Історико-політичні проблеми сучасного світу. 2026. Т. 53. С. 157-167

Modern Historical and Political Issues, 2026, Vol. 53, pp. 157-167

УДК 321:7(4-6ЄС):004.77 https://doi.org/10.31861/mhpi2026.53.157-167

Ivanna Makukh-Fedorkova[1]

European Model of Regulating Digital Platforms as a Tool for Ensuring Democratic Resilience

The article examines the regulation of digital platforms in the European Union as a tool to protect democracy amid digital transformation and geopolitical uncertainty. It explores the impact of platforms on public opinion, political mobilization, and elections, as well as risks of disinformation, manipulation, and concentrated information power. These challenges are intensified by Russia's aggression against Ukraine and unpredictability in U.S. foreign policy, highlighting the EU's need for digital sovereignty.

The study reviews the E-Commerce Directive, the Code of Practice on Disinformation, and the Digital Services and Markets Acts, their complementary roles, and compares EU and U.S. approaches to platform liability and balancing freedom of expression with public interest. It is concluded that the systemic regulation of digital platforms in the EU serves as a key tool for strengthening democratic resilience, protecting user rights, and ensuring the security of the digital space amid contemporary informational and security challenges.

***Keywords*:** digital policy, digital sovereignty, digital platforms, digital transformation, disinformation, information security, European Union.

Іванна Макух-Федоркова[1]

Європейська модель регулювання цифрових платформ як інструмент забезпечення демократичної стійкості

У статті досліджується регулювання цифрових платформ у ЄС як механізм захисту демократії в умовах цифрової трансформації та геополітичної нестабільності. Проаналізовано вплив онлайн-платформ на формування громадської думки, політичну мобілізацію та виборчі процеси, а також ризики поширення дезінформації, маніпулятивного контенту й концентрації інформаційної влади. Особливу увагу приділено загостренню цих викликів у контексті повномасштабної агресії Росії проти України та зростання невизначеності у зовнішній політиці США, що актуалізувало потребу ЄС у зміцненні цифрового суверенітету та автономної моделі врядування.

Розкрито еволюцію нормативної бази ЄС у сфері цифрової політики, зокрема значення Директиви про електронну комерцію, Кодексу практики щодо дезінформації, а також законодавства в рамках Закону про цифрові послуги та Закону про цифрові ринки. Показано їхню взаємодоповнюваність: Закон про цифрові послуги спрямований на забезпечення прозорості, підзвітності та мінімізації системних ризиків в інформаційному середовищі, тоді як Закону про цифрові ринки покликаний обмежити надмірну ринкову владу великих платформ і забезпечити

[1] PhD in Political Science, Associate Professor of the Department of International Relations and Public Communications, Yuriy Fedkovych Chernivtsi National University, Chernivtsi, Ukraine.
Кандидатка політичних наук, доцентка кафедри міжнародних відносин та суспільних комунікацій, Чернівецький національний університет імені Юрія Федьковича, м. Чернівці, Україна.
E-mail: i.makuch-fedorkova@chnu.edu.ua; https://orcid.org/0000-0003-2198-8727.

справедливу конкуренцію. Окремо проаналізовано інституційний механізм реалізації цих актів, включно з роллю Європейської Комісії та національних координаторів цифрових послуг.

У статті також здійснено порівняльний аналіз європейської та американської моделей регулювання цифрових платформ, що дозволило виявити відмінності у підходах до відповідальності платформ і балансу між свободою вираження поглядів та захистом публічних інтересів. Обґрунтовано, що європейська модель має превентивний характер і формує глобальні стандарти через так званий «брюссельський ефект». Зроблено висновок, що системне регулювання цифрових платформ у ЄС є важливим інструментом зміцнення демократичної стійкості, захисту прав користувачів і забезпечення безпеки цифрового простору в умовах сучасних інформаційних та безпекових викликів.

***Ключові слова*:** цифрова політика, цифровий суверенітет, цифрові платформи, цифрова трансформація, дезінформація, інформаційна безпека, Європейський Союз.

Formulation of the Scientific Problem and Its Significance. In the context of the rapid development of information technologies and digital transformation, online platforms are becoming a key channel of communication, information exchange, and political participation for citizens. Social networks, search engines, messaging services, and other digital platforms not only change the way people communicate and access information, but also actively influence the formation of public opinion, political mobilization, and electoral campaigns. In a digitally transforming society, both reliable information and disinformation, manipulative content, or propaganda are often disseminated through the online environment, potentially undermining the principles of transparency, equality, and fairness in democratic processes.

