frontiers | Frontiers in Political Science

TYPE Original Research
PUBLISHED 05 February 2025
DOI 10.3389/fpos.2025.1548562

Check for updates

OPEN ACCESS

EDITED BY
Fanni Tanács-Mandák,
National Public Service University, Hungary

REVIEWED BY
Dominika Moravcová,
University of Trnava, Slovakia
Michal Janovec,
Masaryk University, Czechia

*CORRESPONDENCE
Gábor Hulkó
✉ hulko.gabor@ga.sze.hu

RECEIVED 19 December 2024
ACCEPTED 23 January 2025
PUBLISHED 05 February 2025

CITATION
Hulkó G, Kálmán J and Lapsánszky A (2025) The politics of digital sovereignty and the European Union's legislation: navigating crises.
Front. Polit. Sci. 7:1548562.
doi: 10.3389/fpos.2025.1548562

The politics of digital sovereignty and the European Union's legislation: navigating crises

Gábor Hulkó*, János Kálmán and András Lapsánszky

Ferenc Deák Faculty of Law and Political Sciences, Széchenyi István University, Győr, Hungary

In recent years, the resistance of member states to the strengthening of the European Union and its ambition to extend the powers of nation states has become a dominant political element, especially in the countries of the Central and Eastern European region. At the same time, both nation states and the EU are facing a number of global challenges, one of the most significant of which, alongside climate change, is digitalization. At the dawn of the digital age, technological innovation and the free flow of information promised unprecedented opportunities. However, as digital technologies have increasingly permeated all aspects of economic, social and political life, they have created new crises and challenges, particularly with regard to digital sovereignty. This research explores the complex and interdisciplinary nature of digital sovereignty, with a particular focus on the crises that digitalization has triggered and caused. These crises manifest themselves in various forms, including cybersecurity threats, privacy issues and the economic dominance of global technology companies. The European Union's legislative initiatives, including the Digital Services (DSA), Digital Markets (DMA) and European Media Freedom (EMFA) regulations, as well as the efforts to regulate artificial intelligence, are designed to address the crises inherent in the digital age, while at the same time posing new challenges to the sovereignty and perception of sovereignty of individual states. The research examines the EU's legislative efforts in navigating the politics of digital crises. It sheds light on the interplay between national self-determination and the EU's overall regulatory framework, highlighting the ongoing struggle to balance control and cooperation in a rapidly changing digital environment. The analysis will provide a deeper understanding of how digital sovereignty is shaped by and responds to crisis policy, and insights into the future of digital governance in an increasingly interconnected world. It also seeks to assess the extent to which recently introduced EU legislation can be harmonized with the policy objective of strengthening the autonomy of nation states. This is particularly important in the context of the legislation and practices observed in countries with relatively small populations, such as Hungary, Slovakia and the Czech Republic.

KEYWORDS

state intervention, digital markets, digital sovereignty, innovation, crisis

1 Introduction

At the dawn of the digital age, technological innovation and the free flow of information promised opportunities that were previously unimaginable. The acceleration of global communications, the democratization of information, access to information and the emergence of new digital technologies have given hope that we are entering a new era of human development through digitalization. However, as digital technologies have become more deeply integrated into all aspects of economic, social and political life, a number of new crises and challenges have emerged that threaten the transparency, security and fairness of the digital world.

The rise of digitalization has been accompanied by the emergence of a new form of sovereignty, digital sovereignty. The concept of digital sovereignty refers to the ability of a state or region to manage and regulate its own digital infrastructure, data management and technological development, while protecting the rights and interests of its citizens in the global digital ecosystem. This concept is particularly important for the European Union, which has made digital sovereignty a priority in the areas of data protection, cybersecurity and technological innovation.

One of the biggest challenges of the digital age is crisis management, the ability of states to make and implement decisions that can lead to rapid and strategic intervention. These crises take different forms. Attacks by state and non-state actors that threaten the digital infrastructure of states and companies. Inappropriate handling of personal data and lack of privacy that undermine citizens' trust in digital technologies. The dominance of global technology companies such as Google, Amazon, Facebook, Apple and Microsoft (collectively referred to as GAFAM), which distort competition and limit the opportunities for smaller players.

The European Union finds itself in a particularly complex situation in the implementation of digital sovereignty. On the one hand, one of the EU's main objectives is to strengthen its own strategic autonomy in the digital world, especially in the face of the influence of global technology companies. On the other hand, there are significant differences between EU Member States in the way digital sovereignty is understood and implemented, especially in the Central and Eastern European region.

Countries in Central and Eastern Europe, such as Hungary, Slovakia and the Czech Republic, are paying particular attention to preserving nation-state sovereignty, while at the same time facing global digital challenges. These countries are particularly sensitive to issues of technological innovation and regulatory autonomy due to their smaller populations and limited economic resources. EU legislative initiatives, including regulations on digital services, digital markets and media freedom in Europe, as well as efforts to regulate artificial intelligence, are crucial to addressing digital challenges, but could also create new conflicts over the autonomy of nation states.

This study examines the EU's legislative approach to navigating the crises inherent in the digital ecosystem. It focuses on key regulations, including the General Data Protection Regulation (hereinafter GDPR),[1] the Digital Services Act (hereinafter DSA),[2] the Digital Markets Act (hereinafter DMA),[3] and the European Media Freedom Act (hereinafter EMFA),[4] as well as emerging initiatives like the Artificial Intelligence Act (hereinafter AI Act).[5] These legislative efforts aim to address the multifaceted challenges of the digital age while grappling with tensions between national sovereignty and supranational governance.

The research also delves into the perspectives of Central and Eastern European countries, where the preservation of national sovereignty remains a critical political concern. The study evaluates the extent to which EU-wide digital policies align with the unique priorities of smaller member states, such as Hungary, Slovakia, and the Czech Republic. By analyzing the interplay between EU legislation and national autonomy, the research offers insights into the evolving landscape of digital governance within the Union.

