European Cybersecurity and AI Framework: Towards Proactive Regulation for a Secure Digital Future

Céline Gauthier-Maxence

European Cybersecurity and AI Framework:

Towards Proactive Regulation for a Secure Digital Future

Abstract:

This legal article explores the growing challenges of cybersecurity and artificial intelligence (AI) in the age of digital transformation. As the number of connected objects and the value of AI grow exponentially, so do the risks of cyber-attacks and technological abuse. Faced with this, the European Union (EU) is putting in place a rigorous regulatory framework, with directives and regulations such as the Cybersecurity Act, the NIS 2 Directive, DORA and the AI Act. These texts aim to secure networks, strengthen the resilience of financial systems, and frame the use of AI according to the associated levels of risk, while ensuring the protection of fundamental rights. The article also shows how these regulations are forcing companies to adapt, with strict technical and organizational measures, including vendor monitoring and rapid reporting of security incidents. At the same time, it stresses the importance of principles such as "by-design", which requires security and compliance to be integrated right from the system design stage. The article anticipates future challenges, where cyberthreats will become more sophisticated with the increased use of AI, requiring dynamic regulation and proactive risk management practices.

Keywords: Cybersecurity; European regulation; artificial intelligence; by-design; digital risks; compliance

Author: Céline Gauthier-Maxence[1]

Introduction

Today, we evolve in a society where the number of connected devices is growing exponentially, reaching 1.8 billion in Europe.[2] In correlation, cybersecurity risks are multiplying. Since 2015, the annual global cost of cybercrime is estimated to have doubled, reaching €5.5 trillion by 2020.[3] The global market for artificial intelligence (AI) is already worth over $196 billion. And some experts in the field predict that the value of AI is set to increase 13-fold over the next 7 years, topping $1.81 trillion by 2030. Artificial intelligence is therefore expected to grow by 38.1% between 2022 and 2030.[4] In view of these facts, the legislative framework for cybersecurity and AI is essential to secure the data used in these fields and prevent potential abuses.[5] In this sense, European directives and regulations on cybersecurity and artificial intelligence play a crucial role in securing digital infrastructures and overseeing the use of emerging technologies (I). The rise of new digital technologies and the use of AI in ever wider fields means that the issues at stake are not only current, but will continue to be so in the future. It is vital to anticipate these challenges in both the short and long term (II).

I. Cybersecurity and AI: The State of European Regulation

The European Union has introduced a number of legislative texts aimed at strengthening cybersecurity, including the Cybersecurity Act, the NIS Directive and the forthcoming NIS 2 Directive, as well as the REC Directive, the DORA Regulation, and the Digital Services Act and Digital Markets Act (A). The AI Act extends regulation to AI technologies and the services and organisations that use them (B).

A. European Cybersecurity Regulations

The European Union has developed a robust regulatory framework to enhance cybersecurity, operational resilience, and digital market governance across critical sectors. Three pivotal components have to be examined: the Cybersecurity Act, which establishes a certification framework for ICT products and services (1), the NIS and NIS2 Directives, which strengthen security measures for essential services and critical entities (2), and the DORA Regulation alongside the Digital Acts, which bolster digital resilience in the financial sector and regulate large online platforms (3). Together, these initiatives aim to secure digital ecosystems, protect vital services, and promote fair competition within the EU.

1. Cybersecurity Act

Regulation (EU) 2019/881 (Cybersecurity Act)[6] establishes a European certification framework for ICT (Information and Communication Technology) products. The European Union Cybersecurity Agency (ENISA) is responsible for implementing this framework and evaluating its effectiveness every five years. Implementing Regulation (EU) 2024/482, adopted in January 2024,[7] clarifies standards for the assessment and certification of ICT products according to 'substantial' or 'high' levels of assurance. More specifically, this regulation is aimed at companies that design, develop and sell information and communication technologies (ICT). This includes hardware manufacturers, software publishers and ICT service providers. Member States must designate national certification bodies to assess and monitor ICT products, in line with the European Cybersecurity Certification Framework. The Cybersecurity Act establishes a European certification framework for ICT products. This framework is mainly voluntary, but some certification schemes may become mandatory for certain critical sectors or products. For example, ICT products used in sectors such as critical infrastructure (transport, energy) may be subject to more stringent requirements. ICT products can be certified to different levels of assurance (low, substantial, high) depending on the risks associated with their use. Companies must therefore ensure that their products meet the specific requirements of these levels. The regulation has been in force since 27 June 2019, but certain provisions concerning certification became applicable from 28 June 2021. The first certification system (EUCC) will be mandatory from 27 February 2025.

