EU Regulatory Ecosystem for Ethical AI

Vaios Bolgouras[1*], Apostolis Zarras[1,2], Christian Leka[3], Ioannis Stylianou[1], Aristeidis Farao[1], Christos Xenakis[1,3]

[1*]University of Piraeus, Piraeus, Greece.
[2]Foundation for Research and Technology – Hellas, Heraklion, Greece.
[3]InQbit SRL, Bucharest, Romania.

*Corresponding author(s). E-mail(s): vaiosbolgouras@ssl-unipi.gr;

Abstract

AI applications raise complex ethical, legal, and security challenges that demand comprehensive and coordinated governance at multiple levels. In this paper, we examine how key European Union (EU) regulatory frameworks, such as the AI Act, GDPR, and NIS2, interact to set standards for AI security, functionality, and ethical performance. By comparing the objectives and requirements outlined in these regulatory instruments, we identify points of convergence that encourage a holistic approach to creating transparent, accountable, and fair AI systems. This alignment is pivotal for building user trust and mitigating risks associated with data breaches, algorithmic bias, and privacy violations. Moreover, we explore how harmonizing these regulations can maintain the EU's competitive edge in AI innovation, as clear governance structures help businesses remain agile while protecting consumer interests. Our analysis further addresses the ramifications for global AI governance, emphasizing the significance of a unified, forward-looking strategy to ensure responsible AI development. In doing so, we recommend future harmonization initiatives that promote societal well-being, safeguard human rights, and uphold ethical and technological standards worldwide.

Keywords: EU AI Act; AI Governance; Security; Privacy

1 Introduction

The rapid advancement of *Artificial Intelligence* (AI) technologies has profoundly reshaped numerous sectors, including telecommunications, healthcare, finance, and transportation, delivering unprecedented opportunities for efficiency and innovation [1]. However, this technological proliferation also introduces complex ethical, legal, and security challenges that must not be overlooked [2]. As reliance on AI systems grows, so do concerns related to data privacy, algorithmic transparency, fairness, and cybersecurity [3]. These challenges are compounded by AI's inherently global and cross-sectoral nature, which magnifies risks such as biased decision-making, privacy infringements, and societal manipulation [4]. Recognizing that public trust in AI hinges on its ethically responsible deployment, it becomes imperative to establish robust, comprehensive regulatory mechanisms that address these challenges in a holistic and forward-looking manner [5].

Despite a proliferation of frameworks, such as the EU AI Act, the *General Data Protection Regulation* (GDPR), and the *Network and Information Systems Directive* (NIS2) Directive, existing governance approaches often suffer from

fragmentation. Prior research focuses on individual regulations or narrowly scoped sectoral concerns [6, 7]. For example, while GDPR primarily addresses data protection, NIS2 emphasizes cybersecurity, and the AI Act proposes a risk-based classification of AI applications, less attention is given to their combined effect on organizations that operate across different regulatory domains. This siloed perspective leads to inconsistencies in compliance requirements and uncertainty over ensuring user trust, security, and fairness in real-world AI systems. In highly regulated industries, such as finance, healthcare, and telecommunications, these disjointed frameworks can exacerbate compliance complexity, as organizations must navigate overlapping obligations without clear guidance on unified best practices.

Recent interdisciplinary research in legal informatics has introduced the concept of *legal design patterns*, which articulate rule-of-law principles, such as transparency, contestability, and interpretability, as modular, reusable structures for embedding legality into digital systems [8]. This design-oriented approach offers a structured methodology for translating normative requirements into actionable system-level features. In the context of AI governance, particularly within high-impact domains such as healthcare or communications, legal design patterns provide a unifying language to bridge regulatory mandates and technical implementation. Their integration underscores that instruments such as the EU AI Act do not impose arbitrary compliance burdens, but rather instantiate foundational legal norms directly within system architectures [9].

The research presented here seeks to bridge this critical gap by thoroughly examining security, functional, and non-functional requirements across diverse EU regulatory instruments. It illuminates the cross-cutting principles and synergies that support ethical AI deployment while minimizing contradictory or redundant obligations. Specifically, we compare and synthesize the main provisions of the EU AI Act, GDPR, NIS2, *Cyber Resilience Act* (CRA), *Digital Services Act* (DSA), *Digital Markets Act* (DMA), and related guidelines to offer a unified reference point that stakeholders in multiple industries can rely upon for harmonized compliance. By addressing common challenges such as algorithmic bias, data breaches, and opaque AI decision-making, our study provides both theoretical insights and actionable recommendations for regulators, companies, and consumers[1]. This work underscores the importance of adopting an integrated regulatory strategy that fosters innovation while ensuring transparency, accountability, and the safeguarding of fundamental rights across all sectors where AI is deployed.

2 Background and Related Work

The increasing adoption of AI technologies across diverse domains such as telecommunications, healthcare, finance, and transportation has ushered in a new era of innovation and operational efficiency. AI systems enable capabilities ranging from advanced data analytics to autonomous decision-making, fundamentally transforming industries and reshaping societal norms [10]. However, these advancements bring forth significant ethical, legal, and technical challenges, particularly in ensuring transparency, fairness, accountability, and security while deploying AI systems [11]. Despite the robustness of the EU's regulatory ecosystem, the effective governance of AI systems remains a complex challenge. AI's cross-sectoral and global nature amplifies risks such as algorithmic bias, privacy violations, and cybersecurity threats, necessitating coordinated efforts among policymakers, industry leaders, and researchers [12, 13]. Moreover, aligning these frameworks with emerging AI technologies, such as generative AI, is essential for maintaining their relevance and effectiveness [14].

To address these challenges, the EU has developed a comprehensive regulatory framework to foster ethical and trustworthy AI. Central to this framework is the proposed EU AI Act [15], which introduces a risk-based categorization of AI systems and mandates rigorous requirements for high-risk applications to ensure their safety, transparency, and accountability. This initiative reflects the EU's commitment to aligning innovation with the protection of fundamental rights.

[1] In this paper, the term "consumer" is used broadly to include any entity (individual or group) that interacts with, uses, or is affected by AI systems. This includes not only natural persons acting in a private capacity but also workers, citizens, and other non-commercial stakeholders impacted by AI-enabled services.

Complementing the EU AI Act, the GDPR [16] provides a robust data protection and privacy foundation, emphasizing principles such as data minimization, user consent, and accountability; all critical for AI applications. The ePrivacy Directive [17] further strengthens these protections by focusing on the confidentiality of electronic communications, ensuring that data handling practices remain secure and transparent.

Each of the regulatory frameworks discussed in this paper contributes distinct legal and normative perspectives on AI governance. The EU AI Act proposes a horizontal framework introducing a risk-based classification of AI systems and legally binding obligations for high-risk applications. The GDPR offers foundational protections for personal data, emphasizing user rights, consent, and accountability. The ePrivacy Directive complements this by targeting confidentiality and consent in electronic communications. NIS2 strengthens the cybersecurity posture of essential entities, including those deploying AI systems in critical infrastructure. The CRA mandates security-by-design requirements for digital products, including AI-enabled systems, throughout their lifecycle. The EECC governs telecommunications networks and services, with provisions for user protection and interoperability that increasingly intersect with AI functionality. The DSA and DMA regulate digital services and platform markets, respectively, focusing on algorithmic transparency, fairness, and gatekeeper accountability. Finally, sector-specific frameworks such as DORA (financial resilience), the GPSR (product safety), EHDS (health data interoperability), and the Open Data Directive (public sector data reuse) contribute domain-specific constraints and enablers relevant to AI deployment.

The academic discourse has increasingly turned toward the problem of regulatory fragmentation and normative tensions between instruments. Veale and Zuiderveen Borgesius [18] argue that the operationalization of the AI Act's risk-based taxonomy remains ambiguous, particularly when cross-referenced with existing instruments such as GDPR. Smuha [12] cautions against regulatory competition and stresses the need for coherence across frameworks to avoid compliance uncertainty. Floridi [19] underscores the philosophical underpinnings of the EU's approach, emphasizing that ethics and rights protection must remain central to any technical regulation. These perspectives frame the EU's governance model as both ambitious and contingent, requiring interpretive alignment and institutional cooperation for effective implementation. Our analysis builds on this body of work by offering a systematic comparison of how various EU regulations address security, functional, and non-functional requirements. Rather than focusing on individual instruments, we adopt a cross-framework perspective that reveals patterns of convergence and divergence, thereby addressing the coordination challenge that has been consistently identified in the literature.