Briefly this research aims to analyze the evolving concept of digital sovereignty in the EU, with a focus on the legislative efforts addressing digital crises and their implications for Central and Eastern European countries.

2 Materials and methods

The research employs a qualitative and interdisciplinary methodology, focusing on the intersection of legal, political, and technological dimensions of digital sovereignty. The study integrates a comprehensive analysis of key legislative frameworks within the European Union, including the GDPR, DSA, DMA, EMFA, and the proposed AI Act. It also examines secondary sources, such as policy documents, academic articles, and case studies from Central and Eastern Europe.

The study is rooted in a qualitative research design that integrates legislative analysis, comparative case studies, and thematic content analysis. This approach ensures a nuanced understanding of the legal and political dimensions of digital sovereignty within the EU.

The research focuses on critical legislative instruments, including GDPR, DSA, DMA, EMFA, and the AI Act. The research also includes case studies of Hungary, Slovakia, and the Czech Republic to highlight regional variations in the implementation and reception of EU digital policies. These countries were selected for their distinct political and economic contexts, offering a representative perspective on the challenges and opportunities of aligning national and EU-level digital sovereignty goals. Policy documents, academic articles, and government reports were systematically analyzed to identify recurring themes and patterns in the discourse surrounding digital sovereignty.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (hereinafter GDPR), OJ L 119, 4.5.2016, p. 1–88.

[2] Regulation (EU) No 2022/2065 of the European Parliament and of the Council of 19 October 2022 on the Digital Single Market and amending Directive 2000/31/EC (the Digital Services Regulation) (hereinafter the DSA Regulation), OJ L 277, 27.10.2022, p. 1–102.

[3] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on competitive and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (hereinafter the DMA Regulation), OJ L 265, 12.10.2022, p. 1–66.

[4] Regulation (EU) No 2024/1083 of the European Parliament and of the Council of 11 April 2024 establishing a common framework for media services in the internal market and amending Directive 2010/13/EU (the European Media Freedom Regulation) (hereinafter the EMFA Regulation), OJ L, 2024/1083, 17.4.2024.

[5] Regulation (EU) No 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized rules for artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) No 2018/858, (EU) No 2018/1139, (EU) No 2019/2144 and Directives 2014/90/EU, (EU) No 2016/797 and (EU) No 2020/1828 (the AI Regulation) (hereinafter the AI Act), OJ L, 2024/1689, 12.7.2024.

The study's methodology can be replicated by adopting a similar legislative analysis framework across different EU member states or expanding the case studies to include Southern European nations facing parallel sovereignty concerns.

3 Results

3.1 The concept and elements of digital sovereignty

Digital sovereignty is closely related to the traditional notion of state sovereignty, which refers to the right and ability of states to manage their domestic and foreign affairs autonomously (Lansing, 1914, 61; Philpott, 1995, 355; Steinbach, 2024, 51). However, in the digital age, state sovereignty faces new challenges as global technological companies and the borderless internet pose new threats (Falkner et al., 2024, 2,100). Digital sovereignty requires states to be able to regulate and control digital services and infrastructures, ensuring that the rights of their citizens are protected and their national interests are safeguarded (Suzor, 2018).

Digital sovereignty is a complex and dynamic concept that encompasses several different elements (Couture and Toupin, 2019; Mueller, 2020; Pohle and Thiel, 2020; Roberts et al., 2021; Schmitz et al., 2023). Digital sovereignty is broadly defined as the ability of a country or region to exercise control over its own digital infrastructure, data use and technological developments, independent of external influence (Chander and Sun, 2021; Floridi, 2020; Sheikh, 2022). Digital sovereignty therefore necessarily includes the ability to make strategic decisions, develop legislation and enforce law in the digital space.

Digital sovereignty includes data sovereignty, technological sovereignty, cybersecurity sovereignty and legislative sovereignty. Data sovereignty is the ability of a country or region to exercise full control over the data collected and processed on its own territory. Data sovereignty also extends to the definition of legal and regulatory frameworks for data protection and data management, as well as the development of a national data economy (Hummel et al., 2021). Technological sovereignty already refers to the ability of a country or region to independently develop and control its own technological infrastructure and assets, including hardware, software and network systems. Technological sovereignty is particularly important for national security and innovation (Roumate, 2024). Cybersecurity sovereignty ensures that a country or region can protect its own digital infrastructure and systems from cyber threats. Cybersecurity sovereignty includes the implementation of cybersecurity standards and certifications, and the establishment of mechanisms to manage cybersecurity incidents (Farrand and Carrapico, 2022). Finally, legal sovereignty refers to the ability of a country or region to create and enforce its own legal rules in the digital space. This includes the regulation of online services, digital platforms and e-commerce (Novikov, 2024).

It is important to emphasize that the concept of digital sovereignty and its elements are still evolving, with different countries and regions interpreting and applying it differently. The European Union places a strong emphasis on citizens' data protection and technological independence. The EU aims to become independent from non-EU technology companies and to ensure the privacy and security of its citizens' data. The US approach focuses on promoting technological innovation and free market competition rather than digital sovereignty (Metakides, 2022). The US tech giants (GAFAM), with their global dominance, make the US less focused on digital sovereignty (Liman and Weber, 2023). In contrast, China is strongly pushing to ensure its digital sovereignty, with strict internet regulations and state control over its technological infrastructure. China aims to independently develop and manage its own digital technologies and to minimize external influence in the digital space (Kokas, 2023).

The concepts of digital sovereignty and state sovereignty are closely intertwined in the digital age and pose new challenges for states. The traditional notion of state sovereignty is complemented by a digital dimension that requires new types of regulatory and policy approaches. At the same time, the concept of digital sovereignty is dynamic and constantly evolving as technological developments and the global political environment change. While there is no complete consensus on the exact definition of the concept, digital sovereignty is increasingly becoming a central issue in national and international policy discourse. The example of the EU shows that digital sovereignty is not only a technological or economic issue, but is also essential for national security, citizens' rights and political autonomy.

