EUROPEAN DIGITAL LEGISLATION 2026: A LANDMARK YEAR FOR THE EUROPEAN DIGITAL GOVERNANCE FRAMEWORK

Alexandru TĂBUȘCĂ[1]
Silvia TĂBUȘCĂ[2]

Abstract

The European Union has developed one of the most ambitious and comprehensive digital governance architectures globally. Between 2022 and 2025, numerous legislative instruments were adopted with the objective of creating a competitive, secure, human-centric, and trustworthy digital ecosystem. The year 2026 represents a significant milestone because several of these regulations enter advanced implementation and enforcement phases. This paper examines the evolution of the European digital regulatory framework and analyzes the practical implications of the Data Act, the Artificial Intelligence Act, the Digital Services Act, the Digital Markets Act, the revised eIDAS Regulation and the European Digital Identity Wallet, the Data Governance Act, NIS2, the Cyber Resilience Act, and the emerging Digital Fairness agenda. The study highlights the transformation of digital regulation from isolated legislative initiatives into a coherent governance system intended to support innovation while safeguarding fundamental rights, cybersecurity, transparency, competition, and digital sovereignty. Furthermore, the article evaluates the expected impact on public institutions, private enterprises, technology providers, digital platforms, and European citizens. The research concludes that 2026 marks the transition from digital strategy formulation to large-scale operational implementation of the European Digital Decade objectives.

Keywords: Digital Governance, AI Act, Data Act, Digital Services Act, European Digital Identity, Digital Regulation

JEL Classification: K24, K38, O33, O38, L86

1. Introduction

Digital transformation has become one of the defining characteristics of modern society. Governments, businesses, educational institutions and citizens increasingly depend on interconnected digital infrastructures, cloud services, artificial intelligence solutions and data-driven decision-making processes. While technological innovation provides substantial economic and social opportunities, it also generates risks associated with

[1] PhD Associate Professor, Romanian-American University, Romania, alex.tabusca@rau.ro; corresponding author
[2] PhD, Lecturer, Center for Human Rights and Migration, cdom@rau.ro

privacy, cybersecurity, misinformation, market concentration and algorithmic decision-making.

The European Union has responded to these challenges by developing an extensive regulatory framework capable of balancing innovation with accountability, data protection, cybersecurity, competition and fundamental rights protections [1] [3] [5]. Unlike approaches based primarily on self-regulation or market-driven governance, the European model emphasizes legal certainty, consumer protection, transparency and the protection of fundamental rights.

The importance of 2026 derives from the fact that many major legislative initiatives are no longer merely policy proposals or recently adopted instruments but enter substantive implementation phases with binding compliance obligations for organizations across the European Union [1] [3] [7] [9]. Several regulations now reach decisive implementation stages, transforming legal requirements into concrete operational obligations. Organizations throughout Europe must therefore move beyond regulatory awareness and adopt practical compliance mechanisms.

This paper examines the most important legislative initiatives shaping the European digital environment during 2026 and evaluates their expected impact on the future of digital governance in Europe.

2. The Evolution of the European Digital Regulatory Model

The European Commission's Digital Decade initiative established a comprehensive vision for Europe's digital transformation by 2030, focusing on digital infrastructure, digital skills, business digitalization and digital public services [9]. Key priorities include digital skills, secure infrastructure, business digitalization, and digital public services. The 2026 State of the Digital Decade Report highlights continuing investments and national implementation programs designed to achieve these objectives.

