Politics and Governance
2025 • Volume 13 • Article 10461
https://doi.org/10.17645/pag.10461

ARTICLE

Open Access Journal

Beyond the Ban: TikTok and the Politics of Digital Sovereignty in the EU and US

Fabio Cristiano [1] and Linda Monsees [2]

[1] Department of History and Art History, Utrecht University, The Netherlands
[2] Institute of International Relations Prague, Czechia

Correspondence: Fabio Cristiano (f.cristiano@uu.nl)

Submitted: 1 April 2025 **Accepted:** 19 August 2025 **Published:** 8 October 2025

Issue: This article is part of the issue "The Geopolitics of Transnational Data Governance", edited by Xinchuchu Gao (University of Lincoln) and Xuechen Chen (Northeastern University London), fully open access at https://doi.org/10.17645/pag.i437

Abstract

This article explores the emergence of TikTok as a central issue in contemporary debates on foreign interference, platform regulation, and the governance of transnational data flows. Both the European Union and the United States have expressed concerns about TikTok's potential risks and have implemented various regulations. Through a comparative analysis of EU and US regulatory discourses, this article examines how claims to digital sovereignty are mobilised in efforts to govern the Chinese-based platform. In doing so, this study advances ongoing debates on the regulation of large-scale digital platforms and data infrastructures. Our analysis reveals that whereas the EU emphasises regulatory autonomy, public health, and democratic integrity in governing cross-border data flows, the US frames TikTok in a more overtly securitised approach rooted in techno-nationalism and strategic infrastructural decoupling from China. More broadly, the article also argues that when framed as a countermeasure to foreign interference, digital sovereignty is increasingly rearticulated as a security-centric concept that subsumes broader societal harms, and it risks assuming authoritarian connotations.

Keywords

digital sovereignty; European Union; foreign interference; platform regulation; public health; TikTok; transnational data governance; United States; youth protection

1. Introduction

Foreign interference, cybersecurity, and disinformation are among the key concerns policymakers have regarding the role of large social media platforms. In recent years, TikTok—the short-video platform owned by the Chinese company ByteDance—has become a catalyst for these concerns, prompting exceptional

global scrutiny and policy interventions, including national bans and ad-hoc restrictions in several countries (Gray, 2021; Jia & Liang, 2021). Both the EU and the US have placed TikTok at the top of their policy agendas, with ongoing procedures targeting the platform over concerns of foreign interference. For example, in December 2024, the European Commission launched an investigation into whether TikTok had played a role in facilitating electoral interference during Romania's annulled elections. A few weeks later, on his inauguration day in January 2025, President Trump announced the decision not to go ahead with the long-discussed US ban on the app, instead floating the idea of a takeover by an American sovereign fund. These most recent interventions point to a significant development: TikTok evolved from a video-sharing app popular among Gen Z into a central element of geopolitical struggles over digital technology and regulation.

Central to policymakers' concerns about TikTok are three interconnected issues: First, TikTok's ownership structure raises fears that Chinese authorities might access user data under China's expansive national security laws (Su & Tang, 2023). Second, permissive content moderation policies on the platform have been criticised for facilitating disinformation and amplifying authoritarian narratives (Bösch & Divon, 2024; Zeng & Kaye, 2022). Third, TikTok's unique personalised algorithm has sparked additional worries regarding mental health, addiction, and youth protection (Grandinetti & Bruinsma, 2023). Scholarship on TikTok has broadly explored these multiple concerns from a geopolitical perspective (see Bernot et al., 2024; Gray, 2021; Lin & de Kloet, 2023). In this article, we examine the EU and US regulatory discourses targeting TikTok as elements of enacting digital sovereignty against foreign interference. We situate the discussion firmly in the rising geopolitical and geoeconomic debates that shape contemporary platform and data governance efforts (Bellanova et al., 2022; Broeders, 2021; Fägersten et al., 2023).

Digital sovereignty is usually understood as the attempt to keep tighter control over digital infrastructure and data flows within national borders (Pohle & Thiel, 2020). In today's tense geopolitical context, it is often discussed alongside the threat of foreign interference, states or non-state actors trying to shape political and social life abroad through digital means (Dowling, 2021; Ördén & Pamment, 2022). What makes digital sovereignty particularly complex is the tension between the global, decentralised character of digital platforms and governments' territorial ambitions to regulate them. This article addresses this contradiction, paying particular attention to the way data localisation efforts illustrate it. In doing so, we draw attention to the way many different policy issues are deliberately wrapped into the language of digital sovereignty. This broadens the term's political usefulness, but at the same time leaves it increasingly vague. Taken together, these contradictions come to the fore when digital sovereignty is invoked as a framework for regulating platforms against the backdrop of today's tense geopolitical environment (Casero-Ripollés et al., 2023; Flyverbom et al., 2019; Monsees, 2024).

This article compares the EU and US approaches to regulating TikTok, examining two actors with seemingly distinct policies aimed at establishing digital sovereignty and/or strategic autonomy through decoupling from foreign partners and strengthening domestic supply chains. While both recognise the strategic importance of an autonomous digital infrastructure and share concerns about foreign interference, including from China, the EU and US approaches diverge significantly (Couture & Toupin, 2019). The EU articulates its digital sovereignty ambitions as a comprehensive strategic normative project that brings together democratic, economic, and geopolitical objectives (Bellanova et al., 2022). This framing manifests in systematic regulatory instruments such as the General Data Protection Regulation (GDPR), the Digital Services Act (DSA), and the Digital Markets Act (DMA). Conversely, the US prioritises digital sovereignty

through the lens of national security and technological supremacy over adversaries (Couture & Toupin, 2019). It thus favours more targeted interventions such as executive orders, investment screening, and targeted bans, such as the recent Protecting Americans from Foreign Adversary Controlled Applications Act (PAFACA). The relationship between the EU and the US on these matters is more ambivalent. While more autonomy is the mutual goal, they continue to perceive each other as partners in many areas. Yet, since the start of the second Trump administration, mutual trust in future cooperation has been eroding.

Regulating TikTok is embedded in a (re-)negotiation about the relationship with China. For the EU and US, policy debates around TikTok are to be understood considering broader geopolitical efforts to curb Chinese ambitions in establishing technological and market influence globally. These have been characterised as the "Beijing effect," emphasising how China reshapes data governance through infrastructural exports and normative influence (Erie & Streinz, 2021). This model challenges Western paradigms by promoting data sovereignty in other countries, albeit via centralised control by China (Creemers, 2022). As such, TikTok is increasingly viewed as a potential vector of Chinese influence and, therefore, an element of the broader geopolitical struggle over technology. TikTok is also the only non-US-based large social media platform, thus presenting a unique case study for testing and comparing EU and US approaches to digital sovereignty and the regulation of a digital platform which is "foreign" to both. In this article, we argue that both the US and the EU use TikTok as a trial case to test regulatory mechanisms despite their differences in threat depiction.

