Ius et Securitas 2/2026 | ISSN 3071-799X

Christophe Gaie
University Jean Moulin Lyon III (France)
ORCID: 0000-0002-8252-5278
christophe.gaie@gmail.com

Mirosław Karpiuk
University of Warmia and Mazury in Olsztyn (Poland)
ORCID: 0000-0001-7012-8999
miroslaw.karpiuk@uwm.edu.pl

Jean Langlois-Berthelot
Center for Advanced Military Training (France)
ORCID: 0009-0001-2397-5930
jeanlanglois4@gmail.com

Digital Transformation in the European Union

Abstract

Digital transformation is a phenomenon that affects not only individual countries but also the European Union. In the age of developing new technologies, it can even be argued that it is inevitable worldwide. In fact, the implementation of digital tools in various spheres of life cannot proceed unchecked. Above all, legislators should ensure that violations that may not only undermine the privacy of individuals, but also generate significant damage to states, do not occur.

In the context of digital transformation, it is crucial to prepare society for new challenges, which may require significant changes and a responsible approach to phenomena occurring in the digital world. On the one hand, we are dealing with an alluring virtual world that provides entertainment, streamlines, and accelerates the performance of many tasks. On the other hand, we face threats never before encountered. Therefore, cyberspace should be used with caution to avoid cyberattacks.

The aim of this article is to analyse the digital transformation taking place in the European Union, including the principles underpinning it. The article uses a dogmatic-legal approach to analyse the legal provisions determining the digitalisation process taking place in the EU. A theoretical-legal approach is also employed, referencing the views of legal scholars. A review of the literature clarified the key issues related to digital transformation.

Keywords: new technologies, digital transformation, cybersecurity, artificial intelligence.

Introduction

The Digital European Union is a concept for the development of the European Union that assumes the introduction of digital technologies in all areas of its activity, while respecting the principles and values that underpin its functioning, while taking into account sovereignty, solidarity, and sustainable development. Building a digital European Union is linked to digital transformation, which emphasises increasing digital literacy, cybersecurity, public electronic services, and systemic changes to the entire economy based on new technologies. Digital transformation not only forces a transition to digital technologies in the public sector and the economy, but also promotes the development of a digital society and shapes the demand for digital technologies. Building European society's trust in digital technologies is also crucial, as they significantly facilitate not only the performance of public tasks and business activities, but also everyday life. To optimally implement the digital transformation in the European Union, it is necessary to work to improve the digital environment of EU citizens, taking into account human rights and freedoms. Europe's digital future is a future in which the level of digital exclusion is very low, there is universal access to innovative digital solutions, and digital life is simple, safe, and ethical.

The aim of this article is to define the principles that should guide the European Union in implementing digital solutions. The research methods used include the dogmatic legal method, the theoretical-legal method, and analysis and synthesis. These methods served to characterise the digital transformation in the European Union.

Digital European Union

The ongoing digital transformation requires the participation of many entities, both in the public and private spheres, including the implementation of appropriate policies. It is also important to note that the processes that take place within this digital transformation are also determined by international conditions, so appropriate changes in this area cannot be implemented in isola-

tion from international policy. Digital transformation must take into account not only the current status of individuals in society but also their development and the possibility of more effective handling of their affairs, including by public administration. It cannot proceed in isolation from their needs, which should be increasingly better met. This is supported, among other things, by the implementation of new technologies in the public sector, enabling more efficient service delivery and faster communication with beneficiaries[1].