These challenges have become particularly acute in the context of the full-scale aggression of the Russian Federation against Ukraine, when the information space has become an element of hybrid warfare and a tool of external influence on democratic societies. At the same time, uncertainty is growing regarding the strategic priorities of U.S. foreign policy, as the United States has traditionally acted as a guarantor of security in the European space. Fluctuations in American policy concerning support for Ukraine, regulation of technology giants, and the protection of democratic standards reinforce the need for the European Union to act more autonomously and to develop its own model of digital governance. Under such conditions, the regulation of digital platforms becomes not only a matter of market oversight or consumer rights, but also a component of a broader strategy to safeguard democratic resilience and digital sovereignty.

The issue of the legal regulation of large digital platforms, which exert substantial influence over the information space and can significantly shape the public discourse agenda, is particularly relevant. Insufficient oversight of recommendation algorithms and platform advertising policies may lead to the concentration of informational power, increased political polarization, and heightened risks of manipulation by both state and non-state actors. Therefore, the initiatives of the European Union aimed at establishing clear rules for the functioning of digital platforms are of strategic importance.

Research into the mechanisms of European regulation of the digital space is scientifically significant, as it makes it possible to assess the effectiveness of legal instruments in ensuring democratic procedures under conditions of geopolitical instability and information threats. The relevance of this issue stems from the fact that proper governance of digital platforms directly affects the resilience of democratic institutions, the level of public trust in political processes, and the quality of public discourse in a new security reality.

Analysis of Recent Research. The structure of academic research on the regulation of digital platforms in the EU as a mechanism for safeguarding democracy combines both theoretical and normative-applied dimensions. The theoretical foundation consists of works analyzing the impact of digital communication on democratic institutions, particularly the problems of disinformation and the fragmentation of the public sphere (Bennett and Livingston, 2018; Sunstein, 2017), as well as the concept of the EU's global regulatory influence, known as the "Brussels Effect" (Bradford, 2020).

The normative dimension is shaped by key EU legal acts, including Directive 2000/31/EC (European Union, 2000), Regulation (EU) 2022/1925 (Digital Markets Act) (European Union, 2022a) and Regulation (EU) 2022/2065 (Digital Services Act) (European Union, 2022b), as well as the Charter of Fundamental Rights of the European Union (European Union, 2012), which defines the balance be-

tween freedom of expression and the protection of the democratic order. Studies on mechanisms for countering disinformation and on the practical implementation of the new rules, including sanctions against large platforms (European Commission, 2018, 2022, 2025a and 2025b), are also important. Taken together, these sources make it possible to consider the regulation of digital platforms as a comprehensive instrument for ensuring transparency, accountability, and democratic resilience in the digital age.

Formulation of the Aim and Objectives of the Article. The aim of the article is to examine the regulation of digital platforms in the EU as a mechanism for the protection of democracy. To achieve this aim, the following objectives are defined: to analyze the key EU legal acts concerning digital platforms; to investigate the mechanisms of control and coordination at the national and European levels; to identify the risks of concentration of informational power and the spread of disinformation; and to summarize the effectiveness of the European model of digital regulation for the protection of democracy.

Methodology. The methodological basis of the study is a combination of general scientific and specialized approaches aimed at analyzing the European model of digital platform regulation as a tool for ensuring democratic resilience. The research employs a systemic approach, which allows digital regulation in the EU to be viewed as an integrated multi-level system of legal, institutional, and political mechanisms. An institutional approach is also used to examine the role of the European Commission, national Digital Services Coordinators, and other regulatory bodies in ensuring the implementation of digital legislation.

A comparative legal method is applied to contrast the European and American models of digital platform regulation, particularly regarding intermediary liability and the protection of freedom of expression. Normative legal analysis is used to examine the provisions of key EU acts, such as the Digital Services Act, the Digital Markets Act, the GDPR, and the Code of Practice on Disinformation. Content analysis is applied to study scholarly approaches to disinformation, information manipulation, and algorithmic influence on public opinion.

The historical-genetic method makes it possible to trace the evolution of EU digital regulation from the E-Commerce Directive to the current DSA/DMA framework. A system-functional approach is used to identify the interaction between different elements of digital governance and their role in ensuring democratic resilience. The empirical basis of the study includes official European Union documents, European Commission decisions, and analytical reports on the functioning of digital platforms.

The application of these methods ensures the comprehensiveness of the analysis and supports the conclusion that the European model of digital regulation is an effective mechanism for strengthening democratic resilience, protecting users' rights, and ensuring a secure information environment.

Presentation of the Main Material. Europe today faces complex challenges of the digital age, in which online platforms increasingly shape the topics of public debate, the nature of political communication, and the conditions of access to information. At the same time, the growing influence of global technology corporations gives rise to a number of significant risks, including the spread of disinformation, manipulative influence on public opinion, and the concentration of communicative power in the hands of a limited circle of private actors. Under these conditions, the regulation of digital platforms in the EU has in recent years become one of the priority areas of legal policy, directly linked to ensuring the resilience of democratic institutions and the protection of fundamental human rights.