To explore these dynamics, our study employs a qualitative policy analysis of regulatory discourses. These include legislative texts, public statements, judicial rulings, and media reports from 2020 to mid-2025. This interpretative analysis focuses on the discursive construction of TikTok as a policy concern and security threat and how digital sovereignty is mobilised as a "discursive tool" within this scope (Pohle & Thiel, 2020). Considering the asymmetry in nature between the two compared actors, we focus on regulatory logics rather than deploying a systematic policy comparison. More concretely, we examine how the main themes in digital sovereignty debates—economic questions like trade and market access, geopolitical concerns such as surveillance and great power rivalry, and democratic issues including free speech and electoral integrity—find their way into regulatory discussions about TikTok (Floridi, 2020; Monsees & Lambach, 2022). We then consider TikTok's reactions to EU and US policies, noting both its moves toward compliance and the moments when it has openly pushed back. This helps us understand how digital sovereignty is shaped in relational terms. After this introduction, Section 2 sets out the conceptual tension between digital sovereignty and transnational data governance, with particular attention to the risk of foreign interference on social media platforms. Sections 3 and 4 turn to EU and US regulatory discourses on TikTok, examining how each frames the problem and the kinds of policy responses that follow. In Section 5, we compare the different approaches, pointing out where they overlap and where they diverge. The final section then considers what our findings mean, both for theory and for the practice of digital sovereignty.

2. Platform Regulation Meets Digital Sovereignty: From Foreign Interference to Data Localisation

This section outlines how the idea of digital sovereignty evolved across different political contexts. It then considers how it collides with platform regulation, most clearly around questions of foreign interference and efforts to localise data.

2.1. Digital Sovereignty: An Evolving Agenda

Digital sovereignty has become a prominent theme in policy and academic debates. In its earlier formulations, it has traditionally been understood as the authoritarian alternative to democratic platform and data governance, particularly in countries like China and Russia, where state control over digital infrastructures drifted away from multistakeholder models (Pohle et al., 2025; Litvinenko, 2021). In recent years, however, the term has also gained ground in liberal contexts. Within the EU, in particular, it relates to debates on strategic autonomy and the European ambition to reassert control over digital platforms (Broeders et al., 2023). Policy initiatives under the banner of digital sovereignty combine different aims: protecting the economy, reducing reliance on foreign actors, and building more resilient infrastructures (Floridi, 2020). Related language—"technological sovereignty," "strategic autonomy," or even "de-risking"—is often used interchangeably to describe the same rationale to secure financial, digital, and infrastructural resources (Bellanova et al., 2022).

At the heart of these debates lies the question of how far states can, and should, regulate the activities of transnational tech companies operating within their borders, and in doing so, reassert public authority over them (Floridi, 2020; Kelton et al., 2022). Some scholars consider this a necessary reassertion of public authority over private power (Farrand & Carrapico, 2022). In contrast, others warn that digital sovereignty may legitimise protectionist or illiberal policies under the guise of national security or strategic autonomy (Broeders et al., 2023). While digital sovereignty is often conceptualised within Western discourses as a liberal project promoting resilience and openness, its authoritarian roots reemerge nowadays in a geopolitical tense situation where security measures are enacted through the regulation of technology (Musiani, 2022; Pearson, 2024). As we argue in this article, this development is evident in recent digital sovereignty efforts enacted to counter foreign interference on social media platforms.

2.2. Foreign Interference and the Localisation of Data

The issue of foreign interference is thoroughly entangled with academic and policy conceptualisations of digital sovereignty. Pohle and Thiel (2020, p. 8) define digital sovereignty as "a state's ability to govern, regulate, and protect its digital infrastructure, data flows, and online activities independently, without undue external influence or interference." In its critique of the concept, Mueller (2020) argues that states think that by lacking digital sovereignty, they remain vulnerable to foreign interference through data manipulation, infrastructural control, or cyber espionage. They thus conceive and prioritise reasserting authority over digital platforms as an ontological aspect of their sovereignty. Foreign interference is, however, an elusive concept. On the one hand, it refers to illegitimate, covert manipulation efforts by a foreign entity aimed at interfering with democratic processes and sovereignty. The idea has also faced pushback when it is stretched to cover activities that, while adversarial, are considered lawful—like lobbying or political influence campaigns (Fridman, 2024). At times, it is muddled together with less precise concepts such as hybrid warfare, information warfare, or grey-zone tactics (Cristiano & van den Berg, 2024). Many European civil society groups have warned that leaving "foreign interference" loosely defined risks harming freedom of expression ("EU: Foreign interference directive," 2024). The TikTok case exemplifies the tensions around foreign interference, as states grapple with asserting territorial authority and sovereignty over a platform that crosses national boundaries and whose regulation is entangled with geopolitical competition with China.

Digital sovereignty's ambition to reassert public authority over transnational tech companies also intersects with strategies to govern data and its localisation within national borders (Komaitis, 2017). While states seek to assert territorial authority over digital infrastructures, efforts to impose borders on data are complicated by the decentralised global networks through which data flows operate (Meltzer, 2015). While some advocate for localisation measures, such as requiring data to be stored on servers within national borders, critics argue that such strategies are technically complex, economically costly, and risk fragmenting the internet into competing national silos (Mueller, 2017; Pohle & Santaniello, 2024; Radu, 2019). A growing body of scholarship challenges the binary opposition between transnational data flows and state territory. Lambach (2019) shows how it is continually deterritorialised and reterritorialised through practices like content filtering, infrastructure monitoring, and jurisdictional claims. Similar critiques have been developed in relation to different empirical contexts (Cristiano, 2019; Glasze et al., 2023; Salamatian et al., 2019).

