Research

European Union scholars have only recently begun to examine the topic of digital sovereignty in a European policy context.

It has recently been seen a leitmotif for many states and even non-state actors, who are exploring ways of recapturing 'control' of the governance of the digital sector. It has a variety of different meanings and an equal variety of synonyms, such as network sovereignty, technological sovereignty, and cyber sovereignty (Benhamou and Sorbier 2006; Jackson Adams and Mohamad Albakajai 2016; Chen and Sintov 2016). It was originally used by states such as China to react to the increasing threats of globalisation (Thumfart 2022). In recent years, European actors, particularly at the EU level have started to adopt the language of digital sovereignty or variants of the term, such as 'open strategic autonomy' (Thieulin (2019);Floridi (2020);Pohle and Thiel (2020);Monsees and Lambach (2022);Glasze et al. (2023)). This curiosity in the use of digital sovereignty as a justification for policy development, particularly by the EU, whose 'sovereignty' is contested by many, has piqued interest in the term. Indeed, standardisation was identified as one of the key pillars of the European Commission's Strategic Foresight Report, which focused on the need for strengthened standards processes in order to help the EU develop its concept of open strategic autonomy (European Commission 2022a).

Accordingly, many have tried to explain how the digital economy transforms global institutions, or rather, how these actors – in the case of this literature, the EU – tries to shape its role in these global spaces (Barrinha and Christou 2022). Others, such as Couture and Toupin (2019), have looked at how "sovereignty in relation to the digital" also incorporates different communities (such as indigenous communities). The emergence of new technological challenges and powerful (corporate) actors acting globally in the digital domain contributes to what Gammeltoft-Hansen and Adler-Nissen have termed as a process of "expansion of the playing field related to sovereignty" (Gammeltoft-Hansen and Adler-Nissen 2008).

To understand how digital sovereignty is used as a guiding framework for policy in this area, Adler-Nissen and Gammeltoft-Hansen offer insights from a critical studies perspective (2008). To understand the functioning of sovereignty claims, who performs them, and under which conditions, the authors put forward three key features – players, rules, and moves. Where the players are the ones that enact sovereignty claims, moves would be the strategic use of these claims through political and legal practices to achieve different outcomes. Rules would represent the legal content of sovereignty and "reflect the nonexplicit rules that structure the way we think and act in the name of sovereignty." (ibid.) Moreover, this framework understands (digital) sovereignty not as a claim to supreme authority in a given territory or policy field, but as form of legitimation for a new sort of politics – the sovereignty playing field – where the EU's claim to (digital) sovereignty become understood as meaningful by other players, allowing it to be accepted as a global player, and authority, on digital issues. In framing sovereignty in this way, it reflects the ongoing discussions about the use of the concept as an act of legitimation (Werner and De Wilde 2001).

Indeed, Emmanuel Macron in his speech on 'the Quest for European sovereignty' (2017), described this desire to seek international acknowledgment as a sovereign player: "European sovereignty requires constructing, and we must do it. Why? Because what constructs and forges our profound identity, this balance of values, this relation with freedom, human rights and justice cannot be found anywhere on the planet. This attachment to a market economy, but also social justice". This sentiment was echoed by Commission President von der Leyen (2020): " 'Digital sovereignty' is not just an economic concept. We are a Union of values. One of the great questions is: How can we preserve and promote our values in a digitised world?". Here, I identify the use of digital sovereignty as a legitimating tool, to enable the European Commission to position itself as an equal partner with a specific (domestic) goal of protecting European values in the digital realm (Roberts et al. 2021; Seidl and Schmitz 2023; Heidebrecht 2024).