3.2 The crisis and crisis management

The term "crisis" refers to critical situations that require immediate and strategic responses and in which there is a risk of disruption or collapse of the normal order of operations (Eastham et al., 1970). Crises typically require uncertainty, unpredictability and urgent solutions. In political science, crisis situations are tests of the capacity of power, resources and institutions to function, in which states and organizations are forced to make rapid decisions and adapt flexibly (Hay, 2013).

The digital age has added a new dimension to crises: the speed of technological development and the decentralized nature of the global digital ecosystem mean that crises can occur at both local and global levels. Crises in the digital space are different from traditional political or economic crises because they are more complex from a technological, privacy and cybersecurity perspective, happen faster and often involve invisible or difficult to identify actors.

Crisis management or the politics of crisis is a theoretical framework that describes how sovereign states and international organizations deal with crisis situations (Boin, 2008; McConnell, 2020). This theoretical approach is based on three main dimensions. The first step in crisis policy is to identify the situation quickly and accurately. This involves assessing threats and risks, and assessing the potential consequences. In the digital age, this is particularly difficult as crises are often hidden, for example in the form of cyber-attacks or data security incidents. The second dimension of crisis policy is the development and implementation of responses. This involves taking government action, putting in place regulatory or legal frameworks and mobilizing relevant institutions and actors. Addressing digital crises often requires a multidisciplinary approach involving public authorities, technology companies and civil society. Finally, the third stage of crisis policy is to draw lessons and adapt the policy, legal or institutional framework to better manage future crises. This is particularly important in the digital space, where technology is constantly evolving and previous solutions can quickly become obsolete.

Digital crises have specific characteristics that distinguish them from traditional crises (Lapsánszky, 2021, 140). Cyber attacks, ransomware attacks and other cyber security incidents threaten the functioning of states and companies, as well as the data and privacy of citizens. Personal data breaches, data theft and data security incidents undermine citizens' digital rights and trust. The dominance of global technology companies distorts digital markets and limits the regulatory space of national governments. Digital crises are often global in nature, as technology infrastructures and data flows know no borders. This makes it difficult for individual states to manage crises independently (Saka et al., 2024).

Crisis management plays a central role in achieving digital sovereignty, as crisis management and prevention fundamentally affect the ability of states to manage their digital spaces. Suffice it to say in this regard that managing data security incidents requires that states are able to exercise control over data, including its storage, processing and sharing. The procedures and measures used during cyber security crises directly affect the technological independence and defense capabilities of states.

At the same time, it is worth pointing out here that action against global players dominating digital markets, such as the Digital Markets Act (DMA) introduced by the EU, can be seen as part of the acquisition of crisis management capacity (Rojszczak, 2023). Cooperation between states is essential to tackle digital crises, especially at EU level, where common regulatory frameworks and strategies strengthen collective resilience.

Crisis and crisis management is at the heart of digital sovereignty, as states need to be able to effectively manage crises in the digital space, which in turn fundamentally affects their sovereignty. The example of the European Union illustrates that the crises of the digital age require a new approach to public policy and regulation because of their global, decentralized and rapidly changing nature. Crisis-related public policy is not only about crisis management, but also about how states and international organizations can anticipate, adapt and learn from these situations, while protecting their citizens and interests in the digital space.

3.3 Historical overview and the current issues-the evolution of digital policies in the European Union

Digital policies in the European Union have evolved significantly over the past decades. Initially focused on promoting the internal market and economic integration, the EU has increasingly focused on digital infrastructure, data protection and cybersecurity as technology has developed and digitalization has advanced. The EU's digital strategies aim to develop a digital economy and society and to create a Digital Single Market. Throughout the development of the EU's digital policies, a number of key milestones and decisions have been taken that have fundamentally shaped the pursuit of digital sovereignty (Floridi, 2020).

The starting point for EU digital policy is the Data Protection Directive,[6] which was the first major piece of data protection legislation in the European Union. The Data Protection Directive set out the principles and rules for data protection. This Directive ensured the protection of EU citizens' personal data and paved the way for the introduction of subsequent regulations, such as the GDPR. The next key standard was the ecommerce Directive,[7] which created the legal framework for e-commerce and facilitated the development of online services and commerce in the EU. The Directive aimed to promote the growth of the digital economy while ensuring the protection of consumer rights in the online space.

Building on the Directive, the European Union adopted the Digital Agenda in 2010,[8] which was the EU's overarching digital strategy. The EU set the goal of developing a digital economy and society. The Agenda stressed the importance of creating a single digital market based on high-speed, superfast internet and interoperable applications to deliver sustainable economic and social benefits. Under the Digital Agenda, the EU has introduced a range of measures to develop digital infrastructure and stimulate innovation.[9]

Finally, it is necessary to highlight the GDPR, a landmark piece of legislation in the field of data protection. The GDPR introduced strict data protection rules in the EU to ensure the foundations of digital sovereignty. It aims to protect the personal data of individuals and to increase the responsibility of data controllers. The impact of the GDPR goes beyond EU Member States, as many non-EU companies have also adapted to the rules to continue providing services to EU citizens and businesses in the internal market. In addition to the GDPR, the EU Cybersecurity Act[10] has strengthened the EU's cybersecurity capabilities and introduced EU-wide cybersecurity certification for information and communication technology (ICT) products and services. The Cybersecurity Act aims to enhance the security and protection of the EU's digital infrastructure against cyber threats and to increase trust in digital products and services. In addition to the above, the so-called NIS 2 Directive[11] obliges Member States to report cybersecurity incidents and to cooperate in the management of cybersecurity incidents.

