

Cyberspace as an Emerging Regulatory Domain in European Union Law: Cybersecurity and Digital Strategic Autonomy

Lecturer Aurel - Octavian PASAT¹

Abstract

Cyberspace has evolved from a primarily technological and economic environment into a complex legal and strategic domain in which economic activity, public administration, fundamental rights, security interests, and geopolitical competition increasingly intersect. The growing dependence of the European Union and its Member States on digital infrastructures, information systems, data flows, cloud services, and emerging technologies has exposed significant vulnerabilities, particularly in relation to cyberattacks, critical infrastructure, technological dependencies, and external control over strategic digital resources. These developments have prompted the European Union to progressively construct a regulatory framework capable of addressing cyberspace as a distinct field of legal intervention. This article examines the emergence of cyberspace as a regulatory domain within European Union law. The research adopts a doctrinal and analytical methodology based on the interpretation of relevant provisions of the Treaties, secondary legislation, policy documents, and selected case law of the Court of Justice of the European Union. Particular attention is given to the legal foundations of EU action in the field of cybersecurity, the division of competences between the Union and the Member States, and the role of instruments such as the NIS and NIS 2 Directives, the Cybersecurity Act, the General Data Protection Regulation, the Digital Services Act, and the Digital Markets Act. The analysis demonstrates that, although the Treaties do not expressly recognise cyberspace as an autonomous area of competence, European Union law has gradually developed a functional and cross-sectoral regulatory approach. Cyberspace is increasingly governed at the intersection of the internal market, cybersecurity, public order, fundamental rights, and strategic resilience. This evolution also reveals a persistent tension between the need for coordinated European action and the preservation of Member States' competences in matters of national security. The article further analyses digital strategic autonomy as an emerging legal and political principle through which the European Union seeks to reduce critical technological dependencies, protect digital supply chains, secure essential infrastructures, and strengthen its normative capacity in relation to global technology actors. It argues that digital strategic autonomy is becoming a central element of the Union's collective sovereignty and resilience. Finally, the study advances several proposals de lege ferenda, including the recognition of digital strategic autonomy as a general principle of EU law, the creation of a special legal regime for digital infrastructure of strategic European interest, and the development of a European right to digital continuity. The article concludes that cyberspace should be expressly and coherently integrated into the contemporary legal architecture of the European Union in order to ensure security, competitiveness, institutional resilience, and the effective protection of fundamental rights.

Keywords: *cyberspace; cybersecurity; European Union law; digital strategic autonomy; digital sovereignty; critical infrastructure; fundamental rights; EU competences.*

JEL Classification: K23, K24

¹ Aurel-Octavian Pasat - Cross-Border Faculty, "Dunărea de Jos" University of Galați, Romania, <https://orcid.org/0000-0002-7239-0808>, Aurel.Pasat@ugal.ro.

DOI: 10.62768/PLPA/2026/15/2/08

Please cite this article as: Pasat, Aurel-Octavian, „Cyberspace as an Emerging Regulatory Domain in European Union Law: Cybersecurity and Digital Strategic Autonomy”, <i>Perspectives of Law and Public Administration</i> 15, no. 2 (June 2026): 309-320.	Article History Received: 17 January 2026 Revised: 19 April 2026 Accepted: 07 May 2026
---	--

1. Introduction

The accelerated digitalisation of European society has led to a profound structural transformation of the European Union's economic, administrative and security architecture. Economic processes are increasingly dependent on digital infrastructure; public administration makes extensive use of IT systems and decision-making algorithms; and the security of Member States is closely linked to the resilience of networks and information systems. In this context, cyberspace has moved beyond its status as a mere technological medium to become a genuine arena for the exercise of power, conflict and legal normativity.

The cross-border nature of cyberspace blurs traditional territorial boundaries and gives rise to systemic risks that are difficult to manage exclusively at national level. Attacks on critical infrastructure, information manipulation, the exploitation of digital vulnerabilities and the use of artificial intelligence for hostile purposes reveal the limitations of the traditional paradigm of state sovereignty. Consequently, the protection of the essential interests of the Member States and the Union requires a coordinated approach capable of responding to emerging threats in an interconnected digital environment.