The EU regulatory landscape also incorporates measures to enhance the cybersecurity and resilience of AI systems. The NIS2 Directive [20] establishes stringent requirements for risk management and incident reporting in critical sectors where AI is integrated into essential services. The proposed CRA [21] enforces security-by-design principles for digital products, mandating continuous monitoring and vulnerability management throughout their lifecycle. Furthermore, the *European Electronic Communications Code* (EECC) [22] harmonizes telecommunications regulations across the EU, addressing user rights and security in AI-enabled communication systems.

In addition to safeguarding privacy and security, EU frameworks emphasize fairness and transparency in digital services. The DSA [23] introduces requirements for algorithmic transparency, ensuring that online platforms provide clear information on how AI systems influence content moderation and recommendations. The DMA [24] complements this by fostering fair competition in digital markets, particularly among platforms utilizing AI-driven services. Additionally, the EU's High-Level Expert Group on AI has contributed the *Ethics Guidelines for Trustworthy AI* [25], which, although non-binding, provide critical guidance for embedding fairness, transparency, human oversight, and inclusivity into AI development processes. These guidelines are an ethical compass, shaping the broader discourse on responsible AI governance.

Despite the robustness of this regulatory ecosystem, the effective governance of AI systems remains a complex challenge. AI's cross-sectoral and global nature amplifies risks such as algorithmic bias, privacy violations, and

cybersecurity threats, necessitating coordinated efforts among policymakers, industry leaders, and researchers [26]. Moreover, aligning these frameworks with emerging AI technologies, such as generative AI, is essential for maintaining their relevance and effectiveness [14].

These frameworks collectively outline core AI deployment principles, including transparency, accountability, human oversight, and fairness. While these principles are most comprehensively and explicitly codified in the EU AI Act, particularly for high-risk AI systems, complementary provisions exist in other frameworks such as the GDPR (e.g., data subject rights and transparency), NIS2 (e.g., cybersecurity risk management), and the DSA (e.g., algorithmic transparency on online platforms).The requirements for mandatory conformity assessments, the establishment of enforcement mechanisms involving national supervisory authorities and the EAIB, and the imposition of fines and penalties for noncompliance originate primarily from the EU AI Act. By creating a harmonized regulatory environment across the EU, these frameworks ensure that AI and related technologies are developed and used responsibly, with a strong emphasis on protecting the rights and freedoms of EU citizens. Furthermore, they have global implications, setting a precedent for international standards and encouraging the adoption of similar regulatory frameworks worldwide, particularly as AI continues to evolve [27].

AI governance has become a focal point of academic discourse, particularly concerning the EU's pursuit of comprehensive regulatory frameworks. Veale and Zuiderveen Borgesius [18] critically examine the draft EU AI Act, addressing its definitions, scope, and potential impacts on AI development and deployment. Their discussion highlights challenges related to the Act's risk-based approach, its repercussions for innovation, and the preservation of fundamental rights. In particular, they argue that the operationalization of the risk taxonomy presents significant ambiguities for regulators and developers alike, thereby requiring stronger interpretative guidance and alignment with existing sectoral norms. Similarly, Floridi [19] investigates the philosophical foundations of the EU's AI legislation, illustrating how it endeavors to reconcile technological progress with ethical considerations and fundamental rights protection. This work underscores the importance of grounding AI regulations in ethical principles to cultivate trustworthy AI systems. Along the same lines, Sartor and Lagioia [28] explore the proposed AI Act's potential effects on AI-based business models, focusing on compliance demands, system classification, and economic implications for developers and providers.

The notion of regulatory competition in AI is discussed by Smuha [12], who analyzes how the EU's initiatives may establish precedents for global standards, ultimately shaping international AI governance. She also warns, however, that without meaningful regulatory convergence, overlapping or competing instruments may introduce legal uncertainty and deter innovation. Butcher and Beridze [13] offer a broader perspective where they examine AI governance worldwide, concentrating on the EU's role in influencing international policy and comparing diverse governance models. Their analysis underscores the EU's significance in setting expectations and norms for AI regulation on a global scale. Meanwhile, Leslie [29] assesses the integration of ethical principles into AI regulation by reviewing a range of AI ethics guidelines, including those formulated within the EU. The study investigates how effectively such guidelines promote ethical AI practices and embed these principles within policy and regulation. Complementing these viewpoints, Wischmeyer and Rademacher [30] compile contributions on AI regulation that span legal, ethical, and technical dimensions, discussing topics such as the AI Act, data governance, liability issues, and the interplay between AI and fundamental rights. Their work emphasizes that normative ambitions, such as transparency, fairness, and user empowerment, must be reflected in the enforceable architecture of regulation, calling for a more coherent and harmonized framework across legal domains.

Regarding sector-specific concerns, Aloisi and DeStefano [31] center on applying AI in employment and labor platforms, scrutinizing how EU regulations address algorithmic management. Their analysis emphasizes implications for workers' rights, data protection, and the necessity for transparency and accountability in AI systems. The European Parliamentary Research Service provides further insights [32], which outlines the EU's digital strategy, including the AI Act and

related regulations, emphasizing their collective effect on the digital landscape and the value of a cohesive regulatory framework. Comparative studies shed additional light on the worldwide influence of AI regulation. For example, MacCarthy [33] examines the EU's AI regulatory framework as a template for the United States, detailing the EU's risk-based approach and focus on fundamental rights. This comparative lens highlights the EU's growing impact on shaping global AI governance and the potential for harmonized regulatory practices across jurisdictions.

Despite abundant research on AI regulation, a gap remains in examining the joint integration of multiple EU frameworks and their combined implications for AI systems' security, functional, and non-functional requirements. Many prior investigations hone in on individual regulations or particular concerns, such as ethical issues or industry-specific ramifications, without a holistic analysis of how these regulatory instruments intersect and reinforce each other. To address this gap, the present study provides a unified examination of the EU's regulatory ecosystem, including the AI Act, GDPR, NIS2 Directive, CRA, and additional frameworks. By assessing the security, functional, and non-functional requirements derived from these regulations, we deliver foundational insights into the responsible development and deployment of AI within a robust regulatory setting. While the EECC and the DMA are not AI-specific regulations, their inclusion in this analysis is justified by their growing relevance to AI-enabled services. The EECC governs digital communications infrastructure, where AI functionalities are increasingly deployed, for instance, in network traffic optimization, predictive maintenance, and adaptive service provisioning. Similarly, the DMA targets systemic risks arising from the dominance of digital gatekeepers, many of which rely on AI-driven mechanisms for content ranking, ad targeting, and user profiling. By examining these frameworks, we aim to capture how sector-specific regulations shape the operational context within which AI is developed and deployed. This is especially pertinent for understanding cross-regulatory tensions and complementarities, such as the interplay between data portability obligations under the DMA and consent management requirements under the GDPR. Including these instruments thus allows for a more comprehensive evaluation of the EU's regulatory landscape as it converges around AI-intensive digital markets and infrastructures.

This work contributes to ongoing discourse by illuminating the synergies and complementarities among diverse regulations, pinpointing areas where further convergence or scrutiny may be warranted, and proposing a harmonized method for promoting ethical AI deployment across multiple sectors. While earlier studies have thoroughly investigated individual aspects of AI regulation and ethics in the EU context, the present analysis integrates these components into a comprehensive overview. It elucidates how the EU's multifaceted regulatory strategy promotes ethical AI practices, emphasizing transparency, accountability, and user empowerment, and sets a standard for emerging global trends in AI governance.

3 Regulatory Requirements

Enforcing regulations such as the AI Act, the NIS2 Directive, the GDPR, the ePrivacy Directive, the CRA, the EECC, the DSA, the DMA, the Ethics Guidelines for Trustworthy AI, the *Digital Operational Resilience Act* (DORA), the *General Product Safety Regulation* (GPSR), the *European Health Data Space* (EHDS), and the Open Data Directive calls for a comprehensive and integrated approach to ensure both compliance and the ethical deployment of AI and other digital technologies. The selection of the analysed regulatory instruments is grounded in their broad legal and operational relevance to AI deployment in the European Union. We focus primarily on binding frameworks that either impose explicit obligations on high-risk AI systems or regulate AI-intensive sectors, such as data governance (GDPR), cybersecurity (NIS2), market fairness (DMA), and digital product safety (CRA), as well as influential soft-law instruments like the Ethics Guidelines for Trustworthy AI. This selection captures both horizontal (cross-sectoral) and vertical (sector-specific) regulatory layers, offering a representative basis for assessing harmonization challenges in EU AI governance.