The rapid digitalization of society has led to a situation in which large online platforms have become not only technical intermediaries in the exchange of information, but also influential actors in the public sphere, capable of shaping the agenda, determining the visibility of political content, and indirectly influencing electoral processes. Automated content curation systems, political advertising tools, coordinated information campaigns, and bot networks create qualitatively new risks for fair, transparent, and pluralistic public debate in a democratic society. Digital platforms, including Facebook, Twitter (now X), YouTube, and Google, have become key intermediaries in the dissemination of information, news, and political messages. Their role is no longer limited to the purely technical function of transmitting content, as algorithmic recommendation systems, advertising models, and microtargeting mechanisms are capable of significantly influencing the structure of the information space. As a result, the principles of content selection and promotion, as well as the commercial logic of audience engagement, increasingly shape public opinion and affect citizens' political behavior.

The threat to democracy in Europe has gradually intensified under the influence of digital technology development and changes in political communication practices. Social networks and online platforms have greatly expanded the possibilities for information dissemination, but at the same time they have opened the way for manipulation. The Cambridge Analytica scandal demonstrated that users' personal data can be used to influence their political views through targeted advertising (Isaak and Hanna, 2018, p. 57). This revealed a serious vulnerability of democratic electoral processes in the digital age. In this context, researchers W. Bennett and S. Livingston draw attention to the formation of the so-called "disinformation order." They explain that digital media have become not merely a channel for news, but a systemic tool for manipulating public opinion. The constant repetition of manipulative messages, the spread of fake news, and emotionally charged content undermine trust in state institutions and electoral processes. The American scholars note that in many democratic countries, citizens' trust in traditional institutions, political parties, and the media is declining, creating a favorable environment for disinformation to reach large audiences and shape alternative, often radical narratives (Bennett and Livingston, 2018, pp. 128-130).

After the 2016 U.S. elections, this problem became particularly visible in various countries around the world, as digital platforms were actively used for informational influence by both domestic and foreign actors. Another risk to democracy is the logic of social media algorithms. According to American lawyer and social theorist C. Sunstein, algorithms sort content according to users' preferences and promote messages that evoke strong emotions, as this increases engagement. As a result, "information bubbles" are created, where people mostly see content similar to their own views, while alternative perspectives remain unnoticed. This limits a shared democratic discourse and intensifies societal polarization (Sunstein, 2017, pp. 1-30).

In response to digital threats, Europe has strengthened the protection of democratic institutions and implemented oversight of the online space, notably through the development of a legal framework and regulatory mechanisms for digital platforms. This underscores the need for systemic intervention to establish transparent rules for platform operations and to ensure a balance between freedom of expression and the protection of public interests. To counter these threats and reinforce democratic principles, the EU has introduced a comprehensive set of legislative measures regulating the activities of online platforms and setting standards for transparency and accountability.

The formation of the EU's regulatory space to counter manipulative tools in the digital environment has occurred gradually in response to rapid transformations in the information sphere and new challenges to democracy. Over the past decade, the EU has evolved from a passive observer into a leading global norm-setter in the digital domain. One of the first steps was the establishment in 2015 of the East StratCom Task Force, a Special Group on Strategic Communications of the Eastern Partnership, aimed at identifying and neutralizing harmful information narratives (European Union Websites, 2021).

The EU recognized that the deliberate dissemination of false information and data manipulation poses a serious threat to democracy and societal stability. Such influences were often carried out by state or state-linked actors, notably the Russian Federation, which, following the onset of aggression against Ukraine, actively utilized digital platforms to spread propaganda. In response, the EU began developing comprehensive measures to regulate the information space and protect citizens from manipulation, including legislative initiatives concerning personal data. A key milestone was the adoption of the General Data Protection Regulation (GDPR) in 2016, which came into effect in 2018. The GDPR establishes rules for the collection, processing, and storage of personal information, guaranteeing citizens the right to control the use of their data, restricting automated profiling without consent, and imposing significant sanctions for violations. Penalties can reach up to €20 million or 4% of a company's global turnover, thereby ensuring real accountability for digital platforms and political actors in the improper use of personal information (European Union, 2016).