Alongside the legitimation argument, securitization as part of the digital sovereignty discourse and practice in the EU has come to the fore (see Lambach and Oppermann 2022 for the German narratives around digital sovereignty). Adler-Nissen and Eggeling see digital sovereignty as a " 'third-way' alternative to US surveillance capitalism and Chinese and Russian techno-authoritarianism" (forthcoming p.2), focusing on how this term reflects the increased geopoliticisation of the EU. In building on previous work mentioned above, they see digital sovereignty as a performative discourse, with security as being central to their understanding of how this is executed. In a similar vein, Bellanova et al (2022) reveal that the digital sovereignty as security approach can be coined as the EU's attempt to "control digital security infrastructures" (p.338), which impacts on the nature of European Security integration. Farrand and Carrapico (2022) build on this argument, by stating that digital sovereignty is epitomized by a shift to 'regulatory mercantilism', where the European Commission moves towards oversight and control of the (generally U.S.) private sector actors. Regulatory mercantilism in cybersecurity policy, or neo-dirigiste turns in the EU's industrial policy (Seidl and Schmitz 2023) are markers that reveal a more proactive attempt from the EU (and particularly the European Commission) to position itself as a key player in the global digital economy.

As the literature above argues, the European Commission has used (variants of) digital sovereignty as a tool to legitimise a turn to securitisation of cyberspace within its borders. The EU, through various legislative acts and agencies (Cyber Resilience Act, NIS 2 directive, the EU's Cybersecurity Agency ENISA, and the establishment of the Cybersecurity Competence Centre) has developed a competence inside its borders. This paper contributes to these debates by describing how it uses this security turn to allow it to exercise its domestic competences on a global level. I will argue that the European Commission's use of the language of digital sovereignty as security works to enhance its capacity to work alongside other sovereigns (such as the U.S.) in combating common threats. In this way, digital sovereignty is used as a particular European-Commission-led manifestation of the securitisation of cyberspace. However, the consequences of the use of digital sovereignty as security discourse has important consequences, as Perarnaud and Rossi note: "the most important outcome of these developments relates to one of its unintended consequences – the legitimation of a discursive push towards a state-centred vision of Internet standardisation" (2023, 17).

Benhamou, Bernard, and Laurent Sorbier. 2006. "Souveraineté et réseaux numériques." *Politique étrangère* Automne (3): 519. https://doi.org/10.3917/pe.063.0519.

Chen, Bingye, and Nicole Sintov. 2016. "Bridging the Gap Between Sustainable Technology Adoption and Protecting Natural Resources: Predicting Intentions to Adopt Energy Management Technologies in California." *Energy Research & Social Science* 22 (December): 210–23. https://doi.org/10.1016/j.erss.2016.10.003.

Floridi, Luciano. 2020. "The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU." *Philosophy & Technology* 33 (3): 369–78. https://doi.org/10.1007/s13347-020-00423-6.

Glasze, Georg, Amaël Cattaruzza, Frédérick Douzet, Finn Dammann, Marie-Gabrielle Bertran, Clotilde Bômont, Matthias Braun, et al. 2023. "Contested Spatialities of Digital Sovereignty." *Geopolitics* 28 (2): 919–58. https://doi.org/10.1080/14650045.2022.2050070.

Jackson Adams, and Mohamad Albakajai. 2016. "Cyberspace: A New Threat to the Sovereignty of the State." *Management Studies* 4 (6). https://doi.org/10.17265/2328-2185/2016.06.003.

Monsees, Linda, and Daniel Lambach. 2022. "Digital Sovereignty, Geopolitical Imaginaries, and the Reproduction of European Identity." *European Security* 31 (3): 377–94. https://doi.org/10.1080/09662839.2022.2101883.

Pohle, Julia, and Thorsten Thiel. 2020. "Digital Sovereignty." *Internet Policy Review* 9 (4). https://doi.org/10.14763/2020.4.1532.

Thieulin, Benoit. 2019. "Towards a European Digital Sovereignty Policy." https://www.lecese.fr/sites/default/files/travaux_multilingue/2019_07_souverainete_europeenne_numerique_GB_reduit.pdf.

Thumfart, Johannes. 2022. "The Norm Development of Digital Sovereignty Between China, Russia, the EU and the US: From the Late 1990s to the Covid-Crisis 2020/21 as Catalytic Event." In *Enforcing Rights in a Changing World*, edited by Dara Hallinan, Ronald Leenes, and Paul de Hert, 1–44. Computers Privacy Data Protection (CPDP) 14. London: Hart Publishing.