In addition to framework selection, our analytical structure is grounded in a three-part categorization of system-level requirements—security, functional, and non-functional—which reflects established distinctions in software engineering,

systems design, and AI governance literature. This tripartite model enables a layered analysis of how normative objectives (e.g., data protection, transparency, accountability, risk mitigation) are operationalized across heterogeneous regulatory sources. Rather than treating each instrument in isolation, we classify their provisions according to the type of requirement they instantiate, thereby identifying both convergence patterns and regulatory gaps. Collectively, these frameworks address the multifaceted challenges stemming from the convergence of AI and digital services. Effective implementation demands establishing a detailed set of functional, non-functional, and security requirements to guarantee that AI systems operate safely, transparently, and fairly. Such an approach safeguards fundamental rights and fosters trust in these technologies. By harmonizing this diverse array of regulatory instruments, stakeholders can create a cohesive environment that promotes security, privacy, and resilience across the entire AI ecosystem, thereby upholding the guiding principles mandated by these regulations.

3.1 Security Requirements

Identifying and categorizing security requirements constitute a critical step in evaluating the robustness of the EU's regulatory frameworks for AI and digital systems. Our classification of requirements into three categories (i.e., security, functional, and non-functional) follows established approaches in systems engineering and AI governance literature, where system-level properties are often disaggregated into these interdependent layers to support comprehensive risk assessment and design validation. This analytical structure allows us to identify normative convergence across EU instruments and trace how legal obligations manifest in system architecture. These requirements stem from an analysis of core principles designed to ensure technological ecosystems' security, transparency, and ethical operation. This subsection delves into these requirements, outlining their significance and illustrating how they underpin overarching trust, accountability, and user empowerment objectives.

In the context of safeguarding AI systems and digital infrastructures, several key requirements are vital for ensuring resilient, trustworthy, and ethically grounded operations. Foremost is *Risk and Vulnerability Management*, a core requirement explicitly addressed in Article 9 of the EU AI Act, which mandates the implementation of a risk management system for high-risk AI systems throughout their lifecycle. Similarly, Articles 21–23 of the NIS2 Directive impose cybersecurity obligations on essential and important entities, requiring them to assess, document, and mitigate security risks. These measures are complemented by Article 10 of the CRA, which obliges manufacturers to identify and address vulnerabilities during development and after product placement on the market. This strategy is pivotal for protecting critical sectors, maintaining service continuity, and shielding users from the far-reaching consequences of technological failures. Closely linked is *Data Security and Protection*, a foundational element given the significant volume of personal and sensitive data processed by AI systems. Preserving data confidentiality, integrity, and availability is essential for building trust between users and service providers, as emphasized by regulations such as the GDPR, which mandates measures including encryption, pseudonymization, and access controls.

Equally significant is the principle of *Transparency*, which calls for openness in the functioning of AI systems, enabling users, regulators, and other stakeholders to understand how decisions are made and how data is handled. Transparency fosters trust and supports regulatory compliance by facilitating effective audits and oversight. Complementing transparency is *Accountability*, which requires organizations to assume responsibility for the outcomes and impacts of their AI systems. This includes maintaining comprehensive documentation and undergoing regular audits to demonstrate compliance. Furthermore, *Human Oversight* preserves the role of human judgment in AI applications, particularly in high-stakes contexts, by ensuring the feasibility of meaningful human intervention. This safeguard addresses ethical issues linked to fully autonomous systems and lessens the risk of erroneous or biased decision-making.

Additional requirements reinforce this security framework, including (*i*) *Security-by-Design and Compliance*, (*ii*) *Incident and Post-Market Reporting*, (*iii*) *Fairness and Non-Discrimination*, (*iv*) *Auditability*, (*v*) *Interoperability*, (*vi*) *Global*

Applicability, and (*vii*) *User Empowerment*. Security-by-design embeds security considerations into the early stages of system and product development, making security integral throughout the AI lifecycle rather than an afterthought. Incident and post-market reporting prioritize real-time threat mitigation and continuous monitoring after deployment, thereby strengthening accountability. Fairness and non-discrimination target the potential for AI systems to replicate biases, mandating equitable processes that uphold fundamental rights. Auditability enables external review to ensure alignment with regulatory requirements, reinforcing confidence in the regulatory environment. Interoperability encourages seamless integration and functionality across platforms, reducing fragmentation and enabling innovation. Global applicability reflects the EU's aspiration to influence international standards for AI governance, acknowledging the inherently global character of digital technologies. Finally, user empowerment grants individuals greater authority over their interactions with technology by offering access to personal data, a means to challenge decisions, and effective consent management tools, fostering trust and ethical engagement with AI systems.

When synthesized, these requirements reveal how the EU's regulatory frameworks collectively address the intricate task of governing AI and digital systems. Each framework contributes to this ecosystem, with some emphasizing technical resilience and security while others concentrating on ethical dimensions and user rights.

The EU AI Act serves as a pivotal instrument in AI governance, providing a rigorous framework for regulating high-risk AI systems. It mandates structured risk and vulnerability assessments and continuous post-market surveillance, thereby embedding security-by-design principles to foster reliable, transparent systems. Transparency occupies a central role, obliging developers to convey system limitations and risks clearly so that users may understand and, where necessary, contest decisions. Provisions aimed at mitigating biases address fairness and non-discrimination, while human oversight ensures that autonomous decisions are subject to meaningful human scrutiny. Despite its comprehensive scope, the EU AI Act does not devote substantial attention to interoperability, which lies beyond its primary focus on ethical and functional requirements.

Meanwhile, the NIS2 Directive emphasizes cybersecurity resilience, especially within critical and essential entities. Its risk-based perspective obliges organizations to implement security measures and incident reporting procedures to curtail threats effectively. Although it imposes stringent accountability requirements and prescribes regular audits, the NIS2 Directive prioritizes organizational resilience rather than user-facing considerations, including transparency or user empowerment. Consequently, it complements other frameworks such as GDPR and the CRA by fortifying the security of vital infrastructures.

Renowned as a cornerstone of data protection, GDPR comprehensively tackles data security and user empowerment. It enforces stringent accountability for data controllers and processors while offering individuals extensive rights over their data, including access, correction, and erasure. Transparency remains a salient feature: GDPR requires clear communication regarding data processing practices. It likewise promotes fairness and non-discrimination in data usage, with provisions for human oversight of automated decisions that materially affect individuals. Although GDPR is unparalleled in the domain of privacy and user empowerment, it does not explicitly address interoperability, thus leaving room for regulations such as the EECC and the DMA to fill the gap. In tandem, the ePrivacy Directive bolsters privacy in electronic communications. It enforces user consent for data collection and processing, reinforcing transparency and accountability for service providers. However, its coverage is confined to communications-specific privacy rather than broader security concerns like risk management or security by design. Accordingly, GDPR and the ePrivacy Directive together create a comprehensive privacy framework, although the CRA is needed to address more technical security aspects. The CRA promotes security-by-design and mandates post-market surveillance so that vulnerabilities are managed throughout a product's lifecycle. Accountability is central, as manufacturers must preserve compliance with security standards. However, the Act does not prioritize transparency or user empowerment, focusing on

product-oriented security rather than user-facing ethical issues.

The EECC is pivotal in guaranteeing the security and reliability of communications infrastructures. By stipulating interoperability and transparency, it fosters user confidence in telecommunications networks. Users gain protection through secure communication services and fair access, and providers must alert users to potential risks. Although narrower in scope compared to GDPR or the EU AI Act, the EECC addresses the vital aspect of reliable communication services.

The DSA and the DMA tackle systemic risks and fairness in online platforms and digital marketplaces. The DSA underlines algorithmic transparency, compelling platforms to disclose how content moderation and recommendation systems operate. This provision empowers users to comprehend and govern their digital interactions. The DMA complements this focus by mandating interoperability and data portability for gatekeeper platforms, thereby promoting fair competition and user autonomy. Although both frameworks are robust in transparency and accountability, their security provisions remain restricted to their respective platform and market contexts. While non-binding, the Ethics Guidelines for Trustworthy AI supply a moral foundation by highlighting principles such as human oversight, fairness, and user empowerment. These guidelines help shape best practices and reinforce public confidence in AI. However, their absence of enforcement mechanisms underscores the significance of binding instruments, such as the EU AI Act, in ensuring compliance.

Sector-specific frameworks extend the regulatory tapestry by focusing on resilience and safety in particular domains. For instance, DORA elevates digital resilience in the financial sector, implementing risk management, resilience testing, and reporting obligations. GPSR similarly imposes safety-by-design and post-market monitoring for consumer products. While both frameworks excel in technical and operational security, they do not incorporate transparency, fairness, or user empowerment provisions, given their narrower mandates. In contrast, the EHDS champions secure and equitable access to health data by emphasizing interoperability and user empowerment, facilitating seamless exchange of health information throughout the EU. Its compatibility with GDPR underscores robust data protection standards, although its healthcare-specific focus limits broader applicability. Lastly, the Open Data Directive enhances the reuse of public sector data by promoting fair access to datasets. Its focus on interoperability and global applicability aids AI research and development while fostering transparency in the public sector. Nonetheless, because it does not specifically address security-by-design or risk management, its provisions remain complementary rather than comprehensive.