In the European Union's digital transformation, people are paramount, and technology should therefore serve and benefit all people living in the EU and enable them to safely pursue their aspirations while respecting their fundamental rights. This highlights the need to: 1) strengthen democratic mechanisms in implementing the digital transformation, which benefits EU residents and improves their quality of life; 2) introduce the necessary measures to ensure respect for EU-recognised values and individual rights online; 3) support and ensure appropriate (responsible) action by all actors, public and private, in the digital environment; and 4) actively promote the vision of a responsible digital transformation, including in international relations. The EU also emphasises solidarity and social inclusion. Therefore, technology should be used to connect people, not divide them. Digital transformation should foster a just and inclusive society and a fair economy in the EU. To achieve this goal, we must: 1) ensure that the design, development, implementation, and use of technological solutions respect fundamental rights, enable their enjoyment, and promote solidarity and social inclusion; 2) promote a digital transformation that leaves no one behind. It should benefit all, ensure gender equality, and, in particular, include older people, people living in rural areas, people with disabilities, and marginalised and vulnerable people; 3) implement solutions so that all economic actors benefiting from the digital transformation assume their social responsibility and contribute fairly and proportionately to the costs of public goods, services, and infrastructure, to the benefit of all people living in Europe[2].

A properly executed digital transformation must consider issues related to the safe use of digital tools. It requires the reorganisation of many struc-

[1] C. Gaie, M. Karpiuk, A. Spaziani, *New Technologies in Public Administration*, "Ius et Securitas" 2024, No. 2, p. 50.

[2] Chapters I and II of the European Declaration of Digital Rights and Principles in the Digital Decade (OJ 2023, C 23/01).

tures and even a change in thinking. It is not just about implementing new technologies, but also about building society's resilience to cyber threats. Therefore, education that raises awareness not only of the benefits of implementing digital transformation's postulates, but also of the threats it can generate is crucial. Investing in modern digital tools must also be accompanied by an investment in their safe use, which also requires the costs associated with protecting against unauthorised interference. Cybersecurity will therefore also be crucial in digital transformation.

With the rapid digital transformation, networks and information systems have become a crucial part of everyday life. This change has led to an evolving cyber threat landscape, bringing new challenges that require adapted, coordinated, and innovative responses across all EU member states[3].

Cybersecurity, defined as the actions necessary to protect networks and information systems, their users and other individuals from cyber threats[4], must play a special role in digital transformation. Cybersecurity is a part of the national security system and is a set of policies, procedures, and technologies used to protect information and information systems from unauthorised access, use, modification, destruction, or loss. It encompasses both physical and technological safeguards[5].

---

[3] Recital 3 of Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 concerning measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (OJ 2022, L 333/80). For an analysis of the provisions of the NIS 2 Directive, see: C. Gaie, M. Mueck, *Introduction to the Networks and Information Systems 2 (NIS2) Directive*, [in:] *European Digital Regulations*, M. Mueck, C. Gaie [eds.], Cham 2025, pp. 161-178; E. Chronowska-Sioła, *Unijna dyrektywa NIS 2 w obszarze cyberbezpieczeństwa – analiza podmiotów kluczowych i podmiotów ważnych*, "Cybersecurity and Law" 2025, No. 2, pp. 14-26.

[4] Article 2(1) of Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (European Union Agency for Cybersecurity) and cybersecurity certification in information and communication technologies and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ 2019, L 151/15). On the essence of cybersecurity, see: K. Kaczmarek, *Finland in the light of cyber threats in the context of Russia's aggression against Ukraine*, "Cybersecurity and Law" 2023, No. 1, p. 212; E.M. Włodyka, K. Kaczmarek, *Cyber Security of Electrical Grids – A Contribution to Research*, "Cybersecurity and Law" 2024, No. 2, p. 262-263; K. Chałubińska-Jentkiewicz, *Cyberbezpieczeństwo*, [in:] *Leksykon cyberbezpieczeństwa*, K. Chałubińska-Jentkiewicz [ed.], Warszawa 2024, p. 53-63; K. Kaczmarek, *Nordic countries in the face of digital threats*, "Cybersecurity and Law" 2024, No. 1, p. 152.

[5] E.M. Włodyka, *Cyberbezpieczeństwo sektora publicznego*, [in:] *Leksykon*..., p. 66-67.