Although the Treaties do not expressly recognise cyberspace as an autonomous area of competence, developments in secondary legislation demonstrate an implicit recognition of it as a distinct subject of regulation. EU law has moved beyond a strictly economic approach to digitalisation by incorporating aspects of security, the protection of fundamental rights and systemic stability.

2. The Conceptualisation of Cyberspace in European Union Law

2.1. From Technological Infrastructure to Legal Space

Initially, cyberspace was viewed in European Union law almost exclusively as a functional technological tool designed to achieve the objectives of the internal market and to consolidate the information society. The first European policies and regulatory measures focused on the development of electronic communications infrastructure, the liberalisation of digital markets and the facilitation of e-commerce, following a primarily economic rationale. Cyberspace was thus conceived as a legally neutral environment, devoid of any normative significance of its own, and treated

merely as a vehicle for existing economic and social relations.

This instrumental approach has also been supported by Romanian legal scholarship, which has demonstrated that, in the early stages of European regulation, EU law avoided an autonomous conceptualisation of cyberspace, preferring instead to integrate it into the broader concept of the information society. Within this paradigm, regulatory intervention was aimed exclusively at removing barriers to the free movement of digital services and goods, without taking into account the implications for security, sovereignty or public order. However, the rapid evolution of digital technologies and the emergence of complex cyber-risks have led to a profound reconfiguration of the legal framework governing cyberspace. Cyber-attacks against critical infrastructure, the use of digital networks for criminal or terrorist purposes, and the mass exploitation of personal data have highlighted the vulnerability of this space. Consequently, European Union law has gradually incorporated dimensions such as cybersecurity, the protection of fundamental rights and the maintenance of public order, thereby moving beyond the initial, strictly economic paradigm. As the researchers analyse in *Cybersecurity, European digital sovereignty and the 5G rollout crisis*, the security measures adopted for the roll-out of 5G infrastructure have ‘played a significant role in reshaping EU cybersecurity policies aimed at achieving digital sovereignty’, thereby reflecting the European Union’s ambition to protect its strategic interests and strengthen its normative capacity in the field of cybersecurity governance².

Romanian legal doctrine emphasises that this shift in perspective reflects a normative maturation of EU law, which recognises cyberspace as a systemic risk factor, that has a direct impact on the security of Member States and of the Union as a whole³. Thus, cyberspace becomes a legitimate subject of legal intervention, and its regulation can no longer be justified solely on grounds of economic efficiency, but must also be based on the need to protect the European public interest.

It is important to note that European Union law does not currently provide for a single legal definition of cyberspace; this should not be interpreted as a regulatory gap, but rather as a deliberate choice, determined by the dynamic and evolving nature of the phenomenon. An analysis of European legislation nevertheless reveals an implicit recognition of cyberspace as a complex cross-border environment, comprising communication networks, IT systems, data, digital platforms and users, characterised by a high degree of interdependence and vulnerability. The absence of a single definition reflects the difficulty of adapting traditional legal concepts – territory, jurisdiction, competence – to the realities of the digital space. As Fahey (2024) points out, „neither the EU’s cybersecurity strategy nor the US national strategy for cyberspace explicitly defines the term “cybersecurity”, although both refer to it regularly. This lack of a clear conceptual framework highlights the ongoing challenge

² Berna Akcali Gur, “Cybersecurity, European Digital Sovereignty and the 5G Rollout Crisis,” *Computer Law & Security Review* 46 (2022): 105736, <https://doi.org/10.1016/j.clsr.2022.105736>.