A notable pattern in Table 1 is the consistent emphasis on accountability and transparency across multiple frameworks—principles critical for cultivating trust in AI systems and ensuring that organizations answer for their products and services. Furthermore, the widespread prioritization of user empowerment confirms the EU's dedication to giving individuals more authority over their data and how AI technologies engage with it. Still, gaps remain in the uniform coverage of specific security requirements. For instance, interoperability is explicitly mentioned only in frameworks such as the EECC, DMA, and EHDS, despite the interconnected nature of AI systems and digital platforms. A broader emphasis on interoperability across all frameworks could enhance functionality and security. Likewise, human oversight, fairness, and non-discrimination are not universally integrated into each framework, indicating possible areas for further strengthening. Although the EU AI Act and GDPR have global applicability, other frameworks have a more region-specific scope. Given the cross-border attributes of AI and cybersecurity threats, broader harmonization of these regulations could amplify their global efficacy.

Examining security requirements across EU regulatory frameworks underscores a layered, comprehensive approach to AI governance. Individual frameworks excel in particular domains, yet their collective application creates a security net encompassing technical, ethical, and user-centric concerns. Addressing identified gaps, such as boosting interoperability and systematically incorporating human oversight and fairness, could further reinforce the EU's leadership in ethical and secure AI deployment. This integrated strategy not only defends users and fosters trust but also serves as a global benchmark for AI

Table 1 Comparison of security requirements across frameworks

	AI Act	NIS2	GDPR	ePrivacy Directive	CRA	EECC	DSA	DMA	Ethics Guidelines	DORA	GPSR	EHDS	Open Data Directive
Risk & Vulnerability Management	•	•	•		•	•	•	•		•	•	•	
Data Security & Protection	•		•	•		•		•		•		•	
Transparency	•		•	•		•	•	•	•			•	•
Incident & Post-Market Reporting	•	•	•		•					•	•		
Security-by-Design & Compliance	•				•	•					•	•	
Human Oversight	•		•						•			•	
Fairness & Non-Discrimination	•		•				•	•	•			•	
Accountability	•	•	•	•	•	•	•	•	•	•	•	•	•
Auditability	•	•	•		•		•			•	•	•	
Interoperability												•	•
Global Applicability	•		•									•	•
User Empowerment	•		•	•		•	•	•	•			•	•

governance. Taken together, the examined frameworks illustrate a layered security architecture in which regulatory provisions are interdependent rather than isolated. For instance, while the EU AI Act mandates structured risk assessments for high-risk systems, these are reinforced by NIS2's obligations on incident response and by the CRA's continuous post-market vulnerability management. GDPR complements these technical obligations by enforcing personal data security through encryption and access control measures. Interoperability requirements in the EECC and DMA, although not focused on security per se, have downstream implications for secure data sharing and system integration. The interaction of these provisions across legal texts underpins a holistic governance model where organizational, infrastructural, and user-level security are mutually reinforcing.

3.2 Functional Requirements

A set of critical functional requirements has been established to ensure that AI systems are developed and deployed in alignment with ethical principles, operational robustness, and societal values. Derived from an analysis of regulatory frameworks and guidelines prioritizing transparency, usability, and data governance, these requirements aim to ensure that AI systems are not only functionally effective but also safe, secure, and user-centric.

A fundamental requirement is *Conformity Assessments*, which are mandated by Chapter 4 (Articles 43–51) of the EU AI Act. These provisions require high-risk AI systems to undergo predeployment conformity checks against technical documentation, quality management procedures, and post-market monitoring strategies. In parallel, Article 9 of the CRA requires manufacturers of digital products, including those embedded with AI, to conduct conformity assessments addressing cybersecurity risks. The General Product Safety Regulation GPSR reinforces this by obliging safety assessments throughout a product's lifecycle (Articles 4 and 9). These assessments validate compliance with technical and ethical standards, minimizing potential harm to users and society. Complementing this is *Security-by-Design and Resilience*, which emphasizes integrating security mechanisms throughout the AI system's lifecycle. Inspired by the CRA and GDPR, this requirement promotes proactive measures against cyber threats, ensuring that AI systems remain robust and capable of withstanding evolving challenges. Additionally, *Continuous Monitoring and Adaptive Systems* underscores the need for AI systems to remain safe, effective, and compliant over time by emphasizing real-time monitoring and adaptation to emerging risks or changes in the operational environment.

Another crucial aspect is *Business Continuity and Crisis Management*, which highlights the importance of operational resilience for AI systems, especially in critical sectors such as finance, healthcare, and telecommunications. This requirement calls for designing architectures capable

Table 2 Evaluation of frameworks against functional requirements

	AI Act	NIS2	GDPR	ePrivacy Directive	CRA	EECC	DSA	DMA	Ethics Guidelines	DORA	GPSR	EHDS	Open Data Directive
Conformity Assessments	•				•						•		
Business Continuity & Crisis Management		•				•				•			
User Consent Management			•	•		•			•			•	
Data Minimization & Integrity	•		•						•			•	•
Security-by-Design & Resilience	•		•		•				•	•	•	•	
Interoperability						•		•				•	
Algorithmic Transparency	•		•				•	•	•				•
Cross-Border Data Flow Governance			•										
Usability & Human-Centric Design			•	•		•	•	•	•			•	
Continuous Monitoring & Adaptive Systems	•	•			•		•			•	•		•

of rapid recovery from disruptions or attacks, thereby preserving trust in the reliability of AI solutions. Equally important is *User Consent Management*, ensuring that users have meaningful control over how their data is collected, used, and shared, in line with principles from GDPR and the ePrivacy Directive. Closely related to this is *Data Minimization and Integrity*, which requires AI systems to collect only essential data while ensuring its accuracy and integrity, thus preventing misuse and mitigating risks of bias or unethical practices.

Algorithmic Transparency is likewise essential for ethical AI deployment, mandating clear and comprehensible explanations of decision-making processes to foster trust, mitigate biases, and ensure accountability, particularly in high-impact applications. *Interoperability* is also critical, enabling AI systems to seamlessly integrate with other platforms, fostering collaboration and reducing barriers to adoption. This ensures that AI functionality is not confined by technical silos and promotes compatibility across diverse environments. Additionally, *Usability and Human-Centric Design* focuses on making AI systems intuitive for all users, including those with limited technical expertise, thus promoting equitable access and empowering individuals. Finally, *Cross-Border Data Flow Governance* addresses the secure and lawful transfer of data in global AI operations. While GDPR governs intra-EU data flows, this requirement extends to maintaining compliance when data crosses international borders, a critical consideration for applications relying on diverse data sources. Collectively, these functional requirements establish a comprehensive framework for the responsible development and deployment of AI systems that align with ethical standards, regulatory obligations, and societal expectations. By incorporating these requirements into regulatory frameworks, stakeholders can foster the responsible growth of AI across various domains.

The evaluation of functional requirements across the EU's regulatory frameworks, as presented in Table 2, reveals a multifaceted approach to governing the development and deployment of AI systems. Each framework contributes uniquely to the collective goal of ensuring that AI technologies are functional, safe, secure, and user-centric. The analysis of these frameworks uncovers patterns of emphasis, areas of broad coverage, and notable gaps that carry significant implications for the ethical and effective implementation of AI within the EU.

The EU AI Act is a foundational framework for high-risk AI systems, mandating rigorous conformity assessments to verify compliance with ethical and technical standards. This requirement ensures that AI systems undergo thorough evaluation before deployment, thereby mitigating risks to users and society. The Act's emphasis on data integrity further aligns with AI-specific needs by requiring high-quality, error-free data. In addition, its focus on algorithmic transparency addresses one of the most pressing challenges in AI—making decision-making processes explainable to stakeholders. The Act complements these measures with a strong post-market monitoring

mechanism, allowing systems to adapt to emerging risks throughout their lifecycle. Nevertheless, while the Act underscores technical robustness and ethical safeguards, it does not explicitly address interoperability or usability, areas that other frameworks address.

The NIS2 Directive complements the EU AI Act by emphasizing operational resilience, particularly in critical sectors where AI systems are integrated into essential services. By focusing on business continuity and crisis management, the directive ensures that AI-powered operations can withstand disruptions and recover quickly, thus upholding public trust. Moreover, its requirement for continuous risk monitoring promotes proactive identification and mitigation of vulnerabilities. However, the NIS2 Directive does not cover data governance or algorithmic transparency, highlighting the value of a unified approach across multiple frameworks.