2. The NIS and NIS 2 Directives and their Supplements

Directive (EU) 2016/1148 (NIS Directive) [8] requires Member States to improve the security of networks and information systems for essential services such as energy, transport, and banking. In 2022, the NIS2 Directive[9] was introduced to strengthen and harmonise security standards within the EU. For the time being, the NIS Directive concerns operators of essential services, i.e. companies in critical sectors such as banking, transport infrastructure, energy and healthcare, as well as digital service providers, i.e. online platforms, search engines and cloud computing services. Companies must implement technical and organisational measures to

secure their networks and information systems. They must also report significant security incidents to the competent national authorities. Member States must designate national authorities to monitor compliance with the directive and take action in the event of non-compliance. Companies that fail to comply with the requirements of the NIS or NIS2 Directives are liable to penalties, which vary according to national regulations. The NIS2 Directive, adopted in 2022, strengthens these obligations by imposing enhanced security and stricter incident reporting. The NIS Directive has been in force since May 2018. The NIS2 Directive, adopted in 2022, is expected to come into force gradually, with compliance required by 2024 for most sectors. NIS2 consolidates its predecessor by targeting companies in critical sectors such as energy, transport, healthcare and digital infrastructure. However, it introduces a distinction between essential entities (EE), such as energy suppliers, and important entities (IE), such as postal services or agri-food companies. Covered entities must strengthen their cybersecurity measures, including supply chain risk governance. They are also required to promptly report any major cybersecurity incident to national authorities[10].

The BER Directive[11] is aimed at companies and infrastructures that provide services essential to maintaining the vital functions of society, such as energy, transport and healthcare. This includes critical entities of national and European importance. Critical entities will have to draw up plans to strengthen resilience in the face of physical and cyber threats. This includes setting up infrastructure protection systems, risk management protocols, and regular stress tests. The REC Directive is being implemented in coordination with the NIS2 Directive, ensuring that physical and cyber security are strengthened consistently across the EU. Member States must designate critical entities and transpose the directive into their legislation by October 2024.

3. The DORA Regulation and the Digital Acts

The DORA (Digital Operational Resilience Act) Regulation is also a central piece of digital resilience regulation in the EU. DORA applies primarily to entities in the financial sector, including banks, insurance companies, asset management companies, financial services providers, and crypto-asset companies. Providers of services critical to these entities, such as cloud services, software or infrastructure services, are also covered. The DORA Regulation aims to ensure that EU financial institutions can withstand and respond to IT disruptions, cyber-attacks, and other digital risks. It sets harmonised standards across the EU for ICT risk management. Financial entities must put in place systems to manage ICT-related operational risks, including risk monitoring and mitigation procedures, business continuity plans, and resilience testing. DORA requires financial entities to closely monitor services provided by external providers, such as cloud services. Contractualization and verification obligations are in place to ensure that external providers comply with the same security standards. Companies must report any major incident affecting ICT to the relevant authorities within a defined timeframe. These incidents must be documented and rigorously followed up. DORA was published in the EU's Official Journal in December 2022 and should be applicable from January 2025. Financial entities therefore have time to adapt their systems and procedures before digital resilience obligations are fully implemented. DORA is part of a broader set of measures to strengthen the digital operational resilience of financial institutions, complementing other cybersecurity frameworks such as NIS2. It focuses primarily on ICT risk management and the monitoring of third-party suppliers.

The Digital Services Act (DSA)[12] and the Digital Markets Act (DMA) are also noteworthy. The DSA applies to large online platforms (social networks, online marketplaces, etc.) and aims to regulate digital services. The DMA targets large digital companies, known as gatekeepers, such

as major technology platforms. The DSA imposes strict obligations to protect users against illicit content and enhance the transparency of algorithms, in addition to making platforms responsible for content moderation. As for the DMA, it limits the power of the major platforms by imposing rules to guarantee fair competition and prevent abuse of dominant position. The DSA has applied since February 2024, and the DMA has been in force since 2022, but the first obligations are being applied gradually.