Claiming sovereignty over data also introduces a legal and geopolitical dimension to the discussion on platforms and transnational data governance (Irion, 2012; Woods, 2018). Regarding TikTok, the platform's Chinese ownership raises fears that user data could be accessed by Chinese authorities, thereby undermining national sovereignty and user privacy. In addition, states are concerned with regulating platform content, especially the spread of disinformation and the lack of tools to control it. In this context, the issue is not only where the data are physically located but also which legal regimes apply to them and what this means for accountability and enforcement of data governance (Voss, 2020). In its ideal type, traditional platform governance models emphasise digital platforms' multi-actor dynamics and infrastructural politics. In contrast, digital sovereignty emphasises a state-centred claim to control digital technologies and infrastructures (ten Oever et al., 2024). In recent years, however, the concept has been reformulated in ways that increasingly dictate platform regulation (Pohle & Voelsen, 2022). States now seek to govern—or in some cases exclude—platforms in the name of protecting national interests, securing data, or shoring up political legitimacy. These moves extend beyond strategy and markets. They also reach into the terrain of fundamental freedoms and liberal values (Broeders et al., 2023). As discussed earlier in this section, both digital and data sovereignty intersect in the broader concern over foreign interference, which becomes the disruptive element in otherwise open digital ecosystems. When digital platforms are, or are even thought to be, influenced by a foreign entity, the legitimacy of transnational data flows becomes contested. This is particularly sensitive in places such as the EU, where openness of markets and protection of individual freedoms are taken as core principles (Broeders et al., 2023). Against this backdrop, the use of outright bans to safeguard digital sovereignty reveals another, and more fundamental, tension: how to reconcile liberal values with the need to assert control over data and infrastructures.

3. The EU and TikTok

This section explores the EU's multifaceted regulatory approach to TikTok as part of the Union's broader push for digital sovereignty and an increasingly assertive role in the digital domain. As the previous section highlighted, regulating platforms and countering foreign interference have become central to this project.

3.1. Frameworks and Regulations

The EU's concern with privacy and tech regulation can be traced back to the Snowden revelations, which set off intense debates about surveillance and state power (Deibert, 2015; Der Derian, 2022). Since then, its

regulatory mechanism has expanded dramatically. It now covers not only the largest social media platforms but also a broader set of multinational tech companies (Flonk et al., 2024). The DSA stands out among these measures. It is intended to protect consumers and safeguard citizens' rights (Heldt, 2022). It primarily protects privacy and freedom of speech. Through the DSA, the European Commission has initiated several investigations targeting TikTok and other companies, including X and Alibaba. The DSA is only one aspect of a broader trend of the EU's attempts to strongly regulate digital platforms, which also includes specific policies on foreign interference and data localisation—such as the EU's Cybersecurity Strategy (2020), the Network and Information Security (NIS2) Directive (2022), and data localisation initiatives like the GAIA-X project. In 2023, the European Commission issued a proposal to introduce harmonised EU-wide rules to ensure transparency of lobbying and interest representation activities conducted on behalf of third countries (European Commission, 2023). In line with the EU's quest for digital sovereignty and strategic autonomy, these attempts aim to strengthen the EU's position in relation to the regulation, control, and access to digital data and services. As discussed in the previous section, platform regulation, enhanced digital security, and geoeconomic aims are all interrelated in EU frameworks.

At the EU level, a series of proceedings has been opened against TikTok in recent years, as TikTok was accused of breaking the DSA and DMA regulations. In April 2023, TikTok was designated as a *very large online platform* under the DSA. In September 2023, ByteDance received the gatekeeper status under the DMA together with Alphabet, Amazon, Apple, Meta, and Microsoft. In February 2024, the Commission opened formal proceedings against TikTok under the DSA in areas "linked to the protection of minors, advertising transparency, data access for researchers, as well as the risk management of addictive design and harmful content" (European Commission, 2024a). In April 2024, proceedings were opened against TikTok Lite's reward programme in France and Spain, resulting in the withdrawal of TikTok Lite in August 2024 (European Commission, 2024c). In December 2024, TikTok was additionally asked to freeze and preserve data related to upcoming elections in the EU, and later, formal proceedings were subsequently opened regarding breaches of the DSA in the context of the Romanian election and TikTok's responsibility to mitigate risks of foreign interference. These proceedings are still open and remain unresolved at the time of writing. Within a relatively short timeframe, multiple proceedings have been initiated, targeting different concerns, including the protection of minors, consumer protection, and foreign interference with elections. The following sub-section will explore these distinct justifications in more detail.

3.2. Areas of Justification

One of the recurring themes in both public debate and EU policy about TikTok is the protection of minors, along with worries about addiction and mental health. These concerns are closely related to issues surrounding electoral interference as they both involve algorithmic design and control over platforms. However, they are distinct in that mental health concerns explicitly address health effects beyond solely political implications. The TikTok proceeding under the DSA is still ongoing. Nevertheless, the justification for the opening of the investigation by the DSA highlights how different concerns have been mobilised (European Commission, 2024a). The main areas of concern are risk management related to addictive designs, "rabbit holes," protection of minors, privacy and safety of minors, advertising transparency, and data access to researchers. The first three concerns fall predominantly under consumer protection and safeguarding minors. The European Commission (2024a) highlights explicitly "potentially addictive design" and the need to protect minors from harmful content. Furthermore, it emphasises general mental health concerns related

to the general concern about shared content on the platform. The text also explicitly mentions "the service's risk of leading users down 'rabbit holes' of harmful content," which already highlights that harmful content is not only content that is inappropriate to a specific age group but harmful for all users, e.g., dis- and misinformation or other anti-democratic content (European Commission, 2024a).

Mental health concerns are also at the forefront in the proceedings against TikTok Lite, which was accused of being "launched without prior diligent assessment of the risks it entails, in particular those related to the addictive effect of the platforms" (European Commission, 2024b). A quote by Thierry Breton, the former Commissioner for Internal Market of the European Union from 2019 to 2024, puts the EU's preoccupations in a nutshell:

> Endless streams of short and fast-paced videos could be seen as fun, but also expose our children to risks of addiction, anxiety, depression, eating disorders, low attention spans….We suspect TikTok 'Lite' could be as toxic and addictive as cigarettes 'light.' We will spare no effort to protect our children. (European Commission, 2024b)

The quote presents a strong-worded example of the Commission's portrayal as the primary agent protecting vulnerable children, creating a stark image of the EU's struggle against the robust tobacco industry.