GDPR stands as a cornerstone for data protection and privacy in AI systems. Its robust focus on user consent management grants individuals control over their data, fostering transparency and accountability in data-driven AI processes. Additionally, its data minimization and integrity principles align well with AI needs by limiting unnecessary data collection and promoting accurate inputs, both crucial for reducing bias. GDPR also addresses cross-border data flows, ensuring that personal data transferred internationally adheres to stringent EU standards. This global applicability strengthens its complementarity with frameworks such as the EU AI Act and NIS2, which do not explicitly tackle data flows. Although GDPR promotes usability through its user-centric approach, it does not encompass resilience or interoperability, gaps filled by other regulations.

Taken as a whole, the EU's regulatory frameworks address various dimensions of AI governance, with each framework contributing distinct strengths while also displaying certain limitations. The ePrivacy Directive builds on the GDPR by concentrating on user consent mechanisms specifically for electronic communications, thus enhancing usability and trust in AI-driven communication services. Owing to its narrower scope, however, it does not address AI-specific issues such as algorithmic transparency or security-by-design principles, which are covered more comprehensively by the EU AI Act and the CRA.

The CRA bolsters security standards by demanding conformity assessments for digital products, including AI systems. This requirement ensures that products meet predefined cybersecurity benchmarks before market entry, aligning with the need for AI systems to be resilient against evolving threats. Its strong emphasis on security-by-design and resilience is critical for maintaining AI systems' operational integrity, while post-market surveillance mechanisms ensure ongoing security. Nonetheless, the CRA does not address human-centric design or transparency, which are more effectively guided by the Ethics Guidelines for Trustworthy AI and the DSA.

Bridging technical and user-centric requirements, the European EECC precedes interoperability and user consent within telecommunications. These provisions facilitate the seamless operation of AI systems across communication platforms and empower users to manage their data. The EECC 's commitment to business continuity supports the incorporation of AI into critical infrastructure. Still, it does not extend to algorithmic transparency or continuous monitoring—areas addressed by the EU AI Act and the NIS2 Directive. The DSA further refines AI governance by mandating algorithmic transparency for very large online platforms, requiring them to disclose how AI systems affect content recommendations and moderation. This approach strengthens accountability in high-impact applications. The DSA also mandates continuous risk assessments, helping platforms adapt to emerging threats and societal challenges. While it excels in transparency and adaptability, it lacks directives regarding security-by-design or interoperability, covered by the CRA and the DMA.

The DMA complements the DSA by fostering fair competition and interoperability in digital markets. Ensuring that AI systems can integrate smoothly across platforms lowers barriers to innovation and promotes user empowerment. The DMA also requires transparency for gatekeeper platforms, aligning with broader AI governance objectives. However, because it focuses on competition, it does not tackle resilience or continuous monitoring—key considerations addressed by the NIS2 Directive and the CRA. Meanwhile, the

Ethics Guidelines for Trustworthy AI offer a non-binding yet influential framework for ethical AI deployment. Emphasizing user consent, data minimization, and security-by-design, they closely mirror the aims of the GDPR and the EU AI Act. Their attention to usability and human-centric design ensures that AI systems remain accessible and fair, complementing the technical scope of other frameworks. However, their non-enforceable nature limits their impact, underscoring the need for integration with binding regulations.

Sector-specific frameworks, such as DORA and the GPSR, address operational resilience and safety-by-design within the financial sector and general product safety, respectively. DORA ensures that AI systems can remain functional during crises, aligning with the need for adaptability in high-stakes environments. However, it does not account for broader AI-focused concerns such as transparency or data governance, which are better covered by GDPR and the EU AI Act. Likewise, GPSR mandates conformity assessments and post-market surveillance to uphold safety standards throughout the product lifecycle, yet it does not address AI-specific considerations like algorithmic transparency or usability, which remain crucial for building trust in AI.

In healthcare, the EHDS underscores data minimization, user consent, and interoperability for health-related AI systems. These provisions ensure that shared health data is secure, accurate, and accessible, supporting broader goals of human-centric design. However, EHDS does not enforce continuous monitoring or transparency, leaving those gaps to be filled by complementary frameworks. Lastly, the Open Data Directive promotes accessibility and interoperability for public data, allowing AI systems to benefit from machine-readable and reusable datasets. Although its emphasis on usability aligns with the goals of GDPR and the Ethics Guidelines, it does not address security, transparency, or resilience, which are critical for the safe deployment of AI.

The analysis of Table 2 illustrates that, although many regulatory frameworks overlap in covering specific functional requirements, gaps persist in domains such as conformity assessments, algorithmic transparency, and continuous monitoring, particularly outside the scope of the EU AI Act and the CRA. This finding underscores the need for more comprehensive regulatory measures or enhanced coordination among existing frameworks to ensure uniform coverage of critical functional requirements across sectors. Notably, the consistent absence of algorithmic transparency and continuous monitoring provisions in frameworks other than the EU AI Act, DSA, and DMA suggests that these elements are not sufficiently integrated into regulations governing sectors that increasingly rely on AI. Given the role of transparency in fostering accountability and trust, this gap could have considerable consequences for the ethical deployment of AI technologies. Furthermore, although user consent management and data minimization are thoroughly addressed in GDPR and the ePrivacy Directive, their absence in other frameworks highlights potential vulnerabilities in protecting user data, mainly when AI systems handle personal data without explicit user interaction.

This analysis reveals the strengths and limitations of the EU's regulatory approach to AI. While the EU AI Act is a central pillar addressing many critical functional elements, other frameworks must incorporate additional requirements to support a robust, integrated governance structure. Enhancing interoperability across frameworks and closing the identified gaps will be essential to promoting AI systems that are functionally robust, ethically sound, and aligned with societal values. The comparison of functional requirements reveals not only which frameworks address each obligation but also how these obligations intersect in practice. For example, conformity assessments under the AI Act and CRA are both pre-deployment safeguards that require coordination in the case of embedded AI systems. Business continuity and crisis management appear in NIS2 and DORA with different emphases—organizational resilience versus financial risk mitigation—but functionally overlap in requiring fault-tolerant design. Meanwhile, data minimization and consent under GDPR complement algorithmic transparency under the DSA and AI Act, facilitating both legal compliance and user autonomy. Such interdependencies highlight the importance of regulatory alignment to avoid contradictory obligations or gaps in protection.

3.3 Non-Functional Requirements

The non-functional requirements articulated in the EU's regulatory frameworks for AI and digital systems underscore the overarching qualities that ensure these technologies function ethically, reliably, and sustainably across diverse sectors. In contrast to functional requirements, which specify particular tasks or capabilities, non-functional requirements address higher-level principles that guide AI in meeting societal expectations, maintaining reliability, and upholding stakeholder trust. Foremost among these is *Transparency and Explainability*, which make AI systems interpretable and accountable. Transparency and Explainability are addressed in multiple instruments. Articles 13 and 52 of the EU AI Act require providers of high-risk AI systems to inform users of system capabilities, limitations, and the logic behind outputs, supporting user understanding and accountability. The Digital Services Act (Article 27) mandates that platforms explain recommender systems and content moderation processes, while Article 12 of the GDPR ensures data subjects are informed about automated processing, including meaningful information about logic and consequences. These layered provisions establish a strong legal foundation for system interpretability and public trust. As AI algorithms become more intricate, especially in critical areas such as healthcare, finance, and law enforcement, the ability of users, developers, and regulators to understand decision-making processes becomes indispensable. This emphasis aligns with regulatory demands for algorithmic transparency, as articulated in the EU AI Act and related frameworks, reflecting broader user trust and fairness objectives.

Equally vital is *Resilience and Reliability*, underscoring the need for AI systems to sustain functionality under adverse conditions, including cybersecurity attacks or operational disruptions. This requirement draws on instruments like the NIS2 Directive and the CRA, highlighting the importance of continual operation in essential sectors and advocating robust designs to counter evolving threats. Closely related is *Security and Adaptability*, addressing the fluid nature of risks that AI systems confront in real-world settings. Maintaining secure-by-design approaches and adaptive safeguards is essential for preserving operational integrity and user protection, reflecting principles prioritizing proactive risk identification and mitigation.

Furthermore, *Privacy Protection and User Rights* form core tenets derived from the GDPR and the ePrivacy Directive, underscoring the necessity of safeguarding personal data and granting individuals meaningful control over interactions with AI systems. Incorporating these requirements ensures that AI technologies uphold ethical standards in data usage, thus bolstering public trust and supporting legal compliance. Additionally, *User Safety* is a non-negotiable requirement arising from the need to protect individuals from potentially harmful or unethical AI systems, whether these risks are physical (e.g., autonomous vehicles) or social (e.g., AI-driven online platforms). Regulatory measures such as the EU AI Act explicitly prioritize user safety, positioning it as a foundational element of non-functional requirements.