Following the emergence and evolution of the European Union's digital policies, the Commission has set out its vision for the period up to 2030 in its Communication "Digital Agenda 2030: A European

[6] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, p. 31–50.

[7] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, OJ L 178, 17.7.2000, p. 1–16.

[8] COM (2010)245 the Digital Agenda for Europe.

[9] Such measures have included support for infrastructure development related to broadband internet access, or the introduction of e-government services, the development of e-health systems, and increasing the availability of digital public services.

[10] Regulation (EU) No 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Cybersecurity Agency) and the certification of information and communication technologies for cybersecurity and repealing Regulation (EU) No 526/2013, OJ L 151, 7.6.2019, p. 15–69.

[11] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures to ensure a high uniform level of cybersecurity throughout the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 and repealing Directive (EU) 2016/1148, OJ L 333, 27.12.2022, p. 80–152.

way to deliver the Digital Decade"[12] to empower citizens and businesses through digital transformation. Building on this, the Digital Decade 2030 policy agenda[13] established a monitoring and cooperation mechanism to achieve the common objectives and targets of Europe's digital transformation. And in the Declaration on Digital Rights and Principles, the EU has set out principles for the enforcement of European values underpinning digital sovereignty.[14]

As a first step in the policy programme, the European Commission has defined key performance indicators (KPIs) in an implementing act.[15] The KPIs are based on the existing DESI exercise, which measures the state of Europe's digital transformation every year. Subsequently, the European Commission, in cooperation with the Member States, published EU-wide trajectory indicators to assess whether the progress made against each target is sufficient to reach the 2030 targets.[16] Each year, the European Commission publishes a Digital Decade Progress Report, which assesses and evaluates progress towards the EU-level trajectories and the final Digital Decade targets, and proposes further actions and efforts where necessary. The first Digital Decade Progress Report was published in 2023.[17]

Each Member State sets its own national agenda to achieve common EU agendas and targets. The national roadmaps will be set out in the first national roadmaps, which Member States were required to submit to the Commission in autumn 2023.[18] Member States will review and revise their national roadmaps every 2 years to inform the actions, measures and investments planned to achieve the objectives and targets.

With the advance of the digital age, the European Union has recognized that technological developments are creating new types of challenges to sovereignty and citizens' rights. The dominance of global technology companies, data protection issues, cybersecurity threats and the need to maintain media freedom and pluralism raise complex issues that require a comprehensive regulatory approach. The EU has launched a number of regulatory initiatives to respond to these challenges and to create stability and security in the digital age. Prominent among these initiatives are the attempts to regulate digital services,[19] digital markets,[20] media,[21] and artificial intelligence[22] as essential tools for achieving digital sovereignty (Eifert et al., 2021; Chiarella, 2023; Edelson et al., 2023).

The DSA is one of the EU's most important pieces of legislation aimed at creating a safer and more transparent digital environment. It regulates the operation of digital services, in particular online platforms such as social media and e-commerce sites. The DSA makes these platforms responsible for moderating content, preventing the spread of false information and protecting users. In addition, the law obliges large platforms to operate transparently, disclose the operation of their algorithms and ensure that advertising practices are regulated (Tóth, 2023; Keserű, 2024).

The DSA is a major step forward for digital sovereignty, as it increases Member States' control over online platforms. However, it also creates new challenges, as global technology companies often find it difficult to adapt to the different legal and cultural frameworks in different Member States. This is particularly true in smaller countries such as Hungary and Slovakia, where the capacity of local regulators to control large platforms may be limited.

The DMA is another key EU regulation to ensure fair competition in digital markets. The DMA Regulation aims to limit the monopolistic practices of global technology giants, in particular GAFAM. The law defines the "gatekeeper" players, the large companies that have a dominant position in the online market, and sets rules for them to prevent distortions of competition in the market.

For example, the DMA requires that gatekeeper operators must not favor their own products or services over those of other operators and must not restrict smaller firms' access to essential platforms. This regulation directly contributes to strengthening the EU's digital sovereignty by reducing the economic dominance of global companies and creating opportunities for European businesses to compete in the market. However, the implementation of the DMA also poses challenges, as strong and well-coordinated EU and national institutions are needed to ensure strict enforcement.

The EMFA is the EU's response to the challenges to media freedom and pluralism. The aim of the EMFA is to ensure the independence and transparency of editorial boards and to prevent government and economic interference in media content. It requires transparency in media ownership and financing and introduces rules to protect the decision-making independence of journalists and editors.

The EMFA is particularly important in the digital age, where the role of media is not only in traditional forms but also on digital platforms. The EMFA is directly linked to digital sovereignty, as it ensures that EU citizens have access to reliable and independent information, while reducing the control of global technology companies over media content. However, the implementation of the EMFA may give rise to controversy, especially in Member States where government actors have a significant influence on the media.

[12] COM (2021) 118 Digital Agenda 2030: A European way to deliver the Digital Decade.

[13] Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade 2030 policy programme.

[14] European Declaration on Digital Rights and Principles for the Digital Decade 2023/C 23/01. The declaration sets out to put people at the centre of the digital transition; to promote solidarity and inclusion through: connectivity, digital education, training and skills, fair and equitable working conditions and access to digital public services; to reaffirm freedom of choice and the importance of a fair digital environment; to promote participation in the digital public space; to increase safety, security and empowerment in the digital environment, especially among young people; and to promote sustainability.

[15] Commission Implementing Decision (EU) 2023/1353 of 30 June 2023 establishing the key performance indicators to measure progress towards the digital targets set out in Article 4(1) of Decision (EU) 2022/2481 of the European Parliament and of the Council.

[16] C (2023) 7,500 Setting out planned delivery pathways for digital at EU level.

[17] See https://digital-strategy.ec.europa.eu/en/library/2023-report-state-digital-decade (07-11-2024).