³ Victor Stoica, “Three Pillars of Due Diligence and the European Union Cyber Security Legal Framework,” *Romanian Journal of International Law*, no. 32 (2025): 96–119, <https://rrdi.ro/2025/01/01/three-pillars-of-due-diligence-and-the-european-union-cyber-security-legal-framework/>.

of establishing a unified legal understanding of cyber domains and the associated regulatory responsibilities under international and regional law”⁴. This observation highlights the difficulty of creating a unified legal understanding of cyberspace, whilst justifying the development of a coherent European legal framework to address the systemic risks associated with cyberattacks, the disruption of essential services or the manipulation of information.

Consequently, even in the absence of formal recognition, European Union law regards cyberspace as an emerging legal sphere, situated at the intersection of the internal market, security and the protection of fundamental rights. This development confirms the trend towards recognising cyberspace not only as a technological infrastructure, but also as an autonomous regulatory domain, with direct implications for the sovereignty of Member States, the division of competences and the constitutional architecture of the European Union.

2.2. Cyberspace and the EU Legal Order

The integration of cyberspace into the legal order of the European Union has not been achieved through an ontological or formal definition, but through an essentially functional and normative approach. The European Union regards the digital space as a means through which existing legal relationships are manifested, subjecting it to the same fundamental values and objectives of European integration, adapted to contemporary technological realities. This approach reflects a gradual evolution, through which EU law has extended the applicability of its rules beyond the traditional physical space, without, however, creating a separate, autonomous legal category for cyberspace.

Regulations such as Regulation (EU) 2016/679 on the protection of personal data (GDPR), Regulation (EU) 2022/2065 on digital services (Digital Services Act – DSA) and Regulation (EU) 2022/1925 on digital markets (Digital Markets Act – DMA) eloquently illustrate this regulatory integration. These legal instruments are not limited to regulating digital technologies as such, but enshrine the digital space as a framework for the exercise of fundamental rights, such as the right to privacy, data protection, freedom of expression and the freedom to conduct a business⁵. Cyberspace thus becomes a key vehicle for the realisation of the internal market and the protection of the fundamental interests of EU citizens.

⁴ Elaine Fahey, “The Evolution of EU–US Cybersecurity Law and Policy: On Drivers of Convergence,” *Journal of European Integration* 46, no. 7 (2024): 1073–1088, <https://doi.org/10.1080/07036337.2024.2411240>.

⁵ Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 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), 2016 O.J. (L 119) 1; Regulation (EU) 2022/2065 of the European Parliament and of the Council of October 19, 2022, on a Single Market for Digital Services and Amending Directive 2000/31/EC (Digital Services Act), 2022 O.J. (L 277) 1; Regulation (EU) 2022/1925 of the European Parliament and of the Council of September 14, 2022, on Contestable and Fair Markets in the Digital Sector and Amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), 2022 O.J. (L 265) 1.

In particular, the GDPR marks a paradigm shift by enshrining the principle of extraterritorial applicability of European rules based on the effects produced on data subjects located within the territory of the Union. This approach confirms that cyberspace is regulated not according to the location of the technical infrastructure, but according to the legal and social impact of digital activities. Similarly, the Digital Markets Act (DMA) and the Digital Services Act (DSA) set out clear obligations for digital service providers and online platforms, reinforcing the idea that the digital environment is not an ‘unregulated space’, but a domain subject to the requirements of the rule of law and the market economy⁶.

The case law of the Court of Justice of the European Union has played a decisive role in reinforcing this approach. The Court has consistently recognised that activities carried out in the online environment can produce relevant legal effects within the EU legal order, justifying the application of EU law even in the absence of a physical presence on the territory of the Member States⁷. Through judgments such as *Google Spain*, *Schrems I* and *Schrems II*, the CJEU has emphasised the need for effective protection of fundamental rights in the digital sphere, reaffirming the autonomy and primacy of EU law in the face of the challenges posed by the globalisation of data flows⁸.

In this context, cyberspace is integrated into the Union’s legal order not as a separate territory, but as a functional dimension of the exercise of the Union’s competences and the achievement of its fundamental objectives. This approach confirms the normative maturation of EU law, which is successfully adapting traditional legal concepts to digital realities, whilst preserving the coherence of the European legal system and the protection of its fundamental values.