In parallel, *Fair Competition and Market Transparency* ensure that AI technologies operate within a framework that fosters innovation, prevents monopolistic behavior, and maintains accountability in digital marketplaces. Instruments such as the DMA highlight the value of equitable competition, particularly in environments dominated by a limited number of influential actors, thereby supporting a robust digital ecosystem through interoperability and transparent market practices. Finally, *Ethical Alignment* entails embedding societal values, fairness, and inclusivity in AI systems, as reflected in the Ethics Guidelines for Trustworthy AI and the EU AI Act. By minimizing biases and encouraging inclusivity, ethical alignment reinforces the fundamental ethos upon which AI governance is based.

Together, these requirements target the non-functional dimensions integral to sound AI governance. They emerge from converging regulatory directives, ethical imperatives, and practical considerations, collectively forming a coherent framework to ensure that AI systems function efficiently and responsibly. By incorporating these non-functional requirements, stakeholders can advance AI systems that are trustworthy, resilient, and congruent with societal values.

An analysis of non-functional requirements across various EU regulatory frameworks, as shown in Table 3, reveals how these instruments

Table 3 Evaluation of frameworks against non-functional requirements

	AI Act	NIS2	GDPR	ePrivacy Directive	CRA	EECC	DSA	DMA	Ethics Guidelines	DORA	GPSR	EHDS	Open Data Directive
Transparency & Explainability	•		•				•	•	•				
Resilience & Reliability		•			•	•				•	•		
Privacy Protection & User Rights			•	•					•			•	
Security & Adaptability	•	•	•		•				•	•	•	•	
User Safety	•		•	•	•		•		•		•		
Fair Competition & Market Transparency						•		•					•
Ethical Alignment	•						•	•	•			•	

collectively address core non-functional priorities for AI systems. Each requirement constitutes a vital characteristic for ensuring AI operates ethically, reliably, and in line with societal standards. By reviewing the degree to which each framework incorporates these attributes, one can discern the complementarity and the gaps in the existing regulatory environment. The discussion below elucidates the unique contributions of specific frameworks while emphasizing their interconnectedness and overall impact.

The EU AI Act is a principal framework for several critical non-functional requirements. Its emphasis on Transparency and Explainability bolsters accountability and user trust, particularly in high-risk AI applications. The Act also addresses Security and Adaptability through stipulations that require robust mechanisms to mitigate threats. By mandating these characteristics, the EU AI Act underscores the importance of User Safety and Ethical Alignment, especially in applications where failure could yield profound social consequences. Nevertheless, the Act does not explicitly tackle operational Resilience and Reliability, focusing instead on system robustness and lifecycle monitoring. The NIS2 Directive complements the EU AI Act by emphasizing Resilience and Reliability, particularly in essential services. By ensuring that AI applications embedded in critical infrastructure can sustain operations in unfavorable circumstances, NIS2 addresses a critical dimension absent in frameworks that concentrate on individual system security. Its focus on Security and Adaptability likewise bolsters resilience in the face of rapidly evolving cybersecurity threats. However, the directive does not explicitly confront transparency, privacy, or ethical concerns, reflecting its narrower remit centered on operational continuity rather than broader social values.

The GDPR is paramount in protecting Privacy and User Rights, granting individuals control over their personal data and mandating data minimization. These principles reinforce user trust in data-based decisions, supported by an insistence on Transparency and Explainability. While the regulation partly addresses Security and Adaptability by advocating data protection by design, it does not comprehensively tackle resilience or market competition. The ePrivacy Directive, in turn, expands upon GDPR 's focus on Privacy Protection and User Rights in electronic communications. It also fosters User Safety by safeguarding sensitive communication data. However, its domain remains limited to communication services, leaving transparency, resilience, and adaptability considerations to be handled by other frameworks.

The CRA prioritizes Resilience and Reliability and Security and Adaptability, ensuring robust AI systems and digital products that can withstand emergent threats. Its support for secure-by-design methodologies and post-market oversight illustrates a preemptive stance on vulnerabilities. In addition, the Act emphasizes User Safety, aiming to mitigate physical and digital harm. Nonetheless, it adopts a technical perspective, offering less coverage of broader societal values such as transparency, privacy, and ethical alignment. The EECC excels in stressing Resilience and Reliability within communication networks. It supports

a cohesive digital ecosystem by assuring the continued operation and interoperability of AI-based communication services. Its provisions concerning Privacy Protection and User Rights, as well as Fair Competition and Market Transparency, further amplify user empowerment and fair market conditions. That said, the EECC does not directly address explainability or security, deferring these concerns to regulations like the EU AI Act and CRA.

Collectively, the DSA and DMA aim to enhance transparency and equity in the digital space. The DSA 's focus on Transparency and Explainability enforces accountability for large platforms employing AI-driven processes, especially for content moderation and recommendation systems. It also underscores User Safety by targeting harmful content. Meanwhile, the DMA addresses Fair Competition and Market Transparency, preventing dominant platforms from curbing innovation or user choice. Both acts align with Ethical Alignment, advocating responsible practices in their domains, though they do not explicitly deal with resilience or adaptability, which are essential for operational robustness.

The Ethics Guidelines for Trustworthy AI provide a valuable, albeit non-binding, perspective on non-functional requirements by advocating Transparency and Explainability, Ethical Alignment, and User Safety. Their endorsement of Privacy Protection and User Rights, alongside Security and Adaptability, underscores a holistic approach to responsible AI. However, these guidelines remain voluntary and rely on integration with binding measures such as the EU AI Act and the GDPR to ensure enforcement. Frameworks like DORA and the GPSR are primarily concerned with resilience and safety. DORA underscores Resilience and Reliability and Security and Adaptability within the financial sector, while GPSR enforces stringent safety requirements to guarantee product reliability. Both frameworks, however, have sector-specific scopes and do not address broader mandates such as transparency or ethical alignment.

The EHDS and the Open Data Directive occupy particular niches. The EHDS focuses on secure, interoperable health data sharing, promoting Privacy Protection and User Rights alongside Ethical Alignment. Conversely, the Open Data Directive emphasizes Fair Competition and Market Transparency by ensuring open access to public data. Neither framework, however, explicitly addresses resilience, safety, or adaptability, highlighting the targeted nature of their regulatory objectives.

A prominent theme in this analysis is the domain-specific concentration of each framework, which collectively offers wide-ranging but sometimes disjointed coverage of non-functional requirements. While overarching instruments such as the EU AI Act and the Ethics Guidelines address multiple domains, specialized frameworks provide depth in areas such as operational security (NIS2, CRA) or data protection (GDPR, ePrivacy Directive). One advantage of this approach is that key requirements, including transparency, security, user safety, and ethical alignment, are referenced in multiple frameworks, suggesting a robust EU commitment to these priorities. This overlap also ensures gaps in one framework may be partly addressed by another.

Nevertheless, inconsistencies remain. Resilience and reliability, for instance, receive heightened attention in finance (DORA) and communications (EECC), but are less emphasized elsewhere. Fair competition and market transparency, primarily regulated by the DMA and EECC, are less prominent in other AI-influenced sectors. Moreover, while ethical alignment appears in guidance (the Ethics Guidelines) and some binding legislation, its incorporation in many regulatory texts is neither extensive nor mandatory. Strengthening ethical oversight in binding frameworks such as the EU AI Act, GDPR, or relevant sector-specific regulations could fortify AI governance.

Additionally, the level of user-centric provisions varies across frameworks. Privacy protection and user rights feature strongly in the GDPR and the ePrivacy Directive but receive less attention in instruments such as NIS2 and CRA. A more uniform emphasis on user rights and safety could bolster trust in AI systems. In conclusion, the EU has made notable progress in defining requirements for trustworthy AI, yet greater coherence and synergy among regulatory frameworks are advisable. By identifying and bridging existing gaps and ensuring consistent promotion of critical non-functional requirements, the EU can reinforce its leadership in ethical AI governance, driving

the development of AI solutions that are not only innovative but also aligned with public values and expectations. Non-functional requirements often rely on implicit or explicit interactions across regulatory frameworks. For example, while algorithmic transparency is a core requirement of the EU AI Act and DSA, its practical enforceability is shaped by GDPR's rules on user access to information about automated processing. Similarly, resilience and adaptability provisions in NIS2 and CRA depend on security-by-design mechanisms already established in the AI Act and GPSR. Ethical alignment, while framed in soft-law instruments like the Ethics Guidelines, finds legal grounding in binding commitments to fairness, human oversight, and accountability across multiple instruments. These interlinkages illustrate that effective AI governance requires not only individual compliance but also structural coherence across legal regimes.