The Digital Decade framework does not operate independently. Instead, it connects numerous regulatory instruments that collectively form a coherent governance architecture. These instruments seek to address different dimensions of the digital ecosystem including artificial intelligence governance, data sharing, cybersecurity, online platform accountability and trusted electronic identification services [1] [3] [5] [7] [11]:

- Data governance
- Artificial intelligence
- Platform accountability
- Cybersecurity

- Digital identity
- Competition policy
- Consumer protection

Regulation	Main Objective	Primary Stakeholders	2026 Relevance
AI Act	Trustworthy AI	AI developers and deployers	Major enforcement phase
Data Act	Data sharing and portability	Manufacturers, cloud providers	Operational implementation
DSA	Platform accountability	Online platforms	Ongoing compliance
DMA	Fair digital competition	Gatekeepers	Continued enforcement
eIDAS 2.0	Digital identity	Citizens, governments	Wallet deployment
NIS2	Cybersecurity governance	Essential entities	Full implementation
CRA	Secure digital products	Manufacturers	Compliance preparation

Tabel 1. Comparative Analysis of Major EU Digital Regulations

Source: European Commission regulatory framework documents.

Domain	Example Requirement	Expected Difficulty
AI Governance	Risk assessments	High
Data Sharing	Interoperability	High
Cybersecurity	Incident reporting	Medium
Digital Identity	Wallet integration	Medium
Platform Governance	Transparency obligations	High
Cloud Services	Switching mechanisms	Medium

Tabel 2. Organizational Compliance Challenges Associated with EU Digital Legislation

Source: Author's analysis based on EU legislative requirements.

The emergence of this integrated approach reflects the European belief that technological development requires institutional trust, legal certainty and transparent governance structures.

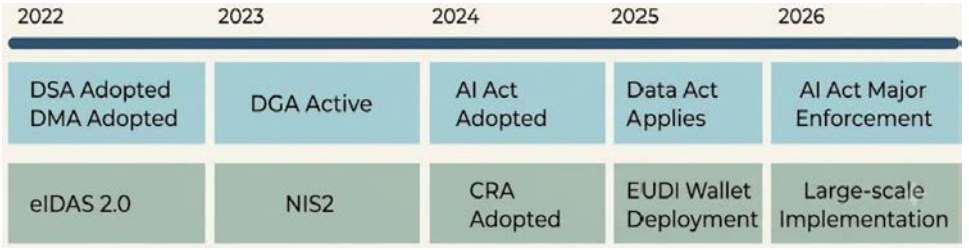

Figure 1. Timeline of Major EU Digital Legislative Milestones (2022-2026)

Source: Author's analysis based on European Commission Digital Strategy, AI Act implementation materials, Data Act documentation and Digital Decade reports

We should also mention that the frameworks regarding the digital infrastructure at EU level are not only directly relevant for legal entities, governments and policy makers. Different stakeholders are also impacted by the different regulations, at different levels of course.

Stakeholder	Main Benefits	Main Challenges
Citizens	Identity portability, safer online services	Learning new digital tools
SMEs	Better market access	Compliance costs
Large Platforms	Regulatory certainty	Extensive oversight
Public Authorities	Improved digital services	Implementation complexity
Researchers	Better data access	Governance requirements
Cloud Providers	Expanded market opportunities	Portability obligations

Figure 2. Benefits and Challenges Created by the 2026 Digital Framework

Source: Author's synthesis from EU digital legislation package.

3. The EU Data Act and the Future of the European Data Economy

The Data Act represents one of the most significant legislative initiatives aimed at creating a functional European data economy by facilitating fair access to data generated through

connected devices and digital services [1] [2]. The regulation entered into force in January 2024 and became applicable in September 2025. Its practical implications continue to expand throughout 2026.

The Data Act seeks to address a central challenge of the digital economy: access to data generated by connected devices and digital services. Traditionally, manufacturers and service providers exercised substantial control over data generated by users. The Data Act attempts to rebalance these relationships.

3.1 Objectives of the Data Act

According to the European Commission, the Data Act establishes a harmonized framework for data access, interoperability and cloud service portability throughout the European Single Market [1] [2]:

- Increasing user access to generated data.
- Facilitating business-to-business data sharing.
- Improving cloud service portability.
- Reducing vendor lock-in.
- Supporting innovation.
- Strengthening the Single Market for Data.

These objectives are expected to stimulate innovation in sectors such as manufacturing, logistics, healthcare, energy and agriculture.