The next systemic legal initiative by the EU in response to digital threats was the EU Code of Practice on Disinformation (European Commission, 2018), which established voluntary standards for online platforms regarding the fight against disinformation, algorithmic transparency, and reporting on content moderation. This document laid the foundation for a systematic approach to regulating the digital environment and provided a basis for subsequent legislative measures. An earlier important step was the adoption of the Directive on Electronic Commerce (Directive 2000/31/EC) (European Union,

2000), which defined the liability of internet intermediaries for user-generated content and established a "safe harbour" regime protecting platforms from direct legal responsibility. These legal frameworks demonstrate that the EU has long been consistently shaping the regulation of the digital space, which is particularly relevant today, as the rapid growth of political and commercial online activity calls for stricter oversight. In 2024, the EU also adopted a regulation on the transparency and targeting of political advertising, which standardized the rules for distributing political ads on digital platforms and provided an additional mechanism for monitoring informational influence on voters (European Union, 2024c).

Given the key role of large online platforms in shaping the digital market and the information environment, a logical continuation of previous initiatives was the adoption of comprehensive regulations that establish an integrated normative framework. A central element of this framework is Regulation (EU) 2022/2065 of the European Parliament and of the Council on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act, DSA) (European Union, 2022b), along with Regulation (EU) 2022/1925 of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act, DMA) (European Union, 2022a).

It is worth noting that the adoption of the new EU legal framework for digital governance was preceded by the recognition that traditional approaches to regulating electronic commerce and online intermediaries, established in the early 2000s, no longer correspond to the scale and influence of modern digital platforms. In particular, the rapid growth of social networks and search engines, the concentration of market power in the hands of a few global corporations, the spread of disinformation, and instances of interference in electoral processes have revealed structural flaws in the previous model of self-regulation. In this context, recognizing the need to balance freedom of expression with the protection of democratic institutions, the EU undertook a comprehensive reform of its digital legislation, resulting in the adoption of two interconnected regulations: the Digital Services Act (DSA) and the Digital Markets Act (DMA). Both merit detailed examination.

When comparing the two EU digital regulations, it is important to note that the DSA has a distinctly public-law orientation and aims primarily to create a safe, transparent, and accountable digital environment. It was adopted in response to the growing volume of illegal content, the spread of disinformation, and the increasing algorithmic influence on public opinion. Under its provisions, fully applicable from 17 February 2024, intermediary services and online platforms must promptly remove illegal content, ensure transparency of algorithmic systems, and protect users' rights effectively (European Union, 2022b). It is also important to highlight that the DSA introduced a differentiated approach: the strictest requirements apply to very large online platforms (VLOPs), whose impact on societal processes is systemic. These platforms must regularly assess and mitigate systemic risks, including those related to disinformation, manipulative practices, or potential interference in electoral processes. In addition, the regulation requires platforms to provide reasoning for content moderation decisions, ensure effective mechanisms for appeals, and guarantee transparency in online advertising, including disclosure of the advertiser and targeting criteria. Thus, the Digital Services Act combines tools for combating illegal content with appropriate safeguards for freedom of expression, a fundamental value of democratic society.

In turn, the DMA adopts a different, yet complementary, regulatory approach. Whereas the DSA concentrates primarily on content moderation and the mitigation of systemic societal risks, the DMA addresses structural imbalances in the digital economy and ensures fair competition across the online market (European Union, 2022b). The regulation introduces the term "gatekeepers" to designate large platforms that have significant influence over the internal market and can restrict or control other companies' access to users. Specific obligations and prohibitions are imposed on these companies to prevent abuse of their dominant position, such as excessively promoting their own services or limiting interoperability with other platforms. In this way, the Digital Markets Act establishes competitive conditions for the functioning of the digital market, which, on a broader scale, promotes informational pluralism and reduces the concentration of communicative power.

Thus, comparing these two regulations, it can be concluded that they serve different but complementary functions. The DSA provides normative mechanisms for controlling the information environment and protecting users' rights, while the DMA creates structural conditions for fair competition and limits excessive market power. Together, these acts form an integrated regulatory model based on

the principles of responsibility, proportionality, and respect for the fundamental rights enshrined in the Charter of Fundamental Rights of the European Union (European Union, 2012). Moreover, unlike previous self-regulatory approaches, the modern model provides clear oversight and sanction mechanisms, and the European Commission is empowered to monitor compliance with the requirements of both regulations and to impose substantial fines in case of violations.

Thus, the adoption of the DSA and DMA represents a logical step in the evolution of European digital policy, as it reflects the EU's ambition not only to adapt the legal framework to new technological realities but also to establish robust legal safeguards for the functioning of an open, competitive, and democratic digital space.