3. The European Union’s Competences in the Field of Cybersecurity

Legal Basis for EU Action. Cybersecurity does not fall expressly within the exclusive competence of the Union. Its action is based on shared or complementary competences, in particular under:

- Article 4 of the TFEU (internal market),
- Article 114 of the TFEU (harmonisation of legislation),
- Article 196 of the TFEU (civil protection),
- Article 222 of the TFEU (solidarity clause).

This legal framework explains the fragmented yet evolving nature of cybersecurity regulation.

⁶ Maria Luisa Chiarella, “Digital Markets Act (DMA) and Digital Services Act (DSA): New Rules for the EU Digital Environment,” *Athens Journal of Law* 9, no. 1 (2023): 33–58, <https://doi.org/10.30958/ajl.9-1-2>.

⁷ Case C-131/12, *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, Judgment of the Court (Grand Chamber) of May 13, 2014, ECLI:EU:C:2014:317, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62012CJ0131>.

⁸ Case C-311/18, *Data Protection Commissioner v. Facebook Ireland Ltd and Maximilian Schrems*, Judgment of the Court (Grand Chamber) of July 16, 2020, ECLI:EU:C:2020:559, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62018CJ0311>.

Relevant Legal Instruments. The adoption of the NIS Directive, followed by the NIS 2 Directive, marks an important step in the development of the regulatory framework. These instruments impose clear obligations on operators of essential services and significant entities, thereby strengthening cooperation between Member States.

The Cybersecurity Regulation also strengthens the role of the European Union Agency for Cybersecurity (ENISA) and establishes a European certification framework.

Limits on the EU's Powers. Although the EU's role is growing, national security remains an exclusive competence of the Member States. This limitation creates tensions between the need for coordinated action at European level and respect for state sovereignty, particularly in the context of cyber-attacks with military or intelligence implications.

4. Digital Strategic Autonomy and Cyberspace

4.1. The Concept of Digital Strategic Autonomy

It is important to note that European Union law does not currently provide for a single legal definition of cyberspace, which reflects the difficulty of adapting traditional concepts – territory, jurisdiction, competence – to digital realities.

Digital strategic autonomy is a key concept for the EU, referring to its ability to control its critical infrastructure, technology supply chains and data flows, in order to reduce its external dependence on global technology powers. At the same time, digital sovereignty remains a contested and multidimensional concept, encompassing state autonomy, economic self-determination and the capacity of individuals to exercise control over digital technologies and data.⁹

As highlighted by the Council of the European Union in its *Conclusions on EU Digital Diplomacy* (26 June 2023): The Council emphasises the need for stronger, more strategic, coherent and effective EU policy and action in global digital affairs in order to reaffirm the EU's commitment and leadership. This is essential for strengthening the EU's strategic autonomy whilst preserving an open economy. Thus, even without a unified legal definition of cyberspace, the EU is taking action to secure its infrastructure and guarantee its strategic digital autonomy¹⁰.

This concept emerged in response to the vulnerabilities revealed by global technological competition, as well as to the risks associated with external surveillance and control of sensitive infrastructure, which could affect the security and sovereignty of the Union.

Digital strategic autonomy reflects, in particular, a paradigm shift in the way the Union perceives its role on the international stage. It marks a transition from mere

⁹ Julia Pohle and Thorsten Thiel, "Digital Sovereignty," Internet Policy Review 9, no. 4 (2020), <https://doi.org/10.14763/2020.4.1532>.

¹⁰ Council of the European Union, *Council Conclusions on EU Digital Diplomacy*, Council doc. 11088/23 (June 26, 2023), <https://data.consilium.europa.eu/doc/document/ST-11088-2023-INIT/en/pdf>.

integration into global digital production and service chains to a drive for mastery and independence in strategic areas, such as data infrastructure, artificial intelligence and emerging technologies. As recent research indicates, the concept of strategic digital autonomy rests on the European Union's ability to reduce its dependence on foreign technologies and to strengthen its own technological capabilities, which has become a priority in the face of geopolitical pressures and global competition in key digital sectors¹¹. In a world characterised by growing geopolitical tensions and technological rivalry, this autonomy is becoming an essential element for ensuring stability, strengthening the competitiveness of the European economy and protecting the EU's democratic values.