Digital transformation, both globally and in Europe and in individual countries, seems unlikely to proceed smoothly without artificial intelligence, which is increasingly being used in various spheres of life. Artificial intelligence is a rapidly evolving group of technologies that bring about a wide range of economic, environmental, and social benefits in all sectors of the economy and areas of social activity. Because the use of AI systems enables better forecasting, optimised resource utilisation, and personalised digital solutions for individuals and organisations (customised to user needs), it can provide businesses with a competitive advantage and improve social and environmental benefits in various areas, such as healthcare, agriculture, education and training, media, sports, culture, infrastructure management, energy, transport, and logistics, public services, security, justice, and environmental monitoring. However, it is important to remember that AI can also pose threats and harm the public interest and fundamental rights protected by European Union law, depending on the circumstances of its application and the level of technological development. These damages may be material or non-material, including physical, psychological, social, or economic[6].

Governance, ethics and societal dimensions of digital transformation

Digital transformation in Europe is driven by a new form of governance called Digital Governance, which aims to establish rules of compliance between public and private organizations, citizens, and associations in the provision of new digital services. It ensures that the use of information technology delivers valuable digital services to citizens and other stakeholders while protecting their various rights, such as property and identity[7].

Interestingly, the European Union's digital governance model balances innovation, accountability, and citizen protection. For example, the Digital

[6] Recitals 4-5 of Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139, (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (OJ 2024, L 2024/1689).

[7] F.A. Algazo, S. Ibrahim, W.S. Yusoff, *Digital governance emergence and importance*, "Journal of Information System and Technology Management" 2021, No. 6, p. 18-26.

Services Act (DSA)[8] establishes new transparency and accountability rules that compel providers of intermediary services to publish annual transparency reports detailing their content moderation practices, algorithmic systems, and user engagement metrics, as outlined in Article 13 of the Regulation.

Complementing this regulatory approach, the European Digital Innovation Hubs (EDIHs) initiative[9] highlights the role of digital governance in driving innovation. Indeed, these hubs provide small and medium-sized enterprises (SMEs) with access to advanced digital tools, AI and cybersecurity expertise, and funding to accelerate digital transformation[10].

The EU is also highly concerned with ensuring the ethics of digital transformation and has defined strong requirements in this regard. First, digital services must comply with fundamental values such as human dignity, privacy, fairness, and solidarity. This principle ensures that technology serves people rather than the reverse (see Chapter 1 of the European Declaration on Digital Rights and Principles[11]). Consequently, human oversight should be ensured for each new digital service, especially when generative AI is used in the development process.

Indeed, the AI Act establishes rules to ensure "trustworthy AI" (objectives, Articles 1 and 95[12]), emphasizing transparency, accountability, and safety. It aims to address concerns such as algorithmic bias, discriminatory outcomes, and the reduction of associated risks, while also highlighting the need for explainable decision-making processes. Moreover, the Act provides a framework that identifies high-risk AI systems and general-purpose AI

[8] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), http://data.europa.eu/eli/reg/2022/2065/oj [accessed: 10.11.2025].

[9] *European Digital Innovation Hubs. Shaping Europe's Digital Future*, https://digital-strategy.ec.europa.eu/en/policies/edihs [accessed: 10.11.2025].

[10] *EDIH Work Programme 2021-2023. European Digital Innovation Hubs Network*, https://european-digital-innovation-hubs.ec.europa.eu/knowledge-hub/guidance-documents/edih-work-programme-2021-2023 [accessed: 12.11.2025].

[11] *European Declaration on Digital Rights and Principles. Shaping Europe's Digital Future*, https://ec.europa.eu/newsroom/dae/redirection/document/94370 [accessed: 13.11.2025].

[12] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), http://data.europa.eu/eli/reg/2024/1689/oj [accessed: 13.11.2025].

models with systemic risks, and outlines the responsibilities of relevant institutions for implementation and enforcement[13]. It also defines exemptions for scientific research and development.

While ethics brings many obligations, its emphasis on developing human-centred digital services also fosters responsible innovation. Many European initiatives discussed earlier (e.g., the Digital Services Act, Digital Innovation Hubs) demonstrate how governance can balance technological progress with ethical responsibility. The approach of defining rules at the very start of the new digital revolution is a key measure to reinforce social progress, ensure acceptability, and guarantee the fundamental rights of citizens.