It is worth noting that these regulations are already being applied in practice, demonstrating their effectiveness in regulating digital platforms and protecting users' rights. A notable first example in the context of the Digital Services Act was the imposition of a fine on platform X (formerly Twitter) in December 2025. The European Commission applied the DSA and fined X €120 million for breaching transparency requirements, specifically for the 'manipulative design' of the blue verification system and for incomplete disclosure regarding advertising information and researchers' access to data. This decision represented the first major penalty under this regulation and clearly demonstrated that the EU not only sets rules but is also capable of enforcing them against global platforms, regardless of their jurisdiction (European Commission, 2025a). Another important example is the first major application of the Digital Markets Act, when in April 2025 the European Commission imposed fines on Apple (€500 million) and Meta (€200 million) for violating the rules of fair competition in the digital market (Corlin, 2025). These cases demonstrate the real-world effectiveness of the regulations, establishing legal accountability even for the largest tech companies that previously could evade EU rules. They also drive platform behavior changes, not just through guidance but via concrete fines and requirements to align practices with European standards. Moreover, such cases strengthen the legal framework for future decisions, expanding the precedent and showing that digital sector regulation can have a tangible impact rather than being purely declarative.

In this context, it is appropriate to consider the European approach within a broader comparative framework, in particular in comparison with the United States. Unlike the EU, where a comprehensive and codified model for regulating digital platforms has been established, in the United States § 230 of the Communications Decency Act provides that "no provider or user of an online service shall be treated as the publisher or speaker of information provided by another user" (United States Congress, 1996), which effectively establishes broad immunity for platforms from liability for user-generated content and shapes a model of minimal state intervention. By contrast, under EU law, in particular Articles 6 and 34-35 of Regulation (EU) 2022/2065 on a Single Market for Digital Services, it is provided that online intermediaries do not bear automatic liability for user content, but are required to take specific measures to mitigate risks, ensure transparency of their algorithms, and respond appropriately to illegal content (European Union, 2022b). This approach demonstrates that the American model primarily protects platforms from legal liability, whereas the European model is aimed at ensuring their accountability in order to safeguard democracy and fundamental rights. The risk-prevention orientation constitutes a key advantage of the DSA and the DMA, as they not only respond to violations but also establish systemic requirements concerning risk assessment, algorithmic transparency, researchers' access to data, and non-discriminatory access to digital markets.

In recent years, European legislation has consistently developed effective mechanisms to counter disinformation, combining stringent rules with flexible regulatory approaches. Particular attention should be paid to the development of co-regulation and voluntary initiatives, notably the strengthened 2022 Code of Practice on Disinformation (European Commission, 2022). Although adherence to the Code is voluntary, its provisions are integrated into the enforcement mechanism of Regulation (EU) 2022/2065 on a Single Market for Digital Services as an instrument for the practical implementation of legal obligations. Pursuant to Articles 35-45, very large online platforms are required to assess systemic risks, including those related to illegal content and disinformation, and to take measures to mitigate them. Strengthened codes of conduct illustrate how the EU combines binding rules with mechanisms of self-regulation and co-regulation, thereby creating a multi-level model of digital governance (European Union, 2022b). Moreover, it is important to emphasize that the European approach is grounded in the values enshrined in the Charter of Fundamental Rights of the European Union. The

regulation of digital platforms is viewed not merely as an economic or technical matter, but as a means of protecting human rights, including freedom of expression, the right to information, non-discrimination, and the protection of personal data, thereby giving digital policy a clear constitutional dimension (European Union, 2012). The European model of digital regulation also influences not only the internal market but global standards as well: companies operating in the EU are compelled to adapt their rules, thereby extending European approaches beyond the Union. The American scholar A. Bradford has described this phenomenon as the "Brussels Effect" (Bradford, 2020). This approach simultaneously protects individual rights and ensures the stability of the digital environment, as the regulations establish a unified legal framework for all member states, enhance predictability for platforms and users, and reduce market fragmentation.

Furthermore, it should be emphasized that digital platform regulation in the EU is gradually acquiring not only a normative but also a clearly institutional dimension, allowing for the emergence of a comprehensive digital security model. This involves not merely setting obligations for platforms, but establishing a system of continuous and structured oversight of their compliance. A central role in this system is played by the European Commission, which is empowered under the DSA to directly supervise the activities of large online platforms and search engines. At the same time, national digital services coordinators operate within member states, ensuring that centralized oversight is aligned with national enforcement and promoting uniform implementation of the rules across the internal market. In Poland, the national digital services coordinator is the President of the Office of Electronic Communications (UKE), responsible for implementing the DSA, including exchanging information with the European Commission, participating in the European Digital Services Board, and cooperating with coordinators from other member states to implement DSA requirements at the national level (UKE Office…, 2024). In France, this role is performed by the regulator Autorité de régulation de la communication audiovisuelle et numérique (ARCOM), which ensures the implementation of the DSA into national law and coordinates practices with other governmental bodies (ARCOM, 2024). In Germany, the functions of the national coordinator are assigned to the Federal Network Agency (Bundesnetzagentur), which has the authority to impose sanctions and supervise platforms operating on the German market (Bundesnetzagentur, 2024). Similar appointments have also taken place in Austria, Italy, Spain, Hungary, and Portugal, where national regulators serve as DSCs or are preparing to assume this role in accordance with the requirements.