This imagery finds a continuation when we look closer at the security concerns raised against TikTok and ByteDance. In 2023, the Commission banned TikTok from its employees' phones, citing cybersecurity concerns stemming from China (Chee, 2023). These security concerns are interlinked with fears of harmful content and disinformation. However, they differ in that the focus is less on TikTok's algorithms and their effects (e.g., addiction) and more on the security impact a Chinese-based company might have. In the justifications about the latest proceedings against TikTok regarding the EU elections and TikTok's negligence regarding risk reduction, familiar themes from the disinformation discourse reappear. Commission President Ursula von der Leyen summarises the concerns as follows:

> We must protect our democracies from any kind of foreign interference…..Following serious indications that foreign actors interfered in the Romanian presidential elections using TikTok, we are now thoroughly investigating whether TikTok violated the Digital Services Act by failing to tackle such risks. It should be crystal clear that in the EU, all online platforms, including TikTok, must be held accountable. (European Commission, 2024d)

Governing digital technology companies thus have the distinct aim of protecting democracy against foreign interference. The EU presents itself as a powerful and determined actor committed to safeguarding its citizens, whether concerning the mental health of minors or ensuring the integrity of democratic elections.

3.3. TikTok's Response

TikTok has responded to the EU's policy interventions unevenly. On some fronts, the company chose compliance. It signed the EU Code of Practice on Disinformation in June 2020 and later published a compliance roadmap. By June 2022, it had also accepted changes to meet EU consumer law requirements (European Commission, 2022). In other instances, TikTok embraced contestation. The company opposed its

designation as a gatekeeper under the DMA (TikTok, 2023). TikTok quickly removed its "Lite" program. Still, the EU believes it did not implement adequate measures in the context of the Romanian election, despite the data freeze and efforts to maintain order. TikTok's defence in the EU mainly relies on market-based arguments, claiming they are neither gatekeepers nor quasi-monopolists. When the app was banned from EU employees' phones, TikTok appealed by citing the importance of politicians and policy-makers to stay in touch with citizens:

> TikTok is enjoyed by 125 million EU citizens and potentially depriving users of access to their representatives is a self-defeating step, especially in our shared fight against misinformation and when this action is being taken on the basis of fears rather than facts. (Chee, 2023)

Thus, TikTok does not engage the EU, at least so far, in a language game of national military security but focuses instead on consumer rights, market freedoms, and the importance of social connection facilitated by the app. Security is only addressed through the topic of foreign interference via disinformation, which is perceived as a *threat* to democracy. The analysis of the different proceedings against TikTok shows how the EU is primarily concerned about foreign interference, which is getting tightly linked to notions of mental health and consumer protection. The regulation of TikTok fits within the broader regulation of all kinds of large platforms, but it is exceptional as it is a Chinese-based platform.

4. The US and TikTok

This section examines the shifting regulatory discourse on TikTok in the US, where the platform has become entangled in the geopolitical rivalry with China over technological dominance. We trace the evolution of state interventions, the justifications attached to them, and TikTok's attempts to respond.

4.1. Frameworks and Regulations

For most of the internet era, the US favoured a "light" normative approach. Platforms and tech companies were expected to regulate themselves. In this context, free speech and market liberalism outweighed state intervention. However, since the Russian interference in the 2016 presidential election, the US regulatory landscape shifted decisively to a more security-oriented approach, focusing particularly on foreign interference, data privacy, and geoeconomic competition (Flew & Gillett, 2021). Since early 2019, TikTok has been subject to multiple regulatory interventions focusing on data privacy violations, national security risks, electoral interference, and public health concerns. The PAFACA is the backbone of the US's attempts to restrict TikTok. The act authorises the executive branch to compel divestiture of any application designated a "foreign adversary-controlled application" (United States Congress, 2024, Section 2). Such a designation applies to applications that have more than one million users and are operated by entities domiciled, headquartered in, or organised under the laws of a country designated as a US foreign adversary (China, Russia, North Korea, or Iran) or by companies with at least 20% ownership by such entities (The White House, 2024). PAFACA thus targets ownership/control of the application and associated data access and dictates a divest-or-ban intervention.

PAFACA is the landing point of a longer federal trajectory. At the federal level, scrutiny of TikTok in the US began in February 2019, when the Federal Trade Commission fined Musical.ly/TikTok $5.7 million for

violating children's privacy under COPPA legislation. In August 2020, President Trump signed Executive Order 13942 and a divestment order aimed at forcing the sale of TikTok's US assets. Both were justified on grounds of national security and the risk of foreign interference (The White House, 2020). This move was quickly challenged. Preliminary injunctions blocked the orders later that year, and in June 2021, President Biden formally revoked them, replacing the measures with a broader directive to review foreign-controlled applications. In December 2022, the Biden administration passed the No TikTok on Government Devices Act (effective February 2023). Over the course of 2023, legislation expanded further, through bills such as the RESTRICT Act and the DATA Act, which were introduced to provide federal authority to limit or ban foreign-owned platforms (and thus circumvent the earlier preliminary injunctions). In April 2024, Congress finally enacted PAFACA, giving ByteDance a deadline in early 2025 to divest TikTok or face a nationwide ban. In January 2025, following his return to office, President Trump signed an executive order delaying enforcement by 75 days to allow negotiations on compliance, including ownership and data-localisation measures. At the time of writing (July 2025), the TikTok ban under PAFACA remains postponed.

4.2. Focus Areas

Central to the US policy discourse is the risk that Chinese authorities might access the data of American users or influence TikTok's systems. Trump's 2020 order warns that TikTok's "data collection threatens to allow the Chinese Communist Party access to Americans' personal and proprietary information" (The White House, 2020). Biden's substitute order reframed the issue at the level of classes of "connected software applications" controlled by foreign adversaries, emphasising unacceptable national-security risk from access to "vast swaths" of personal and business information (The White House, 2020). The two orders differ mainly in how directly they call out TikTok and its supposed links to Chinese authorities. What they share, however, is a focus on the danger that personal data could fall into the hands of a foreign adversary. Put differently, TikTok is cast less as a privacy issue in its own right than as a national security problem. In this framing, questions of data protection are absorbed into broader security imperatives. This is reflected in an official public discourse centred on a martial framing of TikTok. Exemplifying this trend, in a 2023 congressional hearing, House Energy & Commerce Committee Chair McMorris Rodgers bluntly told TikTok's CEO: "TikTok is a weapon by the Chinese Communist Party to spy on you, manipulate what you see and exploit [you] for future generations" (Knight First Amendment Institute at Columbia University, 2024).