4.2. The Legal Dimension of Digital Autonomy

Strategic autonomy encompasses the European Union's normative power vis-à-vis other states and major (foreign) technology companies; ... as well as the EU's capacity to decide and act on the essential aspects of its long-term future in the economy and society¹². Thus, this conception of strategic autonomy – understood as the European Union's normative capacity to act vis-à-vis third countries and major technology companies – is given concrete form, in particular, through the adoption of sector-specific legal instruments designed to protect its infrastructure and regulate external technological dependencies.

A relevant example is the regulation on the security of 5G networks. Directive (EU) 2019/713 on security measures for 5G networks and services imposes strict obligations on infrastructure providers to prevent security risks associated with the use of equipment originating from states or entities considered to be vulnerable¹³. This directive reflects a concerted legal effort to control supply chains and reduce potential entry points for intrusions into critical infrastructure.

At the same time, the development of European capabilities in areas such as cloud computing, semiconductors and artificial intelligence is supported by specific programmes and regulations, designed to ensure the Union's technological competitiveness and reduce its external dependence. Technological sovereignty should not, however, be equated with technological autarky. It primarily concerns the capacity to preserve strategic options, maintain access to critical technologies and manage external dependencies according to the risks that they create for security, economic resilience and political autonomy.¹⁴

¹¹ Gerda Falkner, Sebastian Heidebrecht, Anke Obendiek, and Timo Seidl. 2024. "Digital Sovereignty - Rhetoric and Reality." *Journal of European Public Policy* 31 (8): 2099–2120, <https://doi.org/10.1080/13501763.2024.2358984>.

¹² Arlette Meiring, Svetlana Yakovleva, Kristina Irion, Joris van Hoboken, and Mireille van Eechoud, *Information Law and the Digital Transformation of the University: Part I. Digital Sovereignty* (Amsterdam: Institute for Information Law, University of Amsterdam, 2023), <https://www.ivir.nl/publicaties/download/part-i-digital-sovereignty-1.pdf>.

¹³ Commission Recommendation (EU) 2019/534 of March 26, 2019, Cybersecurity of 5G Networks, 2019 O.J. (L 88) 42, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019H0534>.

¹⁴ Jakob Edler, Knut Blind, Henning Kroll, and Torben Schubert, "Technology Sovereignty as an

The European Cloud Strategy and initiatives such as GAIA-X provide a framework for the development of interoperable and secure cloud infrastructures under European control, whilst legislation on artificial intelligence aims to create a safe and ethical digital space that protects fundamental rights.

The control of data flows and foreign investment is another key legal aspect of digital autonomy. The regulation on the screening of foreign direct investment in the EU enables Member States to monitor and block investments that could jeopardise the security or essential interests of the Union¹⁵. At the same time, the regulation on data protection (GDPR) and cross-border data flows aims to ensure a balance between the free movement of data and the protection of digital sovereignty. Developments in cybersecurity law within the European Union illustrate both significant progress and persistent challenges. Despite the proliferation of legislative instruments, there is regulatory complexity and a lack of a fully coherent legal framework, which makes it difficult to fully recognise a fundamental right to cybersecurity under EU law¹⁶.

These legal initiatives demonstrate that cyberspace has become an area in which the Union is asserting its regulatory sovereignty by establishing a legal framework capable of guaranteeing security, competitiveness and respect for fundamental rights in the digital age. Within EU policy discourse, digital sovereignty is operationalised through several mutually reinforcing fields, particularly data governance, the regulation of platform power, digital infrastructure, emerging technologies and cybersecurity.¹⁷

4.3. Implications for the European Legal Order

The strengthening of digital strategic autonomy is leading to a reconfiguration of the traditional balance between economic freedom and security requirements in European Union law. The shift from a primarily economic perspective to a strategic one reflects the evolving role of EU law, which is incorporating national security and geopolitical priorities into the regulation of the internal market and the digital space.