3.4 Regulatory Frameworks

Although the EU's existing regulatory instruments, such as the AI Act, GDPR, NIS2, and DSA, address a broad range of AI applications, the rapid growth of emerging technologies, including generative AI and advanced machine learning approaches, presents new challenges. Generative AI models can create highly realistic text, images, or voice outputs, raising concerns about misinformation, identity theft, and violation of intellectual property rights that the current risk categories do not explicitly cover. Similarly, advanced reinforcement learning systems can exhibit unpredictable behaviors, making it challenging to ensure compliance with existing safety and transparency requirements.

In light of these developments, existing frameworks may need to adopt more dynamic and adaptive strategies. First, expanding the risk-based classification in the EU AI Act to include special considerations for generative AI models would enable regulators to address novel threats such as synthetic data misuse or large-scale content manipulation. Second, regulators might require developers of generative models to document training datasets and model architecture details to support algorithmic transparency without divulging proprietary information. This would encourage explainable AI practices and enhance accountability for model outcomes.

Furthermore, ensuring adequate cybersecurity protections for advanced models calls for closer alignment between the NIS2 Directive and guidelines on AI lifecycle management. AI developers could be required to conduct more frequent security audits, given the potential for adversarial attacks on large-scale neural networks. In parallel, refining the GDPR to clarify data handling protocols in generative AI contexts, particularly where synthetic personal data could emerge, would bolster privacy safeguards. Finally, continual refinements to the DSA and DMA may be warranted to address the market and content moderation implications of generative AI, such as labeling obligations for synthetic media or constraints on platforms that distribute large volumes of generated content.

Preparing for the next wave of AI innovations entails proactive monitoring of technological advancements and iterative updates to regulatory texts. Creating flexible, future-proof guidelines, potentially supported by stakeholder consultations, regulatory sandboxes, and international collaboration, would help ensure that emerging AI systems remain aligned with ethical imperatives, data protection requirements, and security best practices. Such measures will be crucial for maintaining trust, promoting responsible innovation, and enabling the EU to adapt effectively to ongoing technological evolution.

4 Implementation Strategies and Enforcement Mechanisms/Regulations

The effective implementation and enforcement of the EU's regulatory frameworks for AI can be understood not merely as institutional oversight but also as a matter of systemic design. Recent interdisciplinary work has proposed that enforcement mechanisms themselves can be conceptualized as *legal design patterns*; reusable governance templates that embed core legal principles such as contestability, transparency, and explainability into the architecture of digital systems [9, 34].

These patterns operationalize the Rule of Law by aligning procedural fairness with technical infrastructures, ensuring that legal norms

are not imposed externally but are instantiated from within. For example, the ability to contest automated decisions in high-risk AI systems—mandated under the EU AI Act—can be seen as a manifestation of a design pattern that structurally enables user redress, oversight, and due process.

Central to this endeavor are the national supervisory authorities and the European Artificial Intelligence Board (EAIB), pivotal in monitoring compliance and offering guidance on interpreting regulations such as the AI Act and the GDPR. The EAIB plays a critical role in harmonizing the interpretation and application of the AI Act across Member States. It issues guidelines, coordinates enforcement practices, and mediates disagreements between national authorities. Moreover, the EAIB functions as a hub for cross-border risk assessment, enabling the sharing of threat intelligence, audit findings, and systemic concerns. Its mandate also includes providing opinions on the designation of high-risk AI systems and advising the European Commission on regulatory updates based on technological evolution. In this capacity, the EAIB is positioned not only as a compliance facilitator but also as a strategic actor guiding long-term governance coherence.

National supervisory authorities, meanwhile, are responsible for monitoring conformity at the Member State level. Their roles include conducting audits, investigating breaches, overseeing post-market monitoring obligations, and applying corrective measures or sanctions. These authorities are also expected to engage in capacity-building efforts, such as developing sector-specific compliance templates or partnering with academia and industry to address skills gaps in AI oversight. Notified bodies serve as independent entities authorized to conduct conformity assessments, examining technical documentation, risk management systems, and compliance with transparency and fairness obligations. Their ability to interpret legal standards in context and issue meaningful assessments is essential to the legitimacy of the compliance architecture.

In this model, conformity assessments, incident reporting, algorithmic transparency, and lifecycle monitoring are not isolated mandates but instantiations of deeper normative commitments embedded into system design. Compliance processes revolve around rigorous conformity assessments, particularly for high-risk AI systems. Organizations must undergo pre-deployment evaluations that confirm adherence to technical standards and ethical principles, often involving third-party audits or certifications. These assessments encompass data quality, algorithmic transparency, risk management systems, and security measures. Emphasizing security-by-design and continuous monitoring, the EU's frameworks compel companies to integrate compliance considerations throughout the AI system lifecycle. Incident reporting mechanisms are also mandated, requiring organizations to promptly inform authorities of any security breaches or system malfunctions, enabling swift remedial measures and bolstering overall system resilience.

To support these implementation strategies, the EU provides various resources and mechanisms that facilitate compliance. Documents such as the "Ethics Guidelines for Trustworthy AI" offer practical guidance on embedding ethical principles into AI development. Regulatory sandboxes enable organizations to test AI innovations under supervisory oversight, fostering innovation while ensuring conformity with legal requirements. In addition, capacity-building initiatives address the shortage of AI compliance expertise through specialized training programs, collaborations between industry and academia, and the development of standardized tools for compliance management. Technological solutions, such as automated compliance monitoring systems and data governance platforms, are increasingly employed to streamline these processes and lessen the operational burden on organizations. To support these implementation strategies, targeted policy tools such as regulatory sandboxes, compliance automation, and inter-institutional coordination platforms are recommended. These mechanisms can lower the compliance burden for smaller organizations while improving enforcement responsiveness and scalability across Member States.

Despite these measures, obstacles persist in implementing and enforcing AI regulations. Organizations, particularly small and medium-sized enterprises (SMEs), often face substantial financial and technical constraints in meeting compliance obligations. The complexity and rapid evolution of AI technologies can surpass the scope of existing regulatory frameworks, creating potential

gaps in enforcement and oversight. Furthermore, the intricacy of AI systems complicates compliance assessments, necessitating ongoing dialogue and cooperation between regulatory agencies and industry experts. Embedding enforcement patterns directly into system design could help mitigate such challenges by automating aspects of oversight and reducing the interpretive burden on regulators and auditors [35]. Tackling these challenges calls for a dynamic and adaptive regulatory approach that balances strict enforcement with encouraging innovation and competitiveness within the EU's digital economy.

5 Implications, Challenges, and Future Directions

The EU's comprehensive regulatory landscape for AI governance carries wide-ranging implications for businesses, consumers, and the global digital ecosystem. For businesses operating within the EU, these regulations entail stringent compliance obligations that can substantially shape operational processes and strategies. Although large corporations may have the resources to manage these obligations, SMEs frequently face financial and technical hurdles that could impede innovation and market entry. Nevertheless, adherence to these regulations can offer a competitive edge by strengthening consumer trust, bolstering data security, and aligning with the expanding international focus on ethical AI practices. Organizations that navigate these obligations effectively can be leaders in responsible AI deployment, differentiating their products and services in an increasingly scrutinized marketplace.

Consumers benefit through stronger data privacy, security, and safeguards for their rights in AI interactions. Emphasis on transparency and user empowerment fosters trust and supports more informed decisions about how personal data is collected and processed. At the same time, the technical complexity of AI systems and their regulatory frameworks may limit how readily consumers understand and exercise these protections. Consequently, ongoing efforts to enhance public awareness and digital literacy remain crucial for ensuring that individuals can use their rights meaningfully, translating formal protections into tangible benefits.

On a global scale, the EU's approach has a substantial impact, often called the "Brussels Effect", whereby multinational firms adopt EU standards globally to streamline operations. This dynamic can stimulate broader convergence in AI governance but may also raise questions about reconciling divergent regional requirements and avoiding regulatory fragmentation. As AI technologies evolve rapidly, policymakers must craft flexible frameworks that accommodate emerging techniques like generative AI while preserving space for experimentation and market competitiveness. Overly restrictive regulations risk stifling innovation, whereas lax oversight could undermine public trust and foster harmful uses of AI. While the EU's regulatory model has been widely recognized as a global standard-setter—a phenomenon often described as the "Brussels Effect" [27]—its continued influence is increasingly subject to geopolitical and economic constraints. Recent scholarship and policy discourse suggest that other jurisdictions are selectively adopting, adapting, or even resisting EU norms based on local strategic priorities, industrial policy, and sovereignty concerns. For example, the United States has shown an interest in aligning with European AI values in certain contexts (e.g., algorithmic fairness), while maintaining a decentralized, sector-specific approach to regulation. Meanwhile, major AI actors in Asia often prioritize national innovation ecosystems and data sovereignty, complicating the extraterritorial effect of EU rules. These dynamics suggest that the Brussels Effect should now be understood as a more contingent and negotiated phenomenon, rather than an automatic consequence of EU regulatory design.