The establishment of national Digital Services Coordinators (DSCs) in EU member states not only strengthens the institutional framework for regulation but also ensures clear and consistent enforcement of the DSA at the national level. Researcher M. Yurukova emphasizes that this role is not merely formal, but has significant implications for the effective application of the Act. In particular, the sequence and effectiveness of applying the new regulation in practice largely depend on how a state selects the competent authority and endows it with powers (Yurukova, 2023, p. 176). Indeed, national coordinators oversee compliance with the rules by digital platforms: they handle complaints, monitor transparency and the limitation of illegal content, protect users' rights, and cooperate with the Commission and other Digital Services Coordinators (DSCs) through the European Digital Services Board, thereby ensuring the consistent application of legislation across the EU (European Commission, 2024). The system combines centralized oversight at the EU level with national competence, takes into account local specificities, enhances understanding of the market and risks in individual countries, and ensures consistent enforcement of the rules (Yurukova, 2023, p. 176). Therefore, national coordinators not only supervise compliance but also implement stable procedures that make the application of the DSA predictable, transparent, and effective for platforms, users, and society. This strengthens public trust in EU digital policy and demonstrates the law's tangible impact in practice.

It is also worth noting that the crisis response mechanism established under the DSA is a key tool allowing the EU and major digital platforms to coordinate effectively in emergencies, such as hybrid threats, widespread disinformation, or other uses of digital services that could undermine security and democratic processes. A crucial component of this approach is two key provisions of the DSA: Article 36 (European Union, 2022b), which establishes a mandatory crisis response mechanism, and Article 48 (European Union, 2022b), which provides for voluntary crisis protocols, creating an additional model of coordination between states, regulatory authorities, and digital platforms. In this way, the DSA establishes a clear legal framework for protecting democracy and national security in the digital

environment, combining mandatory obligations for platforms in crisis situations with mechanisms of voluntary coordination that enhance the effectiveness of prevention and response to informational threats.

Particular attention must be paid to the protection of minors and vulnerable groups, as they are most exposed to harmful content, manipulation, and other online risks. A key aspect of the European approach is the combination of legal, technical, and social mechanisms to minimize these risks. Under the Digital Services Act (DSA), platforms are required to assess risks to children and vulnerable users, restrict access to harmful content, apply age restrictions, ensure transparency of recommendation algorithms, and cooperate with experts or organizations that prioritize reporting harmful material and assist platforms in responding promptly.

The European Commission also provides guidance prepared with input from youth focus groups and academic research, including recommendations on content moderation, support tools, and reporting mechanisms for harmful material. In this context, a research team led by Morales-Navarro (Morales-Navarro *et al.*, 2025) demonstrated that adolescents are capable of auditing generative AI systems, independently formulating evaluation criteria, and detecting potential biases in model outputs. This highlights the practical value of involving young people in assessing digital services and developing algorithmic literacy. From a broader regulatory perspective, such participation can be viewed as one element of a comprehensive approach to enhancing the safety and accountability of the digital environment. This experience underscores the need for systemic preventive regulation, where the primary focus is not only on responding to violations that have already occurred but on preventing potential threats to democracy and user security. At this level, the concept of a preventive culture of responsibility emerges, establishing platform obligations regarding the assessment of systemic risks, algorithmic transparency, user safety, and the protection of the information environment from the outset of digital content flows.

The preventive culture of responsibility in digital regulation is closely linked to the idea of EU digital sovereignty, which entails the Union's ability to set its own standards and rules for large technology platforms independently of global corporations. This encompasses not only the development and application of the DSA and DMA regulations but also the creation of an institutional framework for continuous oversight, coordination, and supervision at both national and European levels. As Ursula von der Leyen stated, "the EU sets its own standards, its own rules" (European Parliament, 2025), encompassing not only regulatory norms but also comprehensive security measures to protect the digital space from manipulation, disinformation, and hybrid threats. Digital sovereignty gives the EU the ability to influence global standards, as companies seeking to operate in the Union's internal market are compelled to adapt their policies to European norms, thereby spreading the values of transparency, competition, and user rights protection beyond the EU. In this sense, the EU's approach is unique, combining legal, technical, and security instruments to ensure platform accountability, safeguard democratic processes, and strengthen the sovereignty of the digital environment.