Concerns about the risk of the Chinese acquisition of data, and the threat this poses to national security, are bundled together with different types of threats, including disinformation and health issues. Trump's 2020 order further contended that TikTok "may also be used for disinformation campaigns that benefit the Chinese Communist Party," referencing, for example, "TikTok videos [that] spread debunked conspiracy theories about the origins of the 2019 novel Coronavirus" (The White House, 2020). Other authorities have stressed the risk of influence associated with TikTok's Chinese ownership. In November 2022, the FBI director warned about "the possibility that the Chinese government could use [TikTok] to control data collection on millions of users or control the recommendation algorithm, which could be used for influence operations" (Shepardson, 2022). Lawmakers mobilise a diverse set of threats in their arguments against TikTok. Among these, US officials also frequently use public health analogies. These are meant to convey TikTok's perceived harm to society, particularly to children. For example, Rep. Gallagher, the initiator of the PAFACA bill, has called TikTok "digital fentanyl, addicting our kids, and just like actual fentanyl, it ultimately goes back to the Chinese Communist Party" (Hendrix, 2022). Interestingly, this analogy frames the app as addictive as a deadly opioid, and thus a

public health emergency caused by a hostile foreign power, a discourse resonating with the perceived Chinese responsibility for the Covid-19 pandemic. US lawmakers have also equated TikTok to other events related to China, such as a "spy balloon in your phone," and urged addressing the issue as was done with tobacco (Paul & Bhuiyan, 2023). These framings reinforce the bundling of security and health discourses, broadening the scope of digital sovereignty debates beyond geopolitical risk to societal resilience.

Finally, the US regulation of TikTok consistently conveys a focus on geoeconomic objectives by embedding them into a national security discourse. By allowing the restriction of platforms based on their physical location and their designation, the PAFACA's divestment provisions explicitly represent an extension of federal powers over the market. PAFACA highlights risks to the digital economy from undue foreign influence. This situates TikTok regulation within a geoeconomic logic linking market competitiveness and control to national security. Aiming to establish a new ownership structure "through the right deal"—a "sovereign wealth fund" or "a partnership with very wealthy people"—to mitigate national security concerns, Trump's second administration approach to TikTok also directly embraces economic objectives beyond the ban (Sutton & Mui, 2025). Finally, TikTok is also fully ingrained in the geopolitical debate on tariffs, with President Trump indicating his administration's willingness to reduce tariffs on China if Chinese authorities approve the sale of TikTok's US operations (Hoskins, 2025). In its latest reconfiguration, this ownership approach to platform regulation seems to mirror the authoritarian practices it claims to deter.

4.3. TikTok's Response

Against the backdrop of extensive regulatory pressure in the US, TikTok set out a broad compliance strategy intended to counter fears of geopolitical risk. At the centre of this effort was Project Texas, a $1.5 billion plan to localise American user data and cut operational dependencies on ByteDance's infrastructure in China. Under the proposal, all US user data would be stored on Oracle-managed servers located within the country, with access overseen by a newly created subsidiary, TikTok US Data Security. TikTok presented the project as an unprecedented step (Perault & Sacks, 2023). The company argued that the arrangement demonstrated its willingness to adapt to US regulatory expectations while offering safeguards framed in terms of national security. TikTok's efforts were also designed to anticipate and counter the enforcement logic of the PAFACA, which authorises the executive branch to ban or compel divestiture of applications deemed controlled by foreign adversaries. In a viral testimony before Congress, TikTok CEO Shou Zi Chew (2024) insisted that the platform was not "an agent of China or any other country" and repeatedly emphasised the independence of US operations from ByteDance. As soon as the PAFACA was approved, TikTok filed legal challenges, but the US Supreme Court upheld its constitutionality. In January 2025, in anticipation of the PAFACA ban, TikTok had suspended its services in the US, but these were restored as a result of Trump's postponement and ongoing negotiations.

5. Banning TikTok, Securing Sovereignty?

In this section, we compare the EU and US approaches to TikTok. We focus on convergences and differences in frameworks and regulations, as well as their focus areas and broader digital sovereignty frameworks.

Both the EU and the US approach TikTok with the same broad aim: to tighten control over foreign-owned digital platforms and to cast the app as a geopolitical issue. The similarity ends there. The EU targets platform

conduct within a codified legislative regime consistent with its "normative power" tradition of rule-based governance, consumer protection, and market oversight (Broeders et al., 2023). The US targets *ownership/control* through a more ad hoc, security-led, and executive-driven approach. While both approaches have extraterritorial reach, the EU embeds TikTok regulation in a generalised regime covering all very large platforms. In contrast, the US uses TikTok-specific and foreign adversary-targeted instruments that explicitly link regulation to geopolitical competition with China. Within the larger frameworks of platform regulation and transnational data governance, these responses demonstrate two approaches that differ by object—conduct (EU) versus control (US)—and remedy—risk mitigation (EU) versus divestiture/ban (US).

Although they seem to overlap—most clearly on foreign interference, data access, and risks to minors—the EU and US debates are fundamentally disaligned. Each highlights different problems and frames them in distinct ways. In the EU, TikTok is portrayed as a complex, systemic risk. In this framing, foreign interference is positioned alongside algorithmic harms such as addictive design, the spread of disinformation, and the mental health risks these dynamics pose—particularly for minors. Taken together, these concerns illustrate how the EU's digital sovereignty agenda folds public health, democratic integrity, and consumer protection into a single regulatory project. In this light, the EU's remedies emphasise risk assessments, design changes, transparency, and data access for researchers. On the other hand, the US places national security at the core, framing TikTok primarily as a vector for Chinese state influence through potential data access, espionage, and influence operations. Remedies emphasise structural separation (divestiture), prohibition, and device bans. While US discourse also invokes public health analogies, these primarily serve to reinforce the security frame by portraying social harms as the work of a hostile foreign adversary. The geoeconomic dimension is more explicit in the US case, where divestment is presented as both a security remedy and a market policy tool favouring domestic tech firms. In contrast, in the EU, it remains secondary to regulatory compliance.

In both cases, TikTok's responses combine compliance with selective contestation, but the strategic emphasis differs. The EU frames sovereignty as regulatory capacity to shape platform behaviour within a rules-based internal market, integrating security with consumer and democratic protections. The US frames it as the power to exclude or restructure foreign-controlled platforms to preserve national technological supremacy. In practice, both approaches blur the line between security governance and economic protectionism, illustrating that digital sovereignty is simultaneously a defensive and assertive project in platform regulation.