Nevertheless, replicating or adapting the EU's model beyond Europe presents opportunities and obstacles. The United States, for instance, maintains a fragmented legal landscape where sector-specific legislation (e.g., finance, healthcare) might selectively integrate EU-aligned AI standards without adopting a comprehensive federal framework. In Asia, leading AI hubs such as China and Singapore often prioritize economic growth, national security, and innovation—objectives that may diverge from the EU's primary emphasis on personal privacy and ethical oversight. Despite these differences, there is growing recognition worldwide that AI regulation requires more global coordination to address

inherently cross-border issues like data flows and algorithmic risks.

Despite these regional differences, there is growing consensus on the need for international cooperation to address cross-border challenges inherent in AI governance. Building on the preceding analysis of EU regulatory frameworks, two areas emerge as particularly promising for international coordination: (1) algorithmic transparency and (2) cross-border data flow governance. These areas correspond directly to some of the most structurally pervasive and operationally sensitive requirements observed across EU instruments. Transparency obligations are embedded in the AI Act, GDPR, and DSA, while data flow governance is essential to the cross-border applicability of GDPR, the Open Data Directive, and AI deployment in distributed computing environments. Their prominence and complexity make them ideal candidates for harmonization, as they frequently generate compliance friction in global settings.

1. **Algorithmic Transparency.** Building on existing EU initiatives, international standards bodies could develop consistent guidelines for transparency reporting and impact assessments. A shared taxonomy for identifying and documenting algorithmic bias would facilitate comparability and accountability across jurisdictions.
2. **Cross-Border Data Flow Governance.** Given the dependency of AI systems on global datasets, a multilateral framework for secure and lawful data transfers, potentially under OECD or G20 coordination, could align encryption, consent, and breach notification standards, mitigating regulatory fragmentation.

Achieving such international cooperation requires balancing divergent policy priorities and legal norms. Mechanisms such as regulatory sandboxes, joint research endeavors, and cross-border compliance certifications can foster incremental alignment and mutual learning. Furthermore, ethical considerations, including the mitigation of algorithmic bias, prevention of discriminatory outcomes, and protection of jobs impacted by automation, underscore the broader societal values at stake. Addressing these issues calls for a blend of robust regulatory instruments and proactive ethical frameworks, together with broad stakeholder engagement.

In summary, the EU's regulatory architecture provides a compelling exemplar of comprehensive AI governance that integrates privacy, security, and accountability. Whether this model can be fully replicated elsewhere hinges on reconciling region-specific policy agendas and market conditions. Still, the guiding principles of transparency, user safety, and responsible innovation resonate globally. By collaborating on shared challenges such as algorithmic transparency and cross-border data flows, the international community can move toward a more harmonized and forward-looking AI governance paradigm that preserves public trust and safeguards fundamental rights.

6 Conclusions

The analysis presented in this paper illustrates how aligning multiple EU regulatory frameworks, ranging from the AI Act and GDPR to NIS2, CRA, and DSA, can advance AI governance by reducing fragmentation and harmonizing requirements across diverse sectors. By examining security, functional, and non-functional requirements, we pinpointed complementary provisions that strengthen transparency, accountability, and resilience in high-risk AI applications. This synthesis addresses prevailing compliance gaps and clarifies how organizations can integrate essential principles like data minimization, user oversight, and fairness into AI lifecycle management.

On a broader scale, our proposed integrated approach underscores the growing significance of ethical alignment in AI development. By consolidating technical and ethical priorities across regulations, the EU can foster an environment conducive to responsible innovation while bolstering user trust. These insights guide policymakers and industry practitioners, highlighting where cross-framework synergies can mitigate compliance burdens, support secure data governance, and ensure equitable access to AI solutions. Our findings reinforce the EU's role as a global trailblazer in ethical and trustworthy AI, offering a cohesive governance model adaptable to rapid technological changes.

Acknowledgments

This research has received funding from European Commission's Horizon Europe research and innovation programs under grant agreements No. 101139031 (SAFE-6G), No. 101095634 (ENTRUST), and No. 101120962 (RESCALE).

References

[1] Deloitte: AI Adoption in the Enterprise (2018)

[2] Cath, C., *et al.*: Artificial intelligence and the 'good society': the US, EU, and UK approach. Science and Engineering Ethics **24**(2), 505–528 (2018)

[3] Goodman, B., Flaxman, S.: EU regulations on algorithmic decision-making and a 'right to explanation'. AI Magazine **38**(3), 50–57 (2017)

[4] O'neil, C.: Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy. Crown, New York (2017)

[5] Commission, E.: White Paper on Artificial Intelligence: A European approach to excellence and trust (2020)

[6] Jobin, A., Ienca, M., Vayena, E.: The global landscape of AI ethics guidelines. Nature Machine Intelligence **1**(9), 389–399 (2019)

[7] Winfield, A.F.T., Jirotka, M.: Ethical governance is essential to building trust in robotics and AI systems. Philosophical Transactions of the Royal Society A **376**(2133), 20180085 (2019)

[8] Koulu, R., Pohle, J.: Legal design patterns: New tools for analysis and translations between law and technology. Digital Society (2024)

[9] Diver, L.: Using design patterns to build and maintain the rule of law. Digital Society (2024). Special Issue on Legal Design Patterns

[10] Brynjolfsson, E., Mcafee, A.: The business of artificial intelligence. Harvard business review **7**(1) (2017)

[11] Commission, E.: Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics (2020)

[12] Smuha, N.A.: From a 'race to AI' to a 'race to AI regulation': Regulatory competition for artificial intelligence. Law, Innovation and Technology **13**(1), 57–84 (2021)

[13] Butcher, J., Beridze, I.: What is the state of artificial intelligence governance globally? RUSI Journal **166**(5-6), 88–99 (2021)

[14] Bommasani, R., et al.: On the Opportunities and Risks of Foundation Models. arXiv preprint arXiv:2108.07258 (2021)

[15] Commission, E.: Proposal for a Regulation laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) (2021)

[16] EU: Regulation (EU) 2016/679 (General Data Protection Regulation) (2016)

[17] EU: Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (ePrivacy Directive) (2002)

[18] Veale, M., Zuiderveen Borgesius, F.J.: Demystifying the draft EU Artificial Intelligence Act. Computer Law Review International **22**(4), 97–112 (2021)

[19] Floridi, L.: The European legislation on AI: A brief analysis of its philosophical approach. Philosophy & Technology **35**(4), 843–848 (2022)

[20] Commission, E.: Proposal for a Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive) (2020)

[21] Commission, E.: Proposal for a Regulation on horizontal cybersecurity requirements for products with digital elements (Cyber

Resilience Act) (2022)

[22] EU: Directive (EU) 2018/1972 establishing the European Electronic Communications Code (2018)

[23] Commission, E.: Proposal for a Regulation on a Single Market for Digital Services (Digital Services Act) (2020)

[24] Commission, E.: Proposal for a Regulation on contestable and fair markets in the digital sector (Digital Markets Act) (2020)

[25] Artificial Intelligence, H.-L.E.G.: Ethics Guidelines for Trustworthy AI. European Commission (2019)

[26] Anagnostou, D., *et al.*: Artificial Intelligence for Europe: The EU Commission's proposal for a legal framework. Computer Law Review International **21**(6), 153–159 (2020)

[27] Bradford, A.: The Brussels Effect: How the EU Rules the World. Oxford University Press, Oxford (2020)

[28] Sartor, G., Lagioia, F.: The impact of the EU AI regulation on business models in the AI ecosystem. International Journal of Law and Information Technology **30**(1), 1–28 (2022)

[29] Leslie, D.: Understanding artificial intelligence ethics and safety: A guide for the responsible design and implementation of AI systems in the public sector. The Alan Turing Institute (2019)

[30] Wischmeyer, T., Rademacher, T. (eds.): Regulating Artificial Intelligence. Springer, Cham (2020)

[31] Aloisi, A., DeStefano, V.: Regulating algorithmic management in digital platforms: The use of AI in employment. International Labour Review **161**(1), 47–69 (2022)

[32] Service, E.P.R.: Artificial intelligence act: The EU's approach to AI regulation. Briefing PE 698.792, European Parliament (2022)

[33] MacCarthy, M.: AI regulation: How the US can learn from Europe. Brookings Institution Report (2022)

[34] Söderlund, J., Larsson, S.: Enforcement design patterns in eu law: An analysis of the ai act. Digital Society (2024)

[35] Hakkarainen, L., Santuber, J.: Come in and see: Translating a design pattern from the courtroom into an online environment. Digital Society (2024)