[18] See Hungary's National Strategic Reference Framework for the Digital Decade 2030 Policy Agenda 2030, as set out in Decision 2022/2481 of the European Parliament and of the Council (EU) of 14 December 2022. Available at: https://digital-strategy.ec.europa.eu/hu/policies/national-strategic-roadmaps (07-11-2024).

[19] See DSA.

[20] See DMA.

[21] See EMFA.

[22] See the AI Act.

The EU regulation on Artificial Intelligence (AI), the so-called AI Act, is the first comprehensive piece of legislation aimed at regulating artificial intelligence systems with the intention of ensuring technological progress, the protection of citizens' fundamental rights and the ethical use of AI. The AI Act aims to make the European Union a pioneer in the global regulation of AI, while strengthening its own digital sovereignty.

The AI Act is based on a risk-based approach, whereby AI systems are categorized according to their level of risk. This approach allows for targeted regulation, focusing on the most critical systems.[23] In particular, the AI Act emphasizes data quality, transparency, and compliance assessment to ensure that AI systems operate fairly, reliably, and safely.

The AI Act is a key element of the EU's digital sovereignty strategy in several respects. On the one hand, the AI Act allows the EU to govern the development and application of AI in its territory according to its own rules. This regulatory autonomy is particularly important for taking action against global technology companies, which tend to operate in a transnational framework. On the other hand, the AI Act ensures that AI systems used in the EU comply with EU values and legislation, in particular in the areas of privacy, security and transparency. This move confirms the EU's commitment to protecting the rights of its citizens. Third, the AI Act will support European AI development and innovation, creating opportunities for European businesses to remain competitive in the global market. This will reduce the EU's dependence on non-EU tech firms. Finally, the AI Act includes strict standards for data management, ensuring that the data used by AI systems is secure and reliable. This will directly contribute to strengthening the EU's data sovereignty.[24]

Together, the DSA, DMA and EMFA and the AI Act are the cornerstones of the EU's digital sovereignty strategy.[25] These regulations not only increase the transparency and security of digital markets and services, but also contribute to the EU's technological and economic independence. However, their implementation and effectiveness depend to a large extent on cooperation at EU and Member State level and on the resources available to enforce the rules. These measures will significantly shape the future of the digital space in the EU, while reflecting the different needs and priorities of Member States. The rules aim to strike a balance between national self-determination and cooperation at EU level, and ensure that the EU is able to maintain its sovereignty in the face of global digital challenges. This is particularly important for smaller Member States such as Hungary, Slovakia and the Czech Republic, for whom EU rules provide protection and opportunities to thrive in the digital space.

3.4 Digital sovereignty from the perspective of central and eastern European countries

The issue of digital sovereignty is of general concern within the European Union, but is particularly acute in the countries of Central and Eastern Europe. These countries, such as Hungary, the Slovak Republic, the Czech Republic and Poland, have different approaches to digital sovereignty issues due to their unique political, economic and cultural characteristics.[26] For the states in this region, nation-state sovereignty is particularly emphasized for historical reasons, while global technological challenges and the EU's common regulatory framework create a complex situation that requires a specific approach (Benyusz and Hulkó, 2021; Farkas, 2022).

The historical past of the countries of the Central and Eastern European region has a significant impact on their perception of sovereignty and their relationship with the EU. Their belonging to and subsequent liberation from the Soviet bloc has left a political legacy in which the emphasis on national sovereignty is central. These countries have long been under the rule of external powers, and the restoration and preservation of national self-determination is particularly important for them. Their accession to the EU was often accompanied by ambivalent feelings, while they sought economic and political integration, they also feared that some of their national sovereignty would again be restricted.

This historical legacy is particularly acute in the area of digital sovereignty, where the EU's common regulatory framework and the influence of global technology companies create a situation where the autonomy of nation states often comes into conflict with transnational interests. For the countries of Central and Eastern Europe (CEECs), digital sovereignty is not only a technological or economic issue, but also a means of preserving national identity and political self-determination. The economic structure and technological

[23] Unacceptable risk schemes are schemes that violate basic human rights (e.g., social scoring schemes) are completely prohibited. High-risk systems are AI systems that may have a significant impact on the lives or safety of individuals (e.g., systems used in health, education or critical infrastructure), must meet strict compliance requirements. Medium-risk systems are systems (such as chatbots for consumers) that must meet transparency requirements. Low-risk systems are those applications that carry minimal risk (e.g., entertainment AI) and are therefore subject to less stringent regulation.

[24] The importance of the AI Act goes beyond AI, as the EU is presenting a regulatory approach that focuses on promoting technological progress, protecting human rights and maintaining economic competitiveness. In this way, the AI Act will play a key role in shaping the EU's future digital ecosystem and strengthening its position in the global digital space.

[25] In addition to the regulatory framework, it is important to mention the EU's Gaia-X project. The EU's Gaia-X project is an integral part of the historical development of the European Union's digital sovereignty, as it is an initiative specifically aimed at strengthening Europe's digital infrastructure and achieving technological independence. Gaia-X aims to create an interoperable and secure cloud services ecosystem that operates in accordance with European standards and values. The importance of Gaia-X lies in the fact that it offers an alternative to non-EU based cloud services, while supporting European innovation and local entrepreneurship. In this way, the project not only serves to strengthen digital sovereignty, but also reinforces the foundations of the EU's technological and economic independence, complementing regulatory actions such as the DSA and the DMA (Braud et al., 2021; Tardieu, 2022).

[26] The research data of the chapter is based on National Digital Decade strategic roadmaps of Hungary, Slovakia, the Czech Republic and Poland. See Hungary: Magyarország Nemzeti Stratégiai Ütemterve; Slovakia: National Digital Decade Strategic Roadmap of the Slovak Republic; the Czech Republic: The Path to Europe's Digital Decade: The Strategic Plan for the Digitalization of Czechia by 2030; and Poland: Krajowy plan działania do programu polityki "Droga ku cyfrowej dekadzie" do 2030. Available at: https://digital-strategy.ec.europa.eu/en/policies/national-strategic-roadmaps (08-12-2024).

development of CEECs differ significantly from Western European countries, creating both challenges and opportunities for the realization of digital sovereignty. Countries in this region tend to have smaller economies with limited resources to develop digital infrastructure and support technological innovation. This is particularly the case in Hungary and Slovakia, where the digital switchover is mainly driven by EU funds and foreign investment.