Achieving an efficient and accepted digital transformation throughout the EU also requires paying attention to social inclusion. Indeed, technology aims to bring enhancement for each citizen, especially the weakest, and thus has to ensure equality and accessibility. To this end, it is important to underline the crucial role of education towards technology, in particular revolutionary tools such as Artificial Intelligence, whose profound concepts and functioning are not visible and easily understood.

To address these challenges, a combination of strategies at the European, national, and territorial levels is required. At the European level, we can cite the EU Digital Education Action Plan (2021-2027)[14], which helps provide an accessible and high-quality digital education ecosystem across all Member States. Moreover, the Path to the Digital Decade also helps to develop digital literacy and ensure inclusion by promoting the objective that 80% of Europeans acquire at least basic digital skills by 2030[15].

At the national level, France has implemented the Plan national pour un numérique inclusif (National Plan for Digital Inclusion[16]), which provides a concrete framework to reduce the digital divide across regions and social groups and mobilizes public and private actors to teach digital skills to more

[13] M. Mueck, C. Gaie, D.C. Gkikas, *Introduction to the European Artificial Intelligence Act*, [in:] *European Digital Regulations*, M. Mueck, C. Gaie [eds.], Cham 2025.

[14] *Digital Education Action Plan: policy background. European Education Area*, https://education.ec.europa.eu/focus-topics/digital-education/plan [accessed: 17.11.2025].

[15] *Europe's Digital Decade. Shaping Europe's Digital Future*, https://digital-strategy.ec.europa.eu/en/policies/europes-digital-decade [accessed: 18.11.2025].

[16] *France – National Plan for Digital Inclusion. Digital Skills and Jobs Platform*, https://digital-skills-jobs.europa.eu/en/actions/national-initiatives/national-strategies/france-national-plan-digital-inclusion [accessed: 20.11.2025].

than 1.5 million people. Interestingly, the plan focuses on helping vulnerable populations such as elderly people and persons with disabilities. The specificity of rural populations is also tackled by combining these efforts with the objective of installing fibre in rural regions through the Plan France Très Haut Débit[17].

Finally, at a territorial level, the Greater Paris Metropolis implements complementary strategies to national policy through its Digital Inclusion Programme[18], combining digital skills support with responsible digital practices. By offering a Digital Pass, the initiative has enabled nearly 7,000 residents across 34 communes to receive training in basic digital skills, while Digital Advisors assist vulnerable populations in achieving digital autonomy. This approach illustrates how regional action can effectively adapt national digital inclusion objectives to local contexts for maximum impact.

Conclusions

Digital transformation impacts almost every aspect of life. It affects the economy and public policies implemented by individual countries and the European Union. It influences the economic development and the quality of life of people who, thanks to digital tools, can handle their affairs more quickly, often without leaving home. Digital transformation must be people-centred, respecting their dignity and privacy, and upholding ethical values.

Implementing modern digital technologies requires not only planning but also coordination and consistent action aimed at computerisation, both in the private, economic, and public spheres. Digital transformation is the process of implementing these technologies in all areas of the public and private sectors. This sometimes requires a shift in thinking that must be open to new digital tools that significantly simplify life and streamline social, economic, and public activities.

The digital potential of societies, countries, and the European Union is still not fully exploited; therefore, it is necessary to introduce reforms aimed

[17] *Roll-out of super-fast broadband and the France très haut débit plan. Haut-commissariat à la stratégie et au plan*, https://www.strategie-plan.gouv.fr/en/publications/evaluation-plan-france-tres-debit-premier-rapport [accessed: 20.11.2025].

[18] *Numérique pour tous. Métropole Du Grand Paris*, https://www.metropolegrandparis.fr/fr/numerique-pour-tous [accessed: 25.11.2025].

at increasing the use of new technologies, which must, however, be done in a responsible manner and at the same time minimise digital exclusion.