Despite the effectiveness of the DSA and DMA in creating a transparent and accountable digital environment, the European regulatory model faces a number of challenges. These include the technical complexity of monitoring algorithmic systems, balancing the fight against disinformation with the risk of excessive content moderation, as well as potential political disputes over the limits of state intervention in the digital sphere. Moreover, digital platforms continue to serve as a channel for disseminating political narratives, including those that may reinforce radical or populist tendencies. In some EU countries, this is reflected in the growing support for right-wing and far-right parties, which engage voters through digital channels by spreading nationalist or conservative messages. As the official results of the European Parliament elections held on 9 June 2024 showed, the Rassemblement National party received approximately 31.37% of the votes in France, significantly ahead of President Emmanuel Macron's Renaissance party, indicating the growing influence of right-wing political forces in the EU's digital political environment Parlement européen, 2024). Even with strict European regulations in place, the digital environment continues to shape political processes and pose new challenges to democratic stability. Amid these mounting risks, and in the wake of Russia's full-scale invasion of Ukraine and growing uncertainty over the future direction of U.S. foreign policy, EU member states have shown an unprecedented level of coordination across security, economic, and digital governance domains. In this context, regulating digital platforms in the EU assumes not only

legal but also strategic importance, as the information space has become both a site of hybrid confrontation and a tool of external influence. Enhanced implementation of the DSA and DMA, closer oversight of major platforms, and stronger coordination among member states underscore the European Union's efforts to reinforce digital sovereignty and safeguard the resilience of democratic institutions. As such, EU digital policy is increasingly integrated into the Union's broader security and values-driven strategy, where platform regulation functions as a key instrument for protecting democracy amid ongoing geopolitical turbulence.

Conclusions. The European Union demonstrates a consistent and comprehensive response to the challenges of the digital age by combining a preventive approach to the accountability of online platforms with well developed mechanisms of institutional oversight. The set of regulatory instruments, ranging from the Code of Practice on Disinformation and the E Commerce Directive to the Digital Services Act and the Digital Markets Act, has established a legal framework focused on transparency, accountability, and the security of the digital space, while preserving the competitiveness of the internal market and safeguarding information pluralism. The practical enforcement of these norms, including sanctions imposed on major technology companies, confirms their tangible effectiveness, while the activities of national Digital Services Coordinators ensure coherent implementation across the Member States.

At the same time, the European model faces several structural challenges, including the complexity of overseeing algorithmic systems, the need to maintain an appropriate balance between countering disinformation and protecting freedom of expression, and the growing politicization of the digital sphere. The use of platforms for electoral mobilization, as demonstrated by the results of the 2024 European Parliament elections, highlights the continuing influence of the digital environment on political dynamics. In the context of the full scale war in Ukraine and increasing geopolitical instability, EU Member States have intensified their coordination and increasingly view digital regulation as an integral component of a broader security strategy aimed at strengthening democratic resilience.

Overall, the European approach integrates legal, technological, and institutional mechanisms, promotes digital sovereignty, and contributes to the development of global standards in digital policy. It shows that systematic platform regulation can effectively strengthen democracy, protect users' rights, and enhance the security of the digital environment.

References

1. ARCOM (2024), "*Regulations on Digital Services or DSA: Obligations and concerned services*", available at: https://www.arcom.fr/en/professional-space/regulations-on-digital-services-or-dsa-obligations-and-concerned-services (accessed: 21 February 2026).

2. Bennett, W. and Livingston, S. (2018), "The disinformation order: Disruptive communication and the decline of democratic institutions", *European Journal of Communication*, 33(2), pp. 122-139, available at: https://docslib.org/doc/8248140/the-disinformation-order (accessed 22 February 2026).

3. Bradford, A. (2020), *The Brussels Effect: How the European Union Rules the World*, Oxford University Press, Oxford, available at: https://scholarship.law.columbia.edu/books/232/ (accessed: 19 February 2026).

4. Bundesnetzagentur (2024), "*Bundesnetzagentur becomes central platform supervisory authority for Germany*", available at: https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/EN/2024/20240514_DSC.html (accessed: 21 February 2026).

5. Elections Europeennes (2024), "*France – Elections Européennes 2024*", available at: https://www.electionseuropeennes.eu/france/ (accessed 22 February 2026).

6. Corlin, P. (2025), "EU fines Apple and Meta under digital rules amid trade spat", *Euronews*, 23 April, available at: https://www.euronews.com/business/2025/04/23/eu-fines-apple-and-meta-under-digital-rules-amid-trade-spat (accessed: 14 February 2026).

7. European Commission (2018), "*Code of Practice on Disinformation*", available at: https://digital-strategy.ec.europa.eu/en/library/2018-code-practice-disinformation (accessed: 22 February 2026).