Taken together, the EU and US approaches to TikTok show that digital sovereignty cannot be treated as a single unified project. Instead, it operates as a shifting assemblage of security, economic, and societal objectives, each shaped by specific institutional traditions and geopolitical settings. Both the EU and the US invoke sovereignty claims to legitimise far-reaching interventions in platform regulation. Yet the reasoning behind them diverges. The EU favours a codified, multi-issue framework that reflects a regulatory sovereignty rooted in market and rights protection rationales. Contrarily, the US's executive-led security-centric measures embody a sovereignty grounded in strategic control and techno-nationalism. These differences highlight that digital sovereignty is best understood as a flexible, context-dependent repertoire of governing practices rather than a fixed doctrine. As such, it can accommodate liberal-democratic values even as it adopts interventionist or protectionist measures. At the same time, the US example—particularly its divestment provisions—shows how sovereignty discourses on digital technology can take on more authoritarian characteristics when used to legitimise expropriation or forced ownership

restructuring, practices more commonly associated with the approaches of China and Russia toward platforms (Polyakova & Meserole, 2019). This highlights the need to analyse digital sovereignty not only as a response to external threats such as foreign interference, but as an affirmative framework through which authority and internal scrutiny can be promoted or preserved.

6. Conclusion

This article has examined the regulation of TikTok in the EU and the US to analyse how digital sovereignty is operationalised in the governance of foreign-owned digital platforms. Both cases show how TikTok regulation forms part of broader strategies to (re-)assert some form of authority over digital infrastructures, reflecting an ongoing shift towards further geopoliticisation of transnational data governance. Specifically, both cases demonstrate how liberal democracies increasingly depend on the language and territorial logic of sovereignty to regain control over digital infrastructures. In doing so, they pursue seemingly different but substantively similar approaches that depart from earlier models of regulatory convergence and multistakeholderism. While the US emphasises national security and the EU prioritises broader societal harms, both cases illustrate the institutionalisation of a geopolitical approach to digital governance, combining concerns about foreign interference, market dominance, and security.

Regulating TikTok is thus not an exceptional endeavour but part of a broader shift in platform and data governance. At the same time, in both contexts, sovereignty claims extend beyond standard regulatory tools to include exceptional measures such as forced divestiture or market exclusion—policies more often associated with the approaches of China and Russia. What unites the EU and US approaches is a strategic reterritorialisation of digital governance, where regulating transnational platforms becomes a form of geopolitical intervention. This move fragments the global digital landscape and weakens the shared norms and interoperability on which the internet has long relied. At the core is a structural contradiction: digital infrastructures function across borders, but states continue to press for territorial control. Invoking digital sovereignty captures this contradiction. It demonstrates the concept's flexibility but also shows how easily it can be used to legitimise securitised—and at times authoritarian—forms of data governance. As our analysis indicates, we observe a normalisation of extraordinary measures and the bypassing of established channels for accountability, transparency, and public debate. Future research should examine how these trends affect countries outside the Global North (i.e., how the "Beijing effect" generates normative compliance and contestation). Of equal importance, further research is needed to understand how platforms adapt through compliance, legal contestation, or infrastructural reorganisation in the current tense geopolitical context.

Funding

Publication of this article in open access was made possible through the institutional membership agreement between Utrecht University and Cogitatio Press. Linda Monsees' work has been supported by the European Regional Development Fund project "Foreign Interference in the Context of Geopolitical and Technological Change" (reg. no.: CZ.02.01.01/00/23_025/0008692).

Conflict of Interests

The authors declare no conflict of interests.

References

Bellanova, R., Carrapico, H., & Duez, D. (2022). Digital/sovereignty and European security integration: An introduction. *European Security*, *31*(3), 337–355. https://doi.org/10.1080/09662839.2022.2101887

Bernot, A., Cooney-O'Donoghue, D., & Mann, M. (2024). Governing Chinese technologies: TikTok, foreign interference, and technological sovereignty. *Internet Policy Review*, *13*(1), 1–27. https://doi.org/10.14763/2024.1.1741

Bösch, M., & Divon, T. (2024). The sound of disinformation: TikTok, computational propaganda, and the invasion of Ukraine. *New Media & Society*, *26*(9), 5081–5106. https://doi.org/10.1177/14614448241251804

Broeders, D. (2021). Private active cyber defense and (international) cyber security—Pushing the line? *Journal of Cybersecurity*, *7*(1), Article tyab010. https://doi.org/10.1093/cybsec/tyab010

Broeders, D., Cristiano, F., & Kaminska, M. (2023). In search of digital sovereignty and strategic autonomy: Normative power Europe to the test of its geopolitical ambitions. *JCMS: Journal of Common Market Studies*, *61*(5), 1261–1280. https://doi.org/10.1111/jcms.13462

Casero-Ripollés, A., Tuñón, J., & Bouza-García, L. (2023). The European approach to online disinformation: Geopolitical and regulatory dissonance. *Humanities and Social Sciences Communications*, *10*(1), Article 657. https://doi.org/10.1057/s41599-023-02179-8

Chee, F. Y. (2023, February 28). European Parliament latest EU body to ban TikTok from staff phones. *Reuters*. https://www.reuters.com/technology/european-parliament-ban-tiktok-staff-phones-eu-official-says-2023-02-28

Chew, S. Z. (2024). *Testimony before the US Senate Committee*. United States Congress. https://www.judiciary.senate.gov/imo/media/doc/2024-01-31_-_testimony_-_chew.pdf

Couture, S., & Toupin, S. (2019). What does the notion of "sovereignty" mean when referring to the digital? *New Media & Society*, *21*(10), 2305–2322. https://doi.org/10.1177/1461444819865984

Creemers, R. (2022). China's emerging data protection framework. *Journal of Cybersecurity*, *8*(1), 1–12. https://doi.org/10.1093/cybsec/tyac011

Cristiano, F. (2019). Deterritorializing cyber security and warfare in Palestine: Hackers, sovereignty, and the national cyberspace as normative. *CyberOrient*, *13*(1), 28–42. https://doi.org/10.1002/j.cyo2.20191301.0002

Cristiano, F., & van den Berg, B. (2024). (Eds.). *Hybridity, conflict, and the global politics of cybersecurity*. Bloomsbury Publishing.

Deibert, R. (2015). The geopolitics of cyberspace after Snowden. *Current History*, *114*(768), 9–15. https://doi.org/10.1525/curh.2015.114.768.9

Der Derian, J. (2022). Quantum espionage: A phenomenology of the Snowden affair. *Intelligence and National Security*, *37*(6), 920–936. https://doi.org/10.1080/02684527.2022.2076341

Dowling, M. E. (2021). Democracy under siege: Foreign interference in a digital era. *Australian Journal of International Affairs*, *75*(4), 383–387. https://doi.org/10.1080/10357718.2021.1909534

Erie, M. S., & Streinz, T. (2021). The Beijing effect: China's Digital Silk Road as transnational data governance. *Journal of International Law & Politics*, *54*(1), 1–92.

