NautaDutilh

Technology and the law in 2024

things you need to know

Intro

In 2024, as in-house counsel, you'll encounter major developments in technology and law that could have a significantly impact on your organisation. Our Information & Communication Technology Group has identified five key areas that will influence your strategies and compliance efforts in 2024.

#1 AI policies and regulation morph into concrete action

#2 Cybersecurity risk coverage and allocation is a major area of attention

#3 IT resilience becomes a statutory requirement for all financial institutions

#4 New EU regulations to ensure fair competition, user security and privacy

#5 eIDAS 2.0 and digital ID become key enablers for secure cross-border transactions

#1

↘

The EU AI Act sets out obligations for providers and users depending on the level of risk posed by artificial intelligence, classifying AI systems into limited risk, high-risk, and unacceptable risk categories.

AI policies and regulation morph into concrete action

In 2024, the first steps in Artificial Intelligence (AI) regulation can be expected, in particular with the anticipated enactment of the European Artificial Intelligence Act (AI Act). Key features of the latest version of the Act are (i) the inclusion of general-purpose AI and foundation models; (ii) exclusions of AI applications in R&D activities from its scope; (iii) clearer definition to exclude simpler software systems; and (iv) clarified requirements for 'high-risk' AI systems, including technical risk management systems, data governance, drawing up technical documentation, informing users and ensuring a human oversight of the system.

Additional recitals to the AI Act reportedly aim to address copyright concerns by referring to the data mining exceptions for scientific research and other purposes provided for by national law, as foreseen in the EU Copyright Directive. The agreed text is