8. European Commission (2022), "*2022 Strengthened Code of Practice on Disinformation*", available at: https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation (accessed: 17 February 2026).

9. European Commission (2024), "*European Board for Digital Services – Digital Strategy*", available at: https://digital-strategy.ec.europa.eu/en/policies/dsa-board (accessed: 21 February 2026).

10. European Commission (2025a), "*Commission fines X €120 million under the Digital Services Act*", press release, 05 December, available at: https://digital-strategy.ec.europa.eu/en/news/commission-fines-x-eu120-million-under-digital-services-act?utm_source (accessed 14 February 2026).

11. European Commission (2025b), "*Digital Services Act: Commission publishes report on European and national focus groups of young people on the protection of minors guidelines*", available at: https://digital-strategy.ec.europa.eu/en/library/digital-services-act-commission-publishes-report-european-and-national-focus-groups-young-people?utm_source (accessed 21 February 2026).

12. European Parliament (2025), "*Promoting and protecting digital sovereignty in the EU*", available at: https://www.europarl.europa.eu/news/en/agenda/plenary-news/2025-10-06/3/promoting-and-protecting-digital-sovereignty-in-the-eu (accessed 22 February 2026).

13. European Union (2000), "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 ('Directive on electronic commerce')", *Official Journal of the European Union*, L 178, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32000L0031 (accessed: 22 February 2026).

14. European Union (2012), "Charter of Fundamental Rights of the European Union", *Official Journal of the European Union*, C 326, 26 October, pp. 391-407, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12012P%2FTX (accessed 14 February 2026).

15. European Union (2016), 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 (General Data Protection Regulation)", *Official Journal of the European Union*, L 119, 4 May, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02016R0679-20160504 (accessed: 22. February 2026).

16. European Union (2022a), "Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA relevance)", *Official Journal of the European Union*, L 265, 12 October, available at: https://eur-lex.europa.eu/eli/reg/2022/1925/oj (accessed 14 February 2026).

17. European Union (2022b), "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) (Text with EEA relevance)", *Official Journal of the European Union*, L 277, 27 October, available at: https://eur-lex.europa.eu/eli/reg/2022/2065/oj (accessed 14 February 2026).

18. European Union (2024c), "Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising (Text with EEA relevance)", *Official Journal of the European Union*, L, 2024/900, 20 May, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R0900 (accessed: 22 February 2026).

19. European Union Websites (2021), "*Questions and Answers about the East StratCom Task Force*", 27 October 2021, available at: https:// https://www.eeas.europa.eu/eeas/questions-and-answers-about-east-stratcom-task-force_en (accessed: 20 February 2026).

20. Isaak, J. and Hanna, M.J. (2018), "User data privacy: Facebook, Cambridge Analytica, and privacy protection", *Computer*, 51(8), pp. 56-59, available at: https://doi.org/10.1109/MC.2018.3191268 (accessed: 22 February 2026).

21. Morales-Navarro, L., Gan, M., Yu, E., Vogelstein, L., Kafai, Y.B. and Metaxa, D. (2025), "Learning AI Auditing: A Case Study of Teenagers Auditing a Generative AI Model", *Proceedings of the ACM on Human-Computer Interaction*, Volume 9, Issue 7, Article No.: CSCW439, pp. 1–29. https://doi.org/10.1145/3757620.

22. Parlement européen (2024), "*Résultats des élections*', available at: https://results.elections.europa.eu/fr/france/ (accessed 22 February 2026).

23. Sunstein, C.R. (2017), *#Republic: Divided Democracy in the Age of Social Media*, Princeton University Press, Princeton, NJ, available at: https://assets.press.princeton.edu/chapters/s10935.pdf (accessed: 21 February 2026).

24. UKE Office of Electronic Communications (2024), "*Digital Services Coordinator – UKE*", available at: https://uke.gov.pl/en/digitalservices/coordinator/ (accessed: 21 February 2026).

25. United States Congress (1996), "*Communications Decency Act of 1996, 47 U.S.C. § 230*", available at: https://www.law.cornell.edu/uscode/text/47/230 (accessed 17 February 2026).

26. Yurukova, M. (2023), "The role of the member states' Digital Services Coordinator for ensuring coordinated and consistent enforcement of the Digital Services Act", *Papers from the International Scientific Conference, European Studies Department, Jean Monnet Centre of Excellence, Faculty of Philosophy at Sofia University "St. Kliment Ohridski*", Vol. 10, pp. 176-187, available at: https://periodicals.uni-sofia.bg/index.php/PEU/en/article/view/1878 (accessed: 21 February 2026).

Стаття надійшла / Received: 01.03.2026
Схвалено / Accepted: 15.06.2026
Опубліковано / Published: 30.06.2026