3.2 Economic Implications

The economic significance of data has transformed information into a strategic resource comparable to traditional factors of production. The Data Act is expected to increase innovation opportunities by reducing barriers to access industrial and machine-generated data [1] [2] [12]. By facilitating access to industrial and IoT-generated data, the Data Act may reduce barriers to innovation and support the emergence of new business models based on advanced analytics and AI.

Provision	Expected Impact
User access to device data	Increased transparency
Cloud portability	Reduced lock-in
Fair contractual terms	Improved competition
Public-sector access mechanisms	Enhanced crisis response
Interoperability requirements	Market integration

Table 3. Main Data Act Provision

Source: Adapted from European Commission Data Act documentation

4. AI Act Implementation Milestones in 2026

Artificial intelligence has rapidly become a strategic technology capable of transforming virtually all economic sectors and therefore represents a major focus of European digital governance policy [3] [4]. Consequently, the European Union adopted the AI Act, the first comprehensive regulatory framework dedicated specifically to artificial intelligence.

The AI Act follows a risk-based approach that categorizes AI systems according to their potential impact on society, distinguishing between unacceptable-risk, high-risk, limited-risk and minimal-risk systems [3] [4]. Certain applications are prohibited, while high-risk systems are subject to extensive compliance obligations. Major implementation and enforcement phases become applicable during 2026.

The AI Act represents more than a compliance instrument. It is also a strategic effort to establish Europe as a global leader in trustworthy and human-centric artificial intelligence governance [3] [4] [12]. It is also a strategic effort to establish Europe as a global leader in trustworthy AI governance.

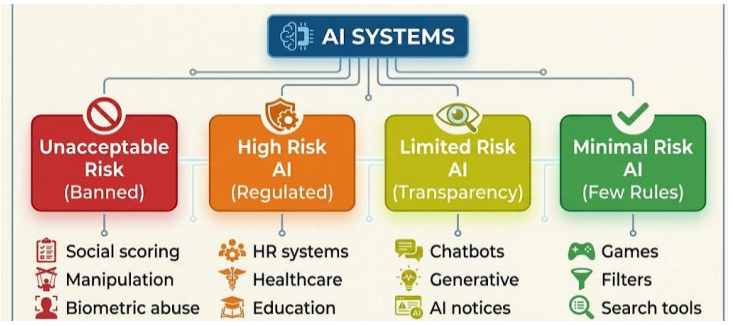

Figure 3. Risk-Based Classification Structure Established by the AI Act

Source: Adapted from Regulation (EU) 2024/1689 on Artificial Intelligence and related implementation guidance

4.1 Categories of AI Systems

The framework identifies:

- Prohibited AI practices
- High-risk AI systems
- Limited-risk applications
- Minimal-risk applications

This tiered structure enables regulators to focus oversight resources where risks are greatest.

Risk Category	Typical Examples	Regulatory Obligations
Unacceptable Risk	Social scoring, manipulative systems	Prohibited
High Risk	Recruitment, healthcare, education, critical infrastructure	Full compliance requirements
Limited Risk	Chatbots, AI-generated content	Transparency obligations
Minimal Risk	Spam filters, recommendation engines	Voluntary best practices

Table 3. Overview of AI Act Categories and Compliance Expectations

Source: Adapted from Regulation (EU) 2024/1689 and implementation guidance

4.2 High-Risk Systems

From 2026 onward, providers and deployers of high-risk AI systems face extensive governance obligations including documentation, risk management and human oversight requirements [3], [4].

- Risk management frameworks
- Technical documentation
- Human oversight mechanisms
- Data quality controls
- Monitoring procedures

These requirements are expected to significantly influence sectors such as healthcare, education, recruitment, finance and critical infrastructure.