The dominance of global technology companies in this region is particularly sensitive to the economy, as these companies often exploit their dominant market position and distort local markets. However, common EU regulatory initiatives such as the DSA and the DMA create opportunities for the region to reduce dependence on global firms and support local businesses. The EU's technological and economic support is key for CEECs, especially in developing digital infrastructure and strengthening cybersecurity capabilities.

The issue of cybersecurity and data protection is of particular importance for the countries of Central and Eastern Europe, which are often exposed to the threat of cyber-attacks and information warfare due to their geopolitical position. Countries in the region face a number of cybersecurity challenges, including attacks on critical infrastructure and the protection of citizens' personal data. The EU's common cybersecurity strategy and regulatory frameworks, such as the Cybersecurity Act, provide significant help in addressing these threats, while national governments also have an important role to play in building local defenses.

From a data protection perspective, the introduction of the GDPR has been an important step forward for Central and Eastern European countries, ensuring the protection of citizens' data and transparency in digital services. However, implementation of the regulation is often challenging for smaller countries with limited resources to enforce legal and technological requirements.

The freedom and pluralism of digital media is also a key issue in Central and Eastern European countries, particularly in view of the political and economic pressures that often threaten independent media. The EMFA can be an important tool for the region to preserve media independence, but its implementation often creates conflicts between national governments and the EU. In the case of Hungary, for example, the EU blames the government for the limited independence of the media and the strong influence of the government. The provisions of the EMFA could run counter to these practices, leading to further disputes between the EU and the Hungarian government. Other countries, such as the Czech Republic and Slovakia, also face challenges in maintaining transparency and pluralism in digital media.

The issue of digital sovereignty in Central and Eastern European countries is particularly complex, as these countries seek to both preserve nation-state sovereignty and integrate into the EU's common regulatory framework. This dichotomy often leads to tensions between EU institutions and national governments, especially in areas such as media freedom, data protection and cybersecurity.

4 Discussion

The European Union's ambition for digital sovereignty has evolved gradually over the past decades, responding to the pressures of global technological developments and transnational digital challenges. The importance of digital sovereignty lies not only in strengthening EU institutions and promoting cooperation between Member States, but also in strengthening the EU's position as a global regulatory actor. Initiatives such as the GDPR, the DSA, the DMA, the EMFA, the AI Act and the Gaia-X project form a comprehensive strategy that seeks to protect citizens' rights, maintain economic competitiveness and promote EU values at a global level.

The European Union's legislative framework, encompassing the DSA, the DMA and the AI Act, has significantly altered the operational landscape for major technology companies such as Google, Amazon, and Meta. These regulations aim to create a more equitable digital ecosystem by curbing monopolistic practices, enhancing user protection, and ensuring transparency in digital services. While these measures align with the EU's broader ambition to assert digital sovereignty, they also impose considerable compliance burdens on large tech firms, reshaping their strategies and business models within the Union.

One of the most direct impacts has stemmed from the DMA's effort to regulate the behavior of gatekeeper platforms, large tech companies that control significant portions of the online market. The DMA specifically targets practices such as self-preferencing, where companies prioritize their own products or services over those of competitors on their platforms.[27] Failure to comply with these provisions carries severe financial penalties. Under the DMA, non-compliant gatekeepers can face fines of up to 10% of their global annual turnover, with repeat offenses potentially leading to fines of up to 20%. In extreme cases, the European Commission can mandate the structural separation of business divisions, demonstrating the substantial leverage the EU wields over even the largest technology firms.

The DSA introduces stringent requirements for content moderation, user privacy, and transparency in advertising. Large platforms, including Meta's Facebook and Instagram, are obligated to proactively identify and remove illegal content, such as hate speech and misinformation, or risk fines amounting to 6% of their global turnover. Additionally, the DSA mandates algorithmic transparency, forcing companies to disclose how content is ranked and recommended to users.[28] The compliance costs associated with the DSA have led to significant operational adjustments for tech companies. These include hiring local legal and regulatory teams, redesigning user interfaces to ensure transparency, and investing heavily in AI-driven moderation tools. Smaller platforms may face challenges in meeting these requirements, but the largest corporations, such as Google and Amazon, have the resources to pivot strategically to align with EU expectations.

The AI Act marks the first comprehensive attempt to regulate artificial intelligence globally. Its risk-based classification imposes

[27] For instance, Google has been compelled to adjust its search algorithms and product display methods to ensure equal visibility for third-party services in online search results. Similarly, Amazon is now required to avoid favoring its in-house brands over external retailers in its marketplace, fostering a fairer competitive environment.

[28] A notable example involves Meta, which has restructured parts of its advertising ecosystem to comply with EU demands for greater transparency in targeted ads and algorithmic fairness. Similarly, Twitter (now X) faced scrutiny and compliance pressures under the DSA, resulting in increased investments in content moderation teams within the EU.

strict obligations on AI systems that could potentially endanger fundamental rights or safety. This has placed pressure on companies like Amazon and Google, whose AI-driven services and products (e.g., facial recognition tools, automated hiring systems) are categorized under high-risk applications. To comply, these companies must ensure robust data governance, algorithmic explain ability, and human oversight in AI systems deployed within the EU. The AI Act's requirement for data transparency and the prohibition of certain AI applications (such as social scoring systems) further restricts tech giants' operational flexibility, prompting preemptive adjustments to their product roadmaps and AI strategies.