This reconfiguration is reflected in the adoption of regulations and policies that place greater emphasis on protecting the Union's fundamental values – democracy, fundamental rights and security – whilst promoting innovation and economic competitiveness¹⁸.

Emerging Frame for Innovation Policy: Defining Rationales, Ends and Means,” *Research Policy* 52, no. 6 (2023): 104765, <https://doi.org/10.1016/j.respol.2023.104765>.

¹⁵ Regulation (EU) 2019/452 of the European Parliament and of the Council of March 19, 2019, Establishing a Framework for the Screening of Foreign Direct Investments into the Union, 2019 O.J. (L 79 I) 1, <https://eur-lex.europa.eu/eli/reg/2019/452/oj/eng>.

¹⁶ Vagelis Papakonstantinou, “Cybersecurity as Praxis and as a State: The EU Law Path towards Acknowledgement of a New Right to Cybersecurity?,” *Computer Law & Security Review* 44 (2022): 105653, <https://doi.org/10.1016/j.clsr.2022.105653>.

¹⁷ Huw Roberts, Josh Cows, Federico Casolari, Jessica Morley, Mariarosaria Taddeo, and Luciano Floridi, “Safeguarding European Values with Digital Sovereignty: An Analysis of Statements and Policies,” *Internet Policy Review* 10, no. 3 (2021), <https://doi.org/10.14763/2021.3.1575>.

¹⁸ European Parliament, “Digital Transformation,” *Conference on the Future of Europe: Key Proposals*

This development confirms that EU law is now structured around the protection of its essential interests in the face of external technological dependencies. As Alain Strowel points out, the EU's recent digital policies reflect a desire for European autonomy or sovereignty, whilst being shaped by the constraints of the globalisation of supply chains and by the influence of powerful technological actors based outside the Union¹⁹. Consequently, cyberspace emerges as a key vehicle for European sovereignty and resilience, insofar as the regulation of data, cybersecurity and digital infrastructure is becoming a central instrument for protecting the Union's strategic interests.

This paradigm shift raises complex legal challenges, such as the harmonisation of security rules with economic freedoms and fundamental rights, coordination between Member States and EU institutions, and rapid adaptation to the accelerating pace of technological change. As legal scholarship highlights, the complexity and growing autonomy of emerging digital technologies pose significant challenges in terms of predictability and legal compliance within the European Union's regulatory framework²⁰.

In this context, strategic digital autonomy is becoming a unifying concept, guiding the Union's legislative and strategic efforts towards the creation of a robust legal framework capable of ensuring the sustainable and secure development of the European digital space.

5. Proposals for Future Legislation on Digital Strategic Autonomy and Cyberspace

Establishing the principle of strategic digital autonomy as a general principle of European Union law. A proposal *de lege ferenda* could aim to expressly enshrine strategic digital autonomy as a legal principle of the European Union, with a cross-cutting scope, similar to the precautionary principle or energy security.

This principle would oblige the European legislator and the Member States, when drafting and implementing rules relating to the digital market, cybersecurity, investment and public procurement, to assess the impact on the EU's ability to function independently of external infrastructure, technologies and suppliers.

Establishment of a special legal framework for digital infrastructure of strategic European interest. *De lege ferenda* could introduce a new legal category: digital infrastructure of strategic European interest (INISE), including:

and Related Work by Parliament, May 2, 2022, <https://www.europarl.europa.eu/news/en/press-room/20220502BKG28407/conference-on-the-future-of-europe-key-proposals-and-related-work-by-parliament/5/digital-transformation>.

¹⁹ Alain Strowel, "Souveraineté européenne dans le numérique : une visée d'autonomie dans un monde de dépendances" [European Sovereignty in the Digital Sphere: Striving for Autonomy in a World of Dependencies], *Revue internationale de droit économique* 37, no. 3 (2023): 55–70, <https://doi.org/10.3917/ride.373.0055>.