Sector	Typical AI Uses	Expected Regulatory Impact
Healthcare	Medical diagnosis	Very High
Education	Student assessment	High
Banking	Credit scoring	High
Public Administration	Automated decision support	High
Manufacturing	Predictive maintenance	Medium
Retail	Recommendation systems	Medium
Media	Content generation	Medium

Table 4. Sector-Specific Impact Assessment of AI Regulation

Source: Author's analysis based on AI Act risk categories and implementation guidance

For the present time, and most likely throughout the foreseeable future if we adopt a rational and realistic perspective, artificial intelligence systems should continue to operate under the ultimate oversight and authority of a human decision-maker. While AI can provide valuable support, analysis, and automation, the final responsibility for critical decisions should remain with human controllers, particularly in highly sensitive and high-stakes sectors such as military operations, healthcare services, and the banking industry, where errors, ethical considerations, and accountability can have significant consequences for individuals and society as a whole.

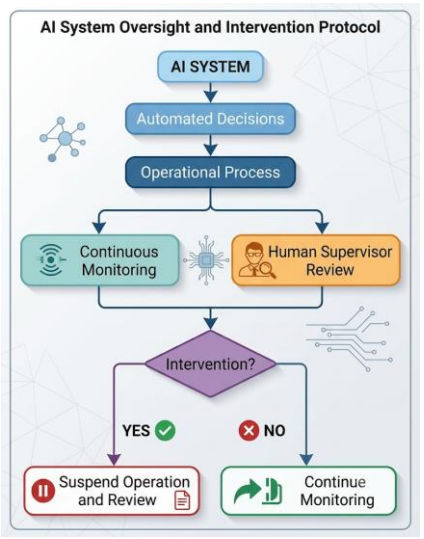

Figure 4. Human-on-the-Loop Supervision Model

Source: Author's synthesis based on post-deployment monitoring and supervisory requirements for high-risk AI applications

In order to establish a consistent and standardized framework for the human monitoring, supervision, and control of artificial intelligence systems, it is essential to develop clear governance guidelines that define responsibilities, decision-making processes, and accountability mechanisms. Such guidelines should ensure that AI systems, regardless of their level of autonomy or complexity, remain subject to effective human oversight throughout their entire lifecycle, from design and deployment to operation and evaluation.

A key element of this governance framework is the application of the four-eyes principle, which requires that critical decisions, approvals, or interventions involving AI systems be reviewed and validated by at least two qualified individuals. This approach helps reduce the risk of human error, bias, negligence, or misuse, while increasing transparency and trust in the decisions supported or generated by artificial intelligence. The *four-eyes principle* is particularly important in high-risk contexts, where the consequences of an incorrect AI-driven recommendation or action may have significant legal, financial, operational, or societal implications.

At the same time, effective AI governance should be structured according to a *governance pyramid*, which distributes responsibilities across multiple organizational levels. At the operational level, specialists and system operators are responsible for the day-to-day monitoring and management of AI applications. At the managerial level, supervisors and department leaders ensure compliance with organizational policies, ethical requirements, and regulatory obligations. At the strategic level, senior executives and governing bodies define the overall vision, risk appetite, and accountability framework for the use of artificial intelligence within the organization.

The combination of the four-eyes principle and the governance pyramid creates a robust control environment in which oversight is not concentrated in a single individual or organizational layer. Instead, responsibilities are distributed, checks and balances are embedded into decision-making processes, and multiple stakeholders contribute to ensuring that AI systems operate safely, ethically, transparently, and in accordance with both organizational objectives and legal requirements. By integrating these two concepts into formal guidelines, organizations can strengthen human control over AI technologies while promoting trust, accountability, and responsible innovation.

