Bertrand & Le Floc'h 2024), or on industry-oriented prospects – especially from a European perspective (author 2023) but also from non-strictly Western lenses (Chander & Sun 2023; Belli & Jiang 2025). Even though these works may tackle digital sovereignty in the security realm (Csernatoni 2023), they focus on peacetime. In other words, although digital sovereignty has partly moved to contentious politics, the literature has not yet addressed how digital sovereignty is conceived of and practiced wartime. This contribution seeks to fill this gap by focusing on Ukraine since February 24th 2022, i.e. the unfinished context of the Russian large-scale invasion and occupation.

Indeed, occupied Ukraine has had to live with a first type of digital dependency: in Russian-annexed regions, digital networks were re-routed to the Russian Federation physical territory, hence enabling Russian decision-makers to submit digitally-consumed information in Eastern Ukraine to Russian (restrictive) laws (Pétiniaud 2024). A second type of digital dependency soon added to the first one. By decisively assisting Ukraine's war efforts, the (mainly) American technological companies (digital platforms, cybersecurity firms, satellite imagery providers, etc.) nonetheless created dependencies with Ukrainian government and organizations. Technical remediation, cyber threat assessment, "information warfare" documentation, data storage, etc., were all undertaken by massive private sector involvement.

This contribution will address this twofold challenge to digital sovereignty building on Mary Bridges' works on "infrastructure power" – understood as the linkages and chains of dependency that transcend national borders and defy traditional governance mechanisms, enabling a country to project power internationally (Bridges 2024). Operating by different rules than traditional forms of state control, infrastructure power as seen in post-2022 Ukraine has given tremendous reach to U.S. influence. We will demonstrate the two opposite ways actors involved – U.S. firms and Russia – have sought to use infrastructure power to enhance their position in the war, along different temporalities and with likely diverging longer-term effects. Besides, we will analyze how does Ukraine have "resisted" to this twofold compromission to its own digital sovereignty, showing that bypassing strategies towards the enemy (Russia) has proved more efficient than trying to reduce contract-made dependencies with private firms. The contribution will finally show that digital sovereignty is not a monolithic concept and that circumstances may weigh in its evolution, in both its nature and especially its expression and modalities.

Civilizational Claims in Cyberspace Governance: Russian Case Study

Liliya Khasanova (Tufts University)

Abstract

With the crisis of the liberal order and the rise of stronger multipolar currents, the global political landscape has witnessed a resurgence in the discourse surrounding 'civilization'. Preliminary analysis reveals an upsurge in cultural identity claims, encompassing normative, value-based, and identity assertions, often expressed through strong cyber sovereignty language – a trend not confined to Russia but resonating on a global scale. In Russia this revival has become particularly prominent in the aftermath of the invasion of Ukraine. The 2023 Russian foreign policy strategy explicitly discusses the country's unique civilizational and cultural identity as an Eurasian power.

This paper seeks to understand how civilizational identity claims are constructed and deployed to shape Russia's national and international law and policy-making in digital governance.

The research methodology comprises the following key components: (a) context analysis of the national policy and normative documents in the past twenty years in Russia, which would illustrate the evolution of Russia's incorporation of civilizational/cultural narratives into the cyber governance model; (b) context analysis of international statements and proposals made by state representatives in the main regional (EAEU, SCTO, BRICS, SOC) and international cyber negotiation forums; (c) discourse analysis of scholarly articles, press and narratives in governmental elites and tech sector that pertain to cyber governance strategies.

This paper begins by examining the concept of a 'civilizational claim' from an evolutionary perspective, focusing on its presence in both international and Russian law. I explore the various ways, forms, contexts, and terms in which these claims manifest, arguing that they represent a flexible, state-constructed narrative that influences policy-making and drives specific legal outcomes. I then describe the analysis of Russian national and international normative documents and proposals in the ICT field in the past 20 years.

Based on this analysis, I identify two key discourse elements that drive these claims: First, the perception of the Western cultural dominance in information space as a threat to 'cultural security'. Second, the need to resist this dominance as part of a broader moral collective international project.

The 'cultural security' logic finds its application both nationally and internationally. It has led to significant legal reforms that prioritize safeguarding cultural and civilizational values through 'territorialization' of the information space: the amendments on 'sovereign internet', strict data localization laws, and restrictions on foreign content incompatible with national values.

The ‘anti-Western’ logic of ICT governance emphasizes the promotion of state sovereignty, conventional lawmaking, and the forging of stronger regional cybersecurity agreements within BRICS, SOC, and EAEU. Furthermore, the 'civilizational choice' narrative proposes that Russia's model is better suited for countries sharing 'non-Western' cultural, political, and social values.

Based on these insights, I argue that a civilizational claim constructed by a Russian state enables a distinct protectionist approach to regulating information space nationally and a promotion of a specific model of cyber governance internationally. I conclude by outlining the implications of these findings for international cyber governance stating that the emergence of epicenters influenced by civilizational and geopolitical claims may lead to the development of distinct regional systems for addressing cybersecurity and Internet governance issues.

The Ninth European Multidisciplinary Conference on Global Internet Governance Actors, Regulations, Transactions and Strategies

ABSTRACT COLLECTION

GIG-ARTS 2025

ORGANISING COMMITTEE

Chairs: Francesco Amoretti, Nicola Palladino, Mauro Santaniello

GIG-ARTS Team: Carlos Andrés Fonseca Diaz

UNISA Team: Natascia Tatiana Fera, Armando Antonio Ferrara, Gerardo Ferrentino, Serena Fraiese, Chiara Spiniello, Grace X. Yang.

CONTACTS

events@gig-arts.eu

www.gig-arts.eu

www.internetpolicyresearch.eu