B. European AI Regulations

When it comes to AI, European regulation has recently been structured around Regulation (EU) 2024/1689, also known as the 'AI Act'[13], which came into force on 1 August 2024. It is aimed at companies developing, deploying or using artificial intelligence systems in the European Union. It concerns large companies as well as start-ups and SMEs. Companies that integrate or use AI systems in their operations (e.g. AI for recruitment, medical care) are also concerned. The text is the world's first comprehensive legal framework governing AI and is based on a risk-based approach, classified into four categories. AIs that threaten fundamental rights, such as social rating systems, are totally prohibited, as they fall under 'unacceptable risk'. AI systems used in critical sectors (recruitment, medical diagnostics, security) are subject to strict requirements for transparency, human supervision and risk management, and fall under 'high risk'. Systems such as chatbots, falling under 'specific transparency risk', must inform users that they are interacting with AI. Finally, low-risk AIs, such as video games or spam filters, are not subject to any obligation, but voluntary codes of conduct may be adopted, insofar as they fall under 'minimal risk'. The regulation is accompanied by the establishment of a European AI Office, responsible for overseeing general-purpose AI models, in coordination with competent national authorities. The regulatory framework also includes measures to foster innovation while protecting the fundamental rights of European citizens.

Although it came into force on 1 August 2024, not all its provisions are immediately applicable. Indeed, several deadlines are foreseen depending on the type of risk that AI systems may represent. For example, bans on certain AI systems deemed of 'unacceptable risk' are applicable within six months, while specific obligations for general purpose systems (GPAI) will come into force in 12 months. Other obligations, notably those concerning 'high-risk' systems, will be phased in over a period of up to 36 months.[14] It should also be remembered that, as a regulation, the AI Act applies directly in all Member States without the need for formal transposition into national law, but competent national authorities will need to be designated to oversee its implementation. These authorities will work in coordination with the European Commission's AI Office to ensure compliance with the regulation and manage market surveillance.[15]

These directives and regulations add to existing measures such as the GDPR[16] and complete the European framework for cybersecurity and AI, digital risk management, and critical infrastructure protection. These texts impose strict compliance deadlines and concern a variety of sectors within the EU, with a gradual entry into force until 2025, under penalty of sanctions for States late in transposition or application (*Commission v Belgium*, Case C-543/17[17]; *Commission v Republic of Austria*, Case C-549/18[18]; *Commission v Germany*, Case C-270/07[19]). This consideration of European regulations and future technological developments therefore implies short- and long-term challenges for Member States and organisations subject to these future constraints.

II. Regulatory Developments in Cybersecurity and AI: Immediate and Future Challenges

In the face of rapidly evolving cybersecurity and artificial intelligence regulations, organisations are facing major challenges. We'll look first at the issues looming a year or so ahead (A), then at the outlook for the next ten years and beyond (B), before exploring the example of a practical solution such as 'by-design' to comply with current standards while anticipating the future (C).

A. Challenges Over the Next Year: An Imminent Evolution

EU Member States must transpose the NIS 2 Directive into national law by 17 October 2024. Organisations must also prepare for new risk management and incident reporting obligations. Companies will need to step up staff training and awareness of cyber threats to comply with the enhanced standards. After national transposition, organisations will need to be fully compliant, or face sanctions. This includes implementing robust technical and organisational measures. Indeed, in addition to Member States, the Court of Justice of the European Union has no hesitation in directly sanctioning companies and organisations that fail to comply with European standards (*Fashion ID*, Case C-40/17[20]; *Planet49*, Case C-673/17[21]). Financial entities will also have to draw up plans to comply with the DORA, which will be applicable from 17 January 2025. On that date, the regulation will require a strengthening of digital operational resilience and ICT risk management.

As far as AI is concerned, the AI Act is already in force, and is being applied progressively according to the degree of risk presented by each AI system. The current challenge is therefore to identify the AI systems in use and assess the associated risks, in order to provide a framework for potential future requirements, firstly under the AI Act, and secondly under future AI regulations. Depending on the AI systems they use, organisations therefore have a transition period to comply, ranging from 0 to 36 months from 1 August 2024. They must therefore prepare or directly apply strategies to meet the requirements in terms of transparency, data governance and risk management. This requires engagement with stakeholders. Organisations should already be working with suppliers, customers and regulators to understand the future implications of the regulation and align practices[22]. For organisations using high-risk AI systems, adaptation time is minimal or non-existent. It was necessary to anticipate by preparing the processes that would enable the required certifications to be obtained rapidly, and to set up auditing and ongoing compliance mechanisms. Cross-functional issues can be identified, impacting cybersecurity and AI systems. The coming months are crucial for organisations as they navigate a rapidly changing regulatory landscape. A proactive approach is essential to ensure compliance, minimise risks and take advantage of the opportunities offered by new technologies, while complying with European directives and regulations. In the near future, this means strengthening risk management frameworks to incorporate new regulatory requirements for cybersecurity and AI. It's also about striking a balance between technological innovation and regulatory compliance to maintain competitiveness while respecting ethical and security standards.[23] Finally, it's a question of investing in the human and technological resources needed to meet the challenges, including recruiting specialist talent and upgrading infrastructures. What's more, the regulations to come are not only the result of a desire to regulate the management and conventional use of IT and AI systems, but also of a rise in potential cyber-attacks in the years to come.