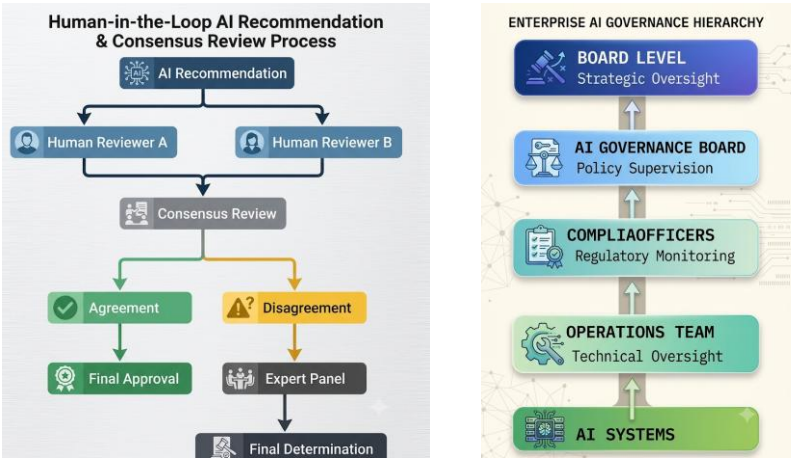

Figure 5. Four-Eyes Principle & Human governance Pyramid for Critical AI Decisions

Source: Author's interpretation of governance mechanisms for AI accountability

5. Digital Services Act and Platform Accountability

The Digital Services Act (DSA) establishes a modern governance framework for online intermediaries, marketplaces, social networks, search engines, hosting services and very large online platforms operating within the European Union [5] [6]. The regulation seeks to create a safer digital environment while preserving innovation and freedom of expression. Organizations covered by the DSA must comply with transparency, reporting and risk-management obligations designed to protect users and reduce systemic online risks [5] [6]:

- Illegal content reporting mechanisms.
- Transparency requirements.
- Risk assessments.
- Independent audits for very large online platforms.
- Enhanced user rights.

The DSA is particularly relevant in combating misinformation, illegal products, online fraud and other systemic risks. DSA addresses a wide range of challenges associated with the digital environment, including the spread of misinformation, the sale and promotion of illegal products, online fraud, and other systemic risks that may negatively affect individuals, businesses, and society as a whole. By establishing a comprehensive set of obligations for online platforms, the DSA seeks to create a safer, more transparent, and

more accountable digital ecosystem in which users are better protected against harmful and unlawful content.

With regard to *misinformation*, the DSA encourages greater transparency in content moderation practices and risk management measures, particularly for very large online platforms whose services can significantly influence public opinion and social discourse. These requirements are intended to reduce the dissemination of false or misleading information that may undermine democratic processes, public health initiatives, or social stability. The DSA is also highly relevant in combating the availability of *illegal products and services* offered through online marketplaces. By imposing stronger due-diligence obligations on digital platforms, the regulation aims to improve the detection, reporting, and removal of unlawful goods, thereby enhancing consumer protection and increasing trust in online commerce.

Furthermore, the regulation plays an important role in addressing *online fraud and deceptive practices*, including scams, identity theft schemes, fraudulent advertising, and other forms of digital misconduct. Through enhanced transparency requirements and accountability mechanisms, the DSA helps limit the opportunities for malicious actors to exploit online services and deceive users.

Beyond these specific issues, the DSA targets a broader category of *systemic risks*, such as threats to fundamental rights, public security, civic discourse, and the integrity of online information ecosystems. By requiring platforms to assess, mitigate, and report such risks on a continuous basis, the regulation promotes a more responsible approach to digital governance and contributes to the long-term resilience, safety, and trustworthiness of the online environment.