The use of new technologies to determine the digital transformation process cannot be arbitrary. It is essential to monitor their effectiveness and implement improvements where necessary. They must serve people, not threaten them. Responsible use of digital tools is an action aimed at improving people's lives, not just maximising profits, and this is precisely what national, EU, and international digital policies must take into account. Actions undertaken as part of the digital transformation must be well planned, organised, and coordinated at the EU level, which should shape this process appropriately in individual member states.

Bibliography

Algazo F.A., Ibrahim S., Yusoff W.S., *Digital governance emergence and importance*, "Journal of Information System and Technology Management" 2021, No. 6.

Chałubińska-Jentkiewicz K., *Cyberbezpieczeństwo*, [in:] *Leksykon cyberbezpieczeństwa*, K. Chałubińska-Jentkiewicz [ed.], Warszawa 2024.

Chronowska-Sioła E., *Unijna dyrektywa NIS 2 w obszarze cyberbezpieczeństwa – analiza podmiotów kluczowych i podmiotów ważnych*, "Cybersecurity and Law" 2025, No. 2.

Gaie C., Karpiuk M., Spaziani A., *New Technologies in Public Administration*, "Ius et Securitas" 2024, No. 2.

Gaie C., Mueck M., *Introduction to the Networks and Information Systems 2 (NIS2) Directive*, [in:] *European Digital Regulations*, M. Mueck, C. Gaie [eds.], Cham 2025.

Kaczmarek K., *Finland in the light of cyber threats in the context of Russia's aggression against Ukraine*, "Cybersecurity and Law" 2023, No. 1.

Kaczmarek K., *Nordic countries in the face of digital threats*, "Cybersecurity and Law" 2024, No. 1.

Mueck M., Gaie C., Gkikas D.C., *Introduction to the European Artificial Intelligence Act*, [in:] *European Digital Regulations*, M. Mueck, C. Gaie [eds.], Cham 2025.

Włodyka E.M., *Cyberbezpieczeństwo sektora publicznego*, [in:] *Leksykon cyberbezpieczeństwa*, K. Chałubińska-Jentkiewicz [ed.], Warszawa 2024.

Włodyka E.M., Kaczmarek K., *Cyber Security of Electrical Grids – A Contribution to Research*, "Cybersecurity and Law" 2024, No. 2.

* * *

Transformacja cyfrowa w Unii Europejskiej

Streszczenie

Transformacja cyfrowa jest zjawiskiem, które dotyczy nie tylko poszczególnych państw, ale też Unii Europejskiej, nawet można stwierdzić, że jest ona w dobie rozwoju nowych technologii nieunikniona na całym świecie. Właściwie wdrażanie narzędzi cyfrowych do różnych sfer życia nie może odbywać się w sposób niekontrolowany. To przede wszystkim prawodawca powinien zadbać o to, żeby nie dochodziło do naruszeń, które mogą nie tylko godzić w prywatność danych osób, ale też generować znaczne szkody dla państw.

W przypadku transformacji cyfrowej bardzo ważne jest przygotowanie społeczeństwa na nowe wyzwania, które mogą wymagać wielu zmian i odpowiedzialnego podejścia do zjawisk występujących w rzeczywistości cyfrowej. Z jednej strony mamy do czynienia z pociągającym, wirtualnym światem dostarczającym rozrywki i usprawniającym oraz przyspieszającym wykonywanie wielu zadań z drugiej zaś z zagrożeniami wcześniej niespotykanymi, dlatego też należy korzystać z cyberprzestrzeni ostrożnie, żeby unikać cyberzagrożeń.

Celem artykułu jest dokonanie analizy transformacji cyfrowej dokonującej się w Unii Europejskiej, w tym zasad stanowiących jej podstawę. W artykule wykorzystano metodę dogmatyczno-prawną, która umożliwiła analizę przepisów prawnych determinujących proces cyfryzacji mającej miejsce w UE. Posłużono też się metodą teoretyczno-prawną, odnosząc się do poglądów doktryny. Analiza literatury pozwoliła na wyjaśnienie głównych problemów związanych z transformacją cyfrową.

Słowa kluczowe: nowe technologie, transformacja cyfrowa, cyberbezpieczeństwo, sztuczna inteligencja.