B. Challenges for the Next 10 Years and Beyond: Long-Term Developments

Within the next 5 years, cyberattacks are likely to become more sophisticated, exploiting emerging technologies such as AI to bypass defences. Indeed, a 2024 study by Deloitte in collaboration with NASCIO (National Association of State Chief Information Officers) highlights the growing risks of AI-powered cyberattacks.[24] Experts note that AI-enabled attacks are rapidly becoming more sophisticated, notably through the creation of falsified content, the automation of information gathering, and real-time adaptation thanks to reinforcement algorithms. These advances are making attacks more complex to detect and outperforming conventional defences. The report also points out that many cybersecurity managers are struggling to keep up with the speed at which these threats are evolving, and only 35% say they are ready to effectively counter AI-enabled attacks in the next five years.[25] This study joins the findings of other analyses, such as Keeper Security's, which reveals that a large majority of cybersecurity professionals (84%) perceive an increase in AI-driven phishing and smishing attacks, making training campaigns and detection tools increasingly crucial to counter these threats.[26]

Companies will therefore need to invest in advanced security solutions and adopt a proactive approach to risk management. While compliance with the NIS 2 Directive and DORA Regulation will have to be fully achieved for all organisations subject to them, the continuous monitoring of critical infrastructures and increased operational resilience imposed by these directives and regulations will be all the more beneficial to organisations, in a context of increased cyber threats.[27] In addition, new directives could extend cybersecurity obligations to other sectors, including small and medium-sized enterprises (SMEs), increasing the scope of compliance. Looking even further ahead, to around 8 years from now, the massive integration of the Internet of Things (IoT), 5G and 6G will increase the attack surface, requiring adapted regulatory frameworks to secure these technologies. Logic would dictate that the EU work more closely with other international jurisdictions to harmonise cybersecurity standards, leading to adjustments for companies operating on a global scale. The focus would then be on the resilience of systems as a whole, not just on the individual protection of organisations. It's easy to imagine that, within 10 years, cybercriminals' use of AI could automate large-scale attacks, requiring AI-based defences and regulations to frame these new threats. A fortiori, regulatory frameworks will need to be more dynamic to keep pace with the rapid pace of technological innovation, requiring companies to keep a constant regulatory watch and be more flexible.[28]

In terms of AI, within 5 years, the AI Act should also be finalised and adopted. Companies will also have to comply with requirements for AI systems, including transparency, data management and bias prevention. It would also be legitimate for the EU to introduce additional guidelines to ensure the ethical use of AI, obliging organisations to integrate ethical considerations into the development and deployment of their systems. Furthermore, with the development of general AI or strong AI, new regulations could emerge to manage the risks associated with these powerful technologies. Stricter legal frameworks concerning liability for damage caused by AI systems could therefore be put in place, impacting insurance and corporate obligations. Within 10 years, the regulation of AI systems capable of fully autonomous decision-making will become critical, with specific laws to guarantee the safety and ethics of these systems.[29] Intuitively, the EU should then strengthen individuals' rights regarding their data and the impact of AI on their privacy, forcing companies to adopt increasingly stringent data protection measures. Companies will have to innovate while integrating security and compliance principles (‘Security by Design’ and ‘Compliance by Design’) right from the design stage.

C. Compliance in Practice: The Example of 'By-Design', Between Complying with Current Regulations and Anticipating the Future

The concept of 'by-design' refers to the principle of 'compliance by design', which encompasses two notions relating to privacy and security. The GDPR already devotes a specific article to 'privacy-by-design' (GDPR, Art. 25, para. 1). To effectively protect privacy, the European text provides for a non-exhaustive list of mandatory technical and organisational measures to secure personal data right from the processing design stage (GDPR, Art. 32). Technical measures include the pseudonymisation and encryption of data, the principle of minimisation, which limits the amount of data collected according to the purpose of the processing, and the implementation of control procedures to assess the security of the processing, such as penetration tests to identify any security breaches. Organisational measures must also make it possible to limit access to data and to the results obtained by cross-checking data within the company or institution. It is essential to train staff in the challenges of personal data protection and to involve the Data Protection Officer as early as possible in the design of a project. Furthermore, the data controller is obliged to carry out Privacy Impact Assessments in order to map the risks (GDPR, Art. 35). These are all obligations for the company, non-compliance with which exposes it to heavy fines of up to 10 million euros or 2% of the company's worldwide annual sales (GDPR Art. 83, para. 5). This concept of 'by-design' is becoming increasingly popular, and will become an essential standard within the next 5 to 10 years.[30]