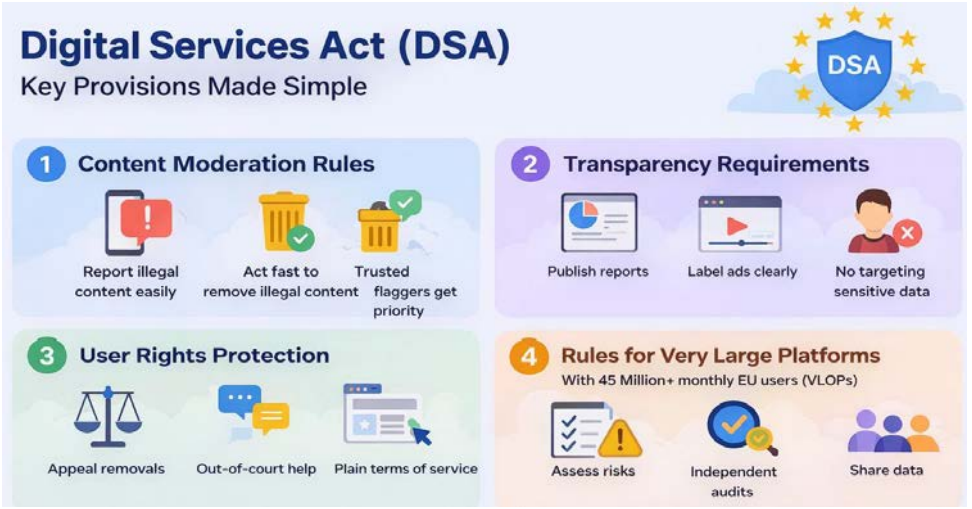

Figure 1. Core Governance Objectives of the Digital Services Act

Source: https://wplegalpages.com/blog/what-is-digital-services-act/

6. Digital Markets Act and Competition in Digital Ecosystems

Complementing the DSA, the Digital Markets Act (DMA) seeks to address structural competition concerns involving major digital platforms designated as gatekeepers, thereby improving market contestability and reducing anti-competitive practices within digital ecosystems [5] [6].

The DMA introduces obligations intended to:

- Prevent unfair self-preferencing.
- Ensure interoperability.
- Facilitate business-user access.
- Support market contestability.

The combined operation of the DSA and the DMA illustrates the EU's comprehensive approach toward digital platform governance.

7. European Digital Identity Wallet and eIDAS 2.0

One of the most ambitious European digital initiatives concerns digital identity. Under eIDAS 2.0, Member States are expected to deploy European Digital Identity Wallets capable of supporting secure authentication and electronic credential management across borders [7] [8]. Deployment activities intensify throughout 2026.

The wallet is expected to support:

- Digital identification.
- Digital driving licences.
- Educational credentials.
- Professional certifications.
- Electronic signatures.

The European Commission expects the EUDI Wallet ecosystem to enhance trust, interoperability and service accessibility throughout the Digital Single Market [7] [8] [9]:

- Cross-border mobility.

- Digital public services.
- Financial onboarding.
- Trust in online transactions.

The initiative also supports broader Digital Decade objectives concerning secure digital public services.

The EUDI Wallet represents a key pillar of the European Union's digital transformation strategy, enabling citizens to securely store and share digital credentials such as identity documents, diplomas, driving licences, and professional certificates. Romania has actively supported the implementation of this initiative through participation in European pilot projects and the development of a national EUDI Wallet ecosystem aligned with the eIDAS 2.0 framework. Several organizations are already contributing to this effort, including Mastercard Europe, which signed a partnership with the Romanian Government to support the deployment of the national digital wallet infrastructure, as well as certSIGN, Banca Transilvania, Visa, and other technology and financial-sector partners involved in testing interoperability, digital identity verification, and secure electronic transactions based on the EUDI Wallet concept.

8. Data Governance Act and European Data Spaces

The Data Governance Act complements the Data Act by strengthening trust-based data sharing mechanisms and supporting the development of Common European Data Spaces [1] [2] [12]. The regulation promotes:

- Data intermediaries.
- Data altruism initiatives.
- Public sector data re-use.
- Cross-border data collaboration.

The long-term objective is the establishment of Common European Data Spaces across strategic sectors, including healthcare, mobility, energy and public administration.

These data spaces may significantly improve innovation capacity while maintaining European values regarding privacy and security.

9. NIS2 and the Cyber Resilience Agenda

Cybersecurity increasingly represents a strategic concern for governments and organizations due to the growing dependence on interconnected digital infrastructures and digital services [10] [11] [14]. The NIS2 Directive expands cybersecurity obligations across critical sectors and introduces stronger governance expectations regarding risk management and incident reporting. While the NIS2 Directive expands cybersecurity obligations across critical sectors the Cyber Resilience Act (CRA) introduces lifecycle security requirements for digital products and software solutions [10] [11], throughout their lifecycle.