²⁰ Claudio Novelli, Federico Casolari, Philipp Hacker, Giorgio Spedicato, and Luciano Floridi, "Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity," *Computer Law & Security Review* 55 (November 2024): 106066, <https://doi.org/10.1016/j.clsr.2024.106066>.

- government data centres,
- critical communications networks,
- public digital platforms.

A strict derogatory regime would apply to them: a majority European shareholding, a ban on outsourcing, ongoing audits and the exclusive competence of the European Union.

Establishment of a European right to digital continuity. An innovative proposal would be to recognise a right of the Union and the Member States to digital continuity, enabling:

- the temporary takeover of essential digital services,
- the suspension of licences held by foreign providers in the event of a geopolitical crisis or a cyberattack,
- guaranteed access to source code and data in exceptional circumstances.

5. Conclusions

Cyberspace has undergone rapid development in recent decades, establishing itself as a fully-fledged regulatory domain within European Union law, characterised by a cross-cutting, multidisciplinary and dynamic approach. This transformation reflects the need to adapt legal rules to the realities of a complex digital environment, where traditional legal boundaries, such as territorial or sovereignty boundaries, prove insufficient to meet current challenges. Although the principle of the delegation of powers sets clear limits on the EU's competences, requiring the Union to act solely within the framework of the powers delegated to it by the Member States, recent legislative and political developments show a clear trend towards extending and strengthening the Union's role in the field of cybersecurity.

The EU has thus moved from a reactive to a proactive stance, adopting ambitious regulations and strategic initiatives aimed at ensuring the protection of critical digital infrastructure and managing emerging risks in the digital sphere.

In this context, the concept of digital strategic autonomy is of central importance in shaping the future of European law. It is no longer limited to the expression of national sovereignty or economic integration, but is becoming a fundamental principle that redefines the relationship between sovereignty, security and European integration. Digital strategic autonomy entails the Union's ability to control its own digital infrastructure, to manage data flows independently and to protect its interests against external influences. This autonomy is not limited to technical or economic aspects, but has a profound legal and political dimension, aimed at strengthening a resilient and secure European digital order that is consistent with the Union's fundamental values.

Consequently, cyberspace transcends its traditional role as a mere technological environment to become a genuine legal space within the European Union. This implies recognition that European legal rules and principles must govern the activities and relationships taking place within it, with direct legal effects on Member States, citizens and economic operators. Within this legal space, digital

strategic autonomy becomes an essential pillar of the Union's collective sovereignty, highlighting the importance of a robust regulatory framework capable of guaranteeing security, the protection of fundamental rights and competitiveness in the digital age.

Thus, EU law can no longer be conceived without coherently and explicitly incorporating the cyber dimension, which is becoming an integral part of the contemporary European legal architecture.