Conclusion

Ultimately, the rapid evolution of digital technologies and artificial intelligence means that regulatory frameworks need to be constantly adapted to guarantee security, ethics and data protection. European directives and regulations such as NIS 2, DORA and the AI Act are crucial steps in framing these developments, but their effective implementation will depend on the proactivity of organisations and Member States. The adoption of 'by-design' as a fundamental principle illustrates the need to integrate compliance and security right from the design stage. As we approach an era where AI and ubiquitous connectivity will redefine our societies, it becomes essential not only to comply with current regulations, but also to anticipate future challenges. This raises a fundamental question: are we ready to rethink our traditional approaches to building a digital future that combines innovation, security and ethical responsibility?

References

[1] Céline Gauthier-Maxence is a PhD student in law, specialising in health law and digital law, Université Jean Moulin Lyon 3, Ifross, CRDMS, a research engineer, CNRS, and a teaching assistant, Université Panthéon-Assas, Paris 2.

[2] 'Le monde de l'Internet des objets : des dynamiques à maîtriser', Assessment of the environmental impact of digital technology in France and prospective analysis, study carried out by French ADEME (Agence de la transition écologique) & ARCEP (Autorité de régulation des communications électroniques, des postes et de la distribution de la presse), February 2022.

[3] Virginie Bensoussan-Brulé et al, *Le Data Protection Officer*, 3e ed., Larcier, 2020.

[4] 'Les chiffres clés de l'IA en 2024 : Tendances et statistiques', *Vision IA by ITDM Group*, 12 April 2024.
[5] Céline Gauthier-Maxence, 'Défis juridiques du droit de la santé à l'ère du numérique et de l'IA', 2024, hal-04624585.
[6] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (European Union Agency for cybersecurity) and on cybersecurity certification of information and communication technologies and repealing Regulation (EU) No 526/2013 (Cybersecurity Regulation).
[7] Commission Implementing Regulation (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC).
[8] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.
[9] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).
[10] For more informations: Elio Machado Neto, "Transposing NIS 2: A Blueprint for EU Cybersecurity Harmonisation", published alongside the present article.
[11] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC.
[12]Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act).
[13]Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).
[14] Directorate-General for Communication, 'AI Act enters into force', 1 August 2024.
[15] Mia Hoffmann, 'The Finalized EU Artificial Intelligence Act: Implications and Insights', CSET, 1 August 2024.
[16] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
[17] Judgment of the Court of Justice of 8 July 2019, European Commission v Kingdom of Belgium, C-543/17.
[18] Judgment of the Court of Justice of 16 July 2020, European Commission v Romania, C-549/18.
[19] Judgment of the Court of Justice of 19 March 2009, *Commission of the European Communities v Federal Republic of Germany*, C-270/07.
[20] Judgment of the Court of Justice of 29 July 2019, *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV*, C-40/17.
[21] Judgment of the Court of Justice of 1 October 2019, *Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV v Planet49 GmbH*, C-673/17.
[22] Christina Montgomery and Jean-Marc Leclerc, 'The EU AI Act Is About to Hit the Books: Compliance Steps You Need to Know', IBM, 30 May 2024.
[23] Amanda Lawson, 'The EU AI Act Explained: Tracking Developments for Responsible AI', *Responsible artificial intelligence institute*, 20 December 2022.
[24] Cam Sivesind, 'Deloitte-NASCIO Study: AI and Cyber Threats Reshape the Landscape', *SecureWorld*, 2 October 2024.
[25] Dilki Rathnayake, 'Cybersecurity in the Age of AI: Exploring AI-Generated Cyber Attacks', *FORTRA*, 11 March 2024.
[26]Mike Vizard, 'Survey sees cyberattacks gaining AI sophistication', *Barracuda*, 15 October 2024.
[27] Simon Toepper, 'NIS 2 vs. DORA: Why there are two regulations for IT security in the EU', *IB Academy*, 18 October 2024.
[28] 'NIS 2, AI Act, and more: How the EU's digital strategy is driving the data-driven economy', *Device Insight*, October 17, 2024.
[29]Vlerë Hyseni, 'Securing Europe's Digital Future: DORA and NIS 2 Directive', PECB, 25 April 2024.
[30] Christiane Féral-Schuhl, 'Privacy-by-design, security-by-design, quand la compliance découle du code', CIO, 27 September 2023.