Instrument	Primary Focus
NIS2	Organizational cybersecurity
Cyber Resilience Act	Product security
eIDAS 2.0	Trust services
Data Act	Secure data sharing
AI Act	AI-related risk management

Table 2. Cybersecurity Regulatory Landscape

Source: author's own research

The combined effect is the emergence of a comprehensive cybersecurity ecosystem. Within this ecosystem, the NIS2 Directive plays a central role by strengthening cybersecurity requirements across a broad range of essential and important entities. NIS2 establishes a harmonized framework for risk management, incident reporting, supply-chain security, business continuity, and corporate accountability, thereby increasing the overall resilience of critical sectors such as energy, transport, healthcare, banking, and digital infrastructure. By requiring organizations to adopt proactive cybersecurity measures and by enhancing cooperation among national authorities and EU Member States, NIS2 contributes significantly to the creation of a more secure and coordinated European cyber environment.

Complementing this regulatory framework, the CRA extends cybersecurity obligations to manufacturers and providers of digital products containing hardware and software components. The CRA introduces a security-by-design and security-by-default approach, requiring products to meet essential cybersecurity requirements throughout their lifecycle, including vulnerability management and security updates. As a result, cybersecurity becomes an intrinsic feature of digital products rather than an afterthought. Together, NIS2 and the CRA create a layered approach to cyber resilience, addressing both organizational

cybersecurity governance and product security, while fostering trust, reducing systemic vulnerabilities, and strengthening the digital resilience of the European economy.

Looking ahead, the Cyber Resilience Act is expected to drive the development of a European digital market in which cybersecurity assurance becomes a fundamental competitive requirement, encouraging continuous innovation in secure-by-design technologies, automated vulnerability management, and trustworthy digital products capable of adapting to emerging cyber threats throughout their entire lifecycle.

10. Digital Fairness and Future Regulatory Developments

European institutions have increasingly focused on digital fairness, particularly regarding online platforms, dark patterns, manipulative interfaces and consumer vulnerabilities [9] [10].

The proposed Digital Fairness Act may represent the next major regulatory initiative affecting platform governance, consumer rights and digital market behavior after the implementation of the current legislative package [9] [10]. Discussions continue within broader digital simplification and Digital Omnibus initiatives.

Potential focus areas include:

- Algorithmic transparency.
- Consumer manipulation.
- Personalized advertising.
- Influencer marketing.
- Digital consumer rights.

These developments demonstrate that European digital governance remains dynamic rather than static.

11. Implications for Public Administration and Businesses

Public administrations face increasing responsibilities regarding digital service delivery, digital identity deployment, cybersecurity governance, data management and responsible AI adoption [3] [7] [9] [10].

Businesses similarly encounter growing compliance requirements associated with AI governance, data sharing obligations, platform accountability, cybersecurity resilience and

digital identity integration [1] [3] [5] [7] [11]. However, these obligations are accompanied by opportunities to enhance transparency, improve digital trust and access new markets.

Organizations that proactively adapt their governance models are likely to gain competitive advantages within the evolving digital economy.

The implementation of the NIS2 Directive and the CRA also has significant implications for both public administrations and businesses, requiring a shift from reactive cybersecurity practices to proactive risk management and resilience strategies. Public authorities must strengthen their governance frameworks, improve incident response capabilities, and ensure effective cybersecurity oversight across critical public services.

For businesses, particularly those operating in critical and digital sectors, compliance with NIS2 and CRA entails greater responsibility for cybersecurity risk assessment, supply-chain security, vulnerability management, and reporting obligations. Organizations will need to invest in secure-by-design technologies, employee awareness, and continuous monitoring systems to meet the new regulatory requirements.