A defining feature of these regulations, including the GDPR, DMA, and AI Act, is their extraterritorial scope. These laws apply not only to EU-based companies but also to foreign service providers that target or process data of EU citizens. This has necessitated compliance by companies worldwide, regardless of their geographical headquarters.[29] The extraterritorial reach of the DMA compels gatekeepers to apply fair market practices across all EU member states, even if the services are managed from non-EU jurisdictions. This mechanism underscores the EU's ambition to set global standards for digital governance, effectively exporting its regulatory model to influence tech policy beyond its borders.

But the EU's digital sovereignty ambitions are not without internal contradictions and challenges. The different interests and capabilities of Member States often make it difficult to develop a coherent regulatory framework. These contrasts are particularly acute in the Central and Eastern European region, where the emphasis on nation-state sovereignty and scepticism towards the EU are dominant political factors. Nevertheless, the EU's digital regulatory initiatives represent a significant step towards an orderly and sustainable transnational digital space.

There are a number of challenges in implementing the EU's digital sovereignty strategy. Large technology companies (GAFAM) wield considerable power in the global digital space. The EU's regulatory initiatives aim to reduce this dominance, but enforcing these regulations requires significant resources and comes under considerable political and economic pressure. EU Member States have different levels of economic development, political priorities and regulatory capacity. This is particularly pronounced in smaller Member States such as Hungary, Slovakia and the Czech Republic, where the development of digital infrastructure and regulatory capacity often depends on EU funding. The decentralized nature of the digital space and cross-border cyber threats make the work of nation-state regulators more difficult and require joint EU action. However, this joint action often requires political compromises that can slow down the regulatory process. A key objective of the EU's Digital Sovereignty Strategy is to support innovation and technological development in Europe. However, the EU often struggles to compete in the global marketplace against technology giants from the US and Asia.

In light of these challenges, a number of proposals can be made to further strengthen the EU's digital sovereignty strategy.

The EU needs to step up cooperation at national and EU level, in particular to strengthen regulatory capacity and allocate resources more efficiently. This is particularly important for smaller and less developed Member States, which often face challenges in implementing common EU rules. The EU should further increase its investment in digital infrastructure, in particular through initiatives such as the Gaia-X project. Developing a European cloud infrastructure not only strengthens technological independence, but also gives European businesses a competitive advantage. The EU must continue to strengthen cybersecurity and data protection regulations to protect its citizens and economy from threats in the digital space. The examples of the Cybersecurity Act and the GDPR show that these measures not only provide internal security, but also create global standards. The EU needs to increase its R&D investment in artificial intelligence, blockchain and other emerging technologies. The AI Act not only provides a regulatory framework, but can also act as a stimulus for innovation, if properly combined with funding programmes such as Horizon Europe. The EU needs to place greater emphasis on raising awareness of citizens' digital rights and opportunities. Digital sovereignty is not only an institutional issue, but also a societal process that requires the active participation and support of citizens.

The EU Digital Sovereignty Strategy is an important and timely response to global technological challenges. Achievements to date, such as the GDPR, DSA, DMA, EMFA and the AI Act, provide a strong foundation for a sustainable and ethical digital space. At the same time, the strategy must continuously adapt to the changing technological environment and the different needs of Member States.

The EU needs to find a balance between nation-state sovereignty and EU-wide cooperation to ensure the stability and security of the digital space, while supporting the rights and interests of European citizens. In doing so, the EU can not only strengthen its internal cohesion, but also become a global leader in digital regulation and governance. This strategy will not only ensure the EU's economic and technological competitiveness, but will also contribute to a more ethical and transparent digital ecosystem that can serve as a model for other regions of the world.

This paper achieved its objective by evaluating the legislative measures and their impact on digital sovereignty, highlighting the specific challenges faced by smaller member states in the process.

Data availability statement

The raw data supporting the conclusions of this article will be made available by the authors, without undue reservation.

Author contributions

GH: Writing – original draft, Writing – review & editing. JK: Writing – original draft, Writing – review & editing. AL: Writing – original draft, Writing – review & editing.

[29] For instance, U.S.-based firms such as Microsoft and Apple must align their services with EU digital laws to continue offering products within the Single Market. GDPR's heavy fines (up to 4% of global turnover) have already led to cases where Meta was fined €1.2 billion for improper data transfers to the U.S. Similarly, Amazon faced €746 million in GDPR fines for alleged privacy violations.

Funding

The author(s) declare that no financial support was received for the research, authorship, and/or publication of this article.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Generative AI statement

The authors declare that no Gen AI was used in the creation of this manuscript.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

Benyusz, M., and Hulkó, G. (2021). A közösségi médiaplatformok új szabályozásának koncepcionális alapjai Lengyelországba. *KözigazgatásTudomány* 1, 70–79. doi: 10.54200/kt.v1i1.7

Boin, A. (2008). Governing after crisis: The politics of investigation, accountability and learning. Cambridge: Cambridge University Press.

Braud, A., Fromentoux, G., Radier, B., and Le Grand, O. (2021). The road to European digital sovereignty with Gaia-X and IDSA. *IEEE Netw.* 35, 4–5. doi: 10.1109/MNET.2021.9387709

Chander, A., and Sun, H.: Sovereignty 2.0., in Georgetown law faculty publications and other works, (2021). Available at: https://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=3422&context=facpub

Chiarella, M. L. (2023). Digital markets act (DMA) and digital services act (DSA): new rules for the EU digital environment. *Athens J. Law* 9, 33–58. doi: 10.30958/ajl.9-1-2

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

Eastham, K., Coates, D., and Allodi, F. (1970). The concept of crisis. *Can. Psychiatr. Assoc. J.* 15, 463–472. doi: 10.1177/070674377001500508

Edelson, L., Graef, I., and Lancieri, F. Access to data and algorithms: For an effective DMA and DSA implementation, in Centre on regulation in Europe (CERRE), (2023). Available at: https://cerre.eu/publications/access-to-data-and-algorithms-for-an-effective-dma-and-dsa-implementation/ (Accessed June 21, 2024).