EU: Foreign interference directive poses risks to freedom of expression. (2024, September 4). *Article 19*. https://www.article19.org/resources/eu-foreign-interference-directive-poses-risks-to-freedom-of-expression

European Commission. (2022, June 1). *EU Consumer protection: TikTok commits to align with EU rules to better protect consumers* https://ec.europa.eu/commission/presscorner/detail/en/ip_22_3823

European Commission. (2023). *Proposal for a Directive of the European Parliament and of the Council establishing harmonised requirements in the internal market on transparency of interest representation carried out on behalf of third countries*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52023PC0637

European Commission. (2024a, February 19). *Commission opens formal proceedings against TikTok under the Digital Services Act* [Press release]. https://ec.europa.eu/commission/presscorner/detail/en/ip_24_926

European Commission. (2024b, April 22). *Commission opens proceedings against TikTok under the DSA regarding the launch of TikTok Lite in France and Spain, and communicates its intention to suspend the reward programme in the EU* [Press release]. https://ec.europa.eu/commission/presscorner/detail/fen/ip_24_2227

European Commission. (2024c, August 5). TikTok commits to permanently withdraw TikTok Lite Rewards programme from the EU to comply with the Digital Services Act [Press release]. https://ec.europa.eu/commission/presscorner/detail/en/ip_24_4161

European Commission. (2024d, December 17). *Commission opens formal proceedings against TikTok on election risks under the Digital Services Act* [Press release]. https://digital-strategy.ec.europa.eu/en/news/commission-opens-formal-proceedings-against-tiktok-election-risks-under-digital-services-act

Fägersten, B., Lovcalic, U., Regnér, A. L., & Vashishtha, S. (2023). *Controlling critical technology in an age of geoeconomics: Actors, tools and scenarios*. Swedish Institute of International Affairs. https://www.ui.se/globalassets/butiken/ui-report/2023/ui-report-no.1-2023.pdf

Farrand, B., & Carrapico, H. (2022). Digital sovereignty and taking back control: From regulatory capitalism to regulatory mercantilism in EU cybersecurity. *European Security*, *31*(3), 435–453. https://doi.org/10.1080/09662839.2022.2102896

Flew, T., & Gillett, R. (2021). Platform policy: Evaluating different responses to the challenges of platform power. *Journal of Digital Media & Policy*, *12*(2), 231–246. https://doi.org/10.1386/jdmp_00061_1

Flonk, D., Jachtenfuchs, M., & Obendiek, A. (2024). Controlling internet content in the EU: Towards digital sovereignty. *Journal of European Public Policy*, *31*(8), 2316–2342. https://doi.org/10.1080/13501763.2024.2309179

Floridi, L. (2020). The fight for digital sovereignty: What it is, and why it matters, especially for the EU. *Philosophy & Technology*, *33*, 369–378. https://doi.org/10.1007/s13347-020-00423-6

Flyverbom, M., Deibert, R., & Matten, D. (2019). The governance of digital technology, big data, and the internet: New roles and responsibilities for business. *Business & Society*, *58*(1), 3–19. https://doi.org/10.1177/0007650317727540

Fridman, O. (2024). *Defining foreign influence and interference*. INSS Special Publication. https://www.inss.org.il/publication/influence-and-interference

Glasze, G., Cattaruzza, A., Douzet, F., Dammann, F., Bertran, M. G., Bômont, C., Braun, M., & Zanin, C. (2023). Contested spatialities of digital sovereignty. *Geopolitics*, *28*(2), 919–958. https://doi.org/10.1080/14650045.2022.2050070

Grandinetti, J., & Bruinsma, J. (2023). The affective algorithms of conspiracy TikTok. *Journal of Broadcasting & Electronic Media*, *67*(3), 274–293. https://doi.org/10.1080/08838151.2022.2140806

Gray, J. E. (2021). The geopolitics of 'platforms': The TikTok challenge. *Internet Policy Review*, *10*(2), 1–26. https://doi.org/10.14763/2021.2.1561

Heldt, A. P. (2022). EU Digital Services Act: The white hope of intermediary regulation. In T. Flew & F. R. Martin (Eds.), *Digital platform regulation: Global perspectives on internet governance* (pp. 69–84). Springer. https://doi.org/10.1007/978-3-030-95220-4_4

Hendrix, J. (2022, December 19). Is TikTok "digital fentanyl?". *TechPolicy Press*. https://www.techpolicy.press/is-tiktok-digital-fentanyl

Hoskins, P. (2025, March 27). China tariffs may be cut to seal TikTok sale, Trump says. *BBC News*. https://www.bbc.com/news/articles/c241ezrpg69o

Irion, K. (2012). Government cloud computing and national data sovereignty. *Policy & Internet*, *4*(3/4), 40–71. https://doi.org/10.1002/poi3.10

Jia, L., & Liang, F. (2021). The globalization of TikTok: Strategies, governance and geopolitics. *Journal of Digital Media & Policy*, *12*(2), 273–292. https://doi.org/10.1386/jdmp_00062_1

Kelton, M., Sullivan, M., Rogers, Z., Bienvenue, E., & Troath, S. (2022). Virtual sovereignty? Private internet capital, digital platforms and infrastructural power in the United States. *International Affairs*, *98*(6), 1977–1999. https://doi.org/10.1093/ia/iiac226

Knight First Amendment Institute at Columbia University. (2024). *Speech & the Border—Episode five: The free speech costs of banning TikTok*. https://www.knightcolumbia.org/content/speech-the-border-transcriptepisode-five-the-free-speech-costs-of-banning-tiktok

Komaitis, K. (2017). The 'wicked problem'of data localisation. *Journal of Cyber Policy*, *2*(3), 355–365. https://doi.org/10.1080/23738871.2017.1402942

Lambach, D. (2019). The territorialization of cyberspace. *International Studies Review*, *21*(3), 482–509. https://doi.org/10.1093/isr/viz022

Lin, J., & de Kloet, J. (2023). TikTok and the platformisation from China: Geopolitical anxieties, repetitive creativities and future imaginaries. *Media, Culture & Society*, *45*(8), 1525–1533. https://doi.org/10.1177/01634437231209203

Litvinenko, A. (2021). Re-defining borders online: Russia's strategic narrative on internet sovereignty. *Media and Communication*, *9*(4), 5–15. https://doi.org/10.17645/mac.v9i4.4292

Meltzer, J. P. (2015). The internet, cross-border data flows and international trade. *Asia & the Pacific Policy Studies*, *2*(1), 90–102. https://doi.org/10.1002/app5.60

Monsees, L. (2024). The paradox of semiconductors—EU governance between sovereignty and interdependence. *Cambridge Review of International Affairs*, *38*(1), 3–21. https://doi.org/10.1080/09557571.2024.2405915

Monsees, L., & Lambach, D. (2022). Digital sovereignty, geopolitical imaginaries, and the reproduction of European identity. *European Security*, *31*(3), 377–394. https://doi.org/10.1080/09662839.2022.2101883

Mueller, M. (2017). *Will the internet fragment?: Sovereignty, globalization and cyberspace*. John Wiley & Sons.