At the same time, these regulatory frameworks create opportunities by increasing trust in digital services, enhancing operational resilience, and fostering a more secure digital marketplace. Over the long term, NIS2 and CRA are expected to contribute to a stronger cybersecurity culture across both the public and private sectors, supporting sustainable digital transformation and greater confidence in Europe's digital economy.

12. Conclusions

The year 2026 represents a landmark moment in the development of European digital governance. The Data Act, AI Act, Digital Services Act, Digital Markets Act, eIDAS 2.0 framework, Data Governance Act, NIS2 and related initiatives collectively establish one of the world's most sophisticated regulatory environments.

Rather than addressing isolated technological challenges or sector-specific regulatory concerns, these instruments collectively establish a comprehensive and interconnected governance architecture designed to guide and shape the development of the future digital society. Their combined impact extends beyond individual policy objectives, creating a coherent framework that promotes legal certainty, digital trust, and sustainable technological progress across the European Union.

Their implementation reflects a distinct European approach to digital governance, one that seeks to balance and reconcile multiple strategic priorities, including innovation, market competitiveness, cybersecurity, transparency, accountability, and the protection of fundamental rights. By embedding these principles into the regulatory framework, the

European Union aims to foster a digital environment that is not only technologically advanced and economically dynamic, but also secure, trustworthy, human-centric, and aligned with democratic values and societal expectations.

The success of this framework will ultimately depend on effective implementation, harmonized enforcement and the ability of public institutions and private organizations to translate regulatory requirements into practical governance mechanisms. Nevertheless, the evidence available in 2026 strongly suggests that the European Union has moved decisively from digital policy design toward digital policy execution through the coordinated implementation of the Data Act, AI Act, Digital Services Act, Digital Identity Framework, cybersecurity legislation and Digital Decade objectives [1] [3] [5] [7] [9] [10].

References

[1] European Commission – *Data Act*. Shaping Europe's Digital Future. Available at: https://digital-strategy.ec.europa.eu/en/policies/data-act

[2] European Commission – *Data Act Explained*. Available at: https://digital-strategy.ec.europa.eu/en/factpages/data-act-explained

[3] Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence.

[4] European Commission – AI Act implementation timeline and guidance materials.

[5] Regulation (EU) 2022/2065 – Digital Services Act.

[6] European Commission – *Digital Services Act Summary*.

[7] Regulation (EU) 2024/1183 concerning the European Digital Identity Framework.

[8] Commission Implementing Regulation (EU) 2026/798 on European Digital Identity Wallet onboarding requirements.

[9] European Commission – State of the Digital Decade 2026 Report.

[10] Data.europa.eu – Digital Omnibus Update 2026.

[11] NIS2 Directive (EU) 2022/2555.

[12] Cyber Resilience Act (EU).

Bibliography

BELLAMY, C. – *Governing in the Information Age*. Oxford University Press.

CASTELLS, M. – *The Rise of the Network Society*. Wiley-Blackwell.

European Commission – *European Data Strategy*.

European Commission – *Digital Decade Policy Programme 2030*.

European Commission – *Shaping Europe's Digital Future*.

European Parliament – *The Digital Services Act*.

European Parliament – *The Digital Markets Act*.

European Parliament – *The Artificial Intelligence Act*.

ENISA – *Threat Landscape Reports*.

OECD – *Digital Economy Outlook*.

OECD – *Going Digital Project*.

World Bank – *Digital Development Reports*.

NIST – *AI Risk Management Framework*.

European Cybersecurity Agency – *Cybersecurity Certification Frameworks*.

European Commission – *Data Governance Act Resources*.

European Commission – *European Digital Identity Framework*.

European Commission – *Common European Data Spaces*.

European Commission – *Digital Fairness Fitness Check*.

JISOM Journal – Author Guidelines and Journal Information (https://digital-strategy.ec.europa.eu/en/policies/2026-state-digital-decade-package)

EU Digital Omnibus developments (https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng)

State of the Digital Decade 2026 package (https://eur-lex.europa.eu/EN/legal-content/summary/digital-services-act.html)