Eifert, M., Metzger, A., Schweitzer, H., and Wagner, G. (2021). Taming the giants: The DMA/DSA package. *Common Market Law Review* 58, 987–1028. doi: 10.54648/cola2021065

Falkner, G., Heidebrecht, S., Obendiek, A., and Seidl, T. (2024). Digital sovereignty - rhetoric and reality. *J. Eur. Publ. Policy* 31, 2099–2120. doi: 10.1080/13501763.2024.2358984

Farkas, B. (2022). Kapitalista átalakulás és változó geopolitikai erőtér: Kelet-Közép-Európa három évtizede. *Korunk* 3, 6–13.

Farrand, B., and Carrapico, H. (2022). Digital sovereignty and taking back control: from regulatory capitalism to regulatory mercantilism in EU cybersecurity. *Eur. Secur.* 31, 435–453. doi: 10.1080/09662839.2022.2102896

Floridi, L. (2020). The fight for digital sovereignty: what it is, and why it matters, especially for the EU. *Philos. Technol.* 33, 369–378. doi: 10.1007/s13347-020-00423-6

Hay, C. (2013). Treating the symptom not the condition: crisis definition, deficit reduction and the search for a new British growth model. *Br. J. Polit. Int. Rel.* 15, 23–37. doi: 10.1111/j.1467-856X.2012.00515.x

Hummel, P., Braun, M., Tretter, M., and Dabrock, P. (2021). Data sovereignty: a review. *Big Data Soc.* 8:12. doi: 10.1177/2053951720982012

Keserű, B. A. (2024). "A DSA és az uniós szerzői jog kapcsolata.: Részletek egy jogi kirakósból, in Koltay, András - Szikora, Tamás -" in A vadnyugat vége? Tanulmányok az Európai Unió platformszabályozásáról. ed. A. Lapsánszky (Budapest: ORAC Kiadó Kft), 88–106.

Kokas, A. (2023). Trafficking data. How China is winning the Battle for digital sovereignty. Oxford: Oxford University Press.

Lansing, R. (1914). A definition of sovereignty, in proceedings of the American Political Science Association. *Tenth Annu. Meet.* 10, 61–75. doi: 10.2307/3038417

Lapsánszky, A. (2021). Az elektronikus hírközlés gazdasági közigazgatása hazánkban. Budapest: Wolters Kluwer Hungary.

Liman, A., and Weber, K. (2023). Quantum computing: bridging the National Security–Digital Sovereignty Divide. *Eur. J. Risk Regul.* 14, 476–483. doi: 10.1017/err.2023.44

McConnell, A. "The politics of crisis terminology," Oxford research encyclopedia of politics. (2020). Available at: https://oxfordre.com/politics/view/10.1093/acrefore/9780190228637.001.0001/acrefore-9780190228637-e-1590 (Accessed December 6, 2024).

Metakides, G. (2022). "A crucial decade for European digital sovereignty" in Perspectives on digital humanism. eds. H. Werthner, E. Prem, E. A. Lee and C. Ghezzi (Berlin: Springer), 219–226.

Mueller, M. (2020). Against sovereignty in cyberspace. *Int. Stud. Rev.* 22, 779–801. doi: 10.1093/isr/viz044

Novikov, Y. (2024). Digital sovereignty: Conceptual challenges and constitutional implications. *Const. Legal Acad. Stud.* 1, 61–69. doi: 10.24144/2663-5399.2024.1.08

Philpott, D. (1995). Sovereignty: an introduction and brief history. *J. Int. Aff.* 48, 353–368.

Pohle, J., and Thiel, T. (2020). Digital sovereignty, in internet. *Pol. Rev.* 9, 1–19. doi: 10.14763/2020.4.1532

Roberts, H., Cowls, J., Casolari, F., Morley, J., Taddeo, M., and Floridi, L. (2021). Safeguarding European values with digital sovereignty: an analysis of statements and policies, in internet. *Pol. Rev.* 10, 1–26. doi: 10.14763/2021.3.1575

Rojszczak, M. (2023). The digital services act and the problem of preventive blocking of (clearly) illegal content. *Inst. Admin. J. Admin. Sci* 3, 44–59. doi: 10.54201/iajas.v3i2.85

Roumate, F. (2024). "AI and technological sovereignty" in Artificial intelligence and the New World order. Frontiers of artificial intelligence, ethics and multidisciplinary applications (Cham: Springer).

Saka, T. N., Hormiga, E., and Valls-Pasola, J. (2024). Crisis response strategies: a digital reluctance perspective. *Rev. Manag. Sci.* doi: 10.1007/s11846-024-00822-5

Schmitz, L., and Seidl, T. (2023). As open as possible, as autonomous as necessary: understanding the rise of open strategic autonomy in EU trade policy. *J. Common Mark. Stud.* 61, 834–852. doi: 10.1111/jcms.13428

Sheikh, H. (2022). European digital sovereignty: a layered approach. *Digit. Soc.* 1, 1–25. doi: 10.1007/s44206-022-00025-z

Steinbach, A. (2024). Digitale Souveränität, in List. *Forum* 50, 51–74. doi: 10.1007/s41025-023-00252-3

Suzor, N. (2018). Digital constitutionalism: Using the rule of law to evaluate the legitimacy of governance by platforms. *Soc. Media Soc.* 4:812. doi: 10.1177/2056305118787812

Tardieu, H. (2022). "Role of Gaia-X in the European data space ecosystem" in Designing data spaces. eds. B. Otto, H. M. Tan and S. Wrobel (Berlin: Springer), 41–60.

Tóth, A. (2023). A Digital Services Act és az EU fogyasztóvédelmi joga. *KözigazgatásTudomány* 3, 24–34. doi: 10.54200/kt.v3i2.67