Mueller, M. (2020). Against sovereignty in cyberspace. *International Studies Review*, *22*(4), 779–801. https://doi.org/10.1093/isr/viz044

Musiani, F. (2022). Infrastructuring digital sovereignty: A research agenda for an infrastructure-based sociology of digital self-determination practices. *Information, Communication & Society*, *25*(6), 785–800. https://doi.org/10.1080/1369118X.2022.2049850

Ördén, H., & Pamment, J. (2022). *What is so foreign about foreign influence operations?* Carnegie Endowment for International Peace. https://carnegieendowment.org/2021/01/26/what-is-so-foreign-about-foreign-influence-operations-pub-83706

Paul, K., & Bhuiyan, J. (2023, March 23). Key takeaways from TikTok hearing in Congress—And the uncertain road ahead. *The Guardian*. https://www.theguardian.com/technology/2023/mar/23/key-takeaways-tiktok-hearing-congress-shou-zi-chew

Pearson, J. S. (2024). Defining digital authoritarianism. *Philosophy & Technology*, *37*(73), 1–19. https://doi.org/10.1007/s13347-024-00754-8

Perault, M., & Sacks, S. (2023, January 26). Project Texas: The details of TikTok's plan to remain operational in the United States. *Lawfare*. https://www.lawfaremedia.org/article/project-texas-the-details-of-tiktok-s-plan-to-remain-operational-in-the-united-states

Pohle, J., & Santaniello, M. (2024). From multistakeholderism to digital sovereignty: Toward a new discursive order in internet governance? *Policy & Internet*, *16*(4), 672–691. https://doi.org/10.1002/poi3.426

Pohle, J., & Thiel, T. (2020). Digital sovereignty. *Internet Policy Review*, *9*(4), 1–19. https://doi.org/10.14763/2020.4.1532

Pohle, J., & Voelsen, D. (2022). Centrality and power. The struggle over the techno-political configuration of the Internet and the global digital order. *Policy & Internet*, *14*(1), 13–27. https://doi.org/10.1002/poi3.296

Pohle, J., Nanni, R., & Santaniello, M. (2025). Unthinking digital sovereignty: A critical reflection on origins, objectives, and practices. *Policy and Internet*, *16*(2), 666–671. https://doi.org/10.1002/poi3.437

Polyakova, A., & Meserole, C. (2019). *Exporting digital authoritarianism: The Russian and Chinese models*. Brookings Institution.

Radu, R. (2019). *Negotiating internet governance*. Oxford University Press.

Salamatian, L., Gill, P., Ensafi, R., & Gill, H. (2019). The geopolitics behind the routes data travels: A case study of Iran. In *Proceedings of the 2019 ACM Internet Measurement Conference* (pp. 49–62). Association for Computing Machinery. https://doi.org/10.1145/3355369.3355592

Shepardson, D. (2022, November 15). U.S. FBI director says TikTok poses national security concerns. *Reuters*. https://www.reuters.com/business/media-telecom/us-fbi-director-says-tiktok-poses-national-security-concerns-2022-11-15

Su, C., & Tang, W. (2023). Data sovereignty and platform neutrality–A comparative study on TikTok's data policy. *Global Media and China*, *8*(1), 57–71. https://doi.org/10.1177/20594364231154340

Sutton, S., & Mui, C. (2025, February 3). Trump orders creation of sovereign wealth fund, hints it could buy TikTok. *Politico*. https://www.politico.com/news/2025/02/03/trump-sovereign-wealth-fund-tiktok-00202154

ten Oever, N., Perarnaud, C., Kristoff, J., Müller, M., Resing, M., Filasto, A., & Kanich, C. (2024). Sanctions and infrastructural ideologies: Assessing the material shaping of EU digital sovereignty in response to the war in Ukraine. *Policy & Internet*, *16*(4), 692–710. https://doi.org/10.1002/poi3.422

TikTok. (2023, November 16). *Appealing our 'gatekeeper' designation under the Digital Markets Act*. Newsroom TikTok. https://newsroom.tiktok.com/appealing-our-gatekeeper-designation-under-the-digital-markets-act?lang=en-150

The White House. (2020). *Executive order 13942: Addressing the threat posed by TikTok, and taking additional steps to address the national emergency with respect to the information and communications technology and services supply chain*. https://www.presidency.ucsb.edu/documents/executive-order-13942-addressing-the-threat-posed-tiktok-and-taking-additional-steps

The White House. (2024). *Executive order 14117: Preventing access to Americans' bulk sensitive personal data and United States government-related data by countries of concern*. https://www.presidency.ucsb.edu/documents/executive-order-14117-preventing-access-americans-bulk-sensitive-personal-data-and-united

United States Congress. (2024). *Protecting Americans from Foreign Adversary Controlled Applications Act*. https://www.congress.gov/bill/118th-congress/house-bill/7521

Voss, W. G. (2020). Cross-border data flows, the GDPR, and data governance. *Washington International Law Journal*, *29*(3), 485–532. https://digitalcommons.law.uw.edu/wilj/vol29/iss3/7

Woods, A. K. (2018). Litigating data sovereignty. *Yale Law Journal*, *128*(2), 328–406. https://www.yalelawjournal.org/pdf/Woods_i233nhrp.pdf

Zeng, J., & Kaye, D. B. V. (2022). From content moderation to visibility moderation: A case study of platform governance on TikTok. *Policy & Internet*, *14*(1), 79–95. https://doi.org/10.1002/poi3.287

About the Authors

Fabio Cristiano is an assistant professor in conflict studies at Utrecht University. His research explores the intersections of international security and emerging technologies, with a particular focus on cybersecurity and digital sovereignty. He is the editor of *Artificial Intelligence and International Conflict in Cyberspace* (2023) and *Hybridity, Conflict, and the Global Politics of Cybersecurity* (2024).

Linda Monsees is a senior researcher at the Institute of International Relations, Prague. Her research covers topics such as cybersecurity, disinformation, and digital sovereignty. Her work has been published in *International Political Sociology*, *International Affairs*, and *Security Dialogue*, among others.