Bibliography

1. Akcali Gur, Berna. "Cybersecurity, European Digital Sovereignty and the 5G Rollout Crisis." *Computer Law & Security Review* 46 (2022): 105736. <https://doi.org/10.1016/j.clsr.2022.105736>.
2. Chiarella, Maria Luisa. "Digital Markets Act (DMA) and Digital Services Act (DSA): New Rules for the EU Digital Environment." *Athens Journal of Law* 9, no. 1 (2023): 33–58. <https://doi.org/10.30958/ajl.9-1-2>.
3. Commission Recommendation (EU) 2019/534 of March 26, 2019, Cybersecurity of 5G Networks. 2019 O.J. (L 88) 42. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019H0534>.
4. Council of the European Union. *Council Conclusions on EU Digital Diplomacy*. Council doc. 11088/23. June 26, 2023. <https://data.consilium.europa.eu/doc/document/ST-11088-2023-INIT/en/pdf>.
5. Edler, Jakob, Knut Blind, Henning Kroll, and Torben Schubert, "Technology Sovereignty as an Emerging Frame for Innovation Policy: Defining Rationales, Ends and Means," *Research Policy* 52, no. 6 (2023): 104765, <https://doi.org/10.1016/j.respol.2023.104765>.
6. European Parliament. "Digital Transformation." *Conference on the Future of Europe: Key Proposals and Related Work by Parliament*. May 2, 2022. <https://www.europarl.europa.eu/news/en/press-room/20220502BKG28407/conference-on-the-future-of-europe-key-proposals-and-related-work-by-parliament/5/digital-transformation>.
7. Fahey, Elaine. "The Evolution of EU–US Cybersecurity Law and Policy: On Drivers of Convergence." *Journal of European Integration* 46, no. 7 (2024): 1073–1088. <https://doi.org/10.1080/07036337.2024.2411240>.
8. Falkner, Gerda, Sebastian Heidebrecht, Anke Obendiek, and Timo Seidl. "Digital Sovereignty—Rhetoric and Reality." *Journal of European Public Policy* 31, no. 8 (2024): 2099–2120. <https://doi.org/10.1080/13501763.2024.2358984>.
9. Meiring, Arlette, Svetlana Yakovleva, Kristina Irion, Joris van Hoboken, and Mireille van Eechoud. *Information Law and the Digital Transformation of the University: Part I. Digital Sovereignty*. Amsterdam: Institute for Information Law, University of Amsterdam, 2023. <https://www.ivir.nl/publicaties/download/part-i-digital-sovereignty-1.pdf>.
10. Novelli, Claudio, Federico Casolari, Philipp Hacker, Giorgio Spedicato, and Luciano Floridi. "Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity." *Computer Law & Security Review* 55 (November 2024): 106066. <https://doi.org/10.1016/j.clsr.2024.106066>.
11. Papakonstantinou, Vagelis. "Cybersecurity as Praxis and as a State: The EU Law Path towards Acknowledgement of a New Right to Cybersecurity?" *Computer Law & Security Review* 44 (2022): 105653. <https://doi.org/10.1016/j.clsr.2022.105653>.
12. Pohle, Julia and Thorsten Thiel, "Digital Sovereignty," *Internet Policy Review* 9, no.

- 4 (2020), <https://doi.org/10.14763/2020.4.1532>.
13. Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 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). 2016 O.J. (L 119) 1.
14. Regulation (EU) 2019/452 of the European Parliament and of the Council of March 19, 2019, Establishing a Framework for the Screening of Foreign Direct Investments into the Union. 2019 O.J. (L 79 I) 1. <https://eur-lex.europa.eu/eli/reg/2019/452/oj/eng>.
15. Regulation (EU) 2022/1925 of the European Parliament and of the Council of September 14, 2022, on Contestable and Fair Markets in the Digital Sector and Amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act). 2022 O.J. (L 265) 1.
16. Regulation (EU) 2022/2065 of the European Parliament and of the Council of October 19, 2022, on a Single Market for Digital Services and Amending Directive 2000/31/EC (Digital Services Act). 2022 O.J. (L 277) 1.
17. Roberts, Huw, Josh Cowls, Federico Casolari, Jessica Morley, Mariarosaria Taddeo, and Luciano Floridi, "Safeguarding European Values with Digital Sovereignty: An Analysis of Statements and Policies," *Internet Policy Review* 10, no. 3 (2021), <https://doi.org/10.14763/2021.3.1575>.
18. Stoica, Victor. "Three Pillars of Due Diligence and the European Union Cyber Security Legal Framework." *Romanian Journal of International Law*, no. 32 (2025): 96–119. <https://rrdi.ro/2025/01/01/three-pillars-of-due-diligence-and-the-european-union-cyber-security-legal-framework/>.
19. Strowel, Alain. "Souveraineté européenne dans le numérique : une visée d'autonomie dans un monde de dépendances" [European Sovereignty in the Digital Sphere: Striving for Autonomy in a World of Dependencies]. *Revue internationale de droit économique* 37, no. 3 (2023): 55–70. <https://doi.org/10.3917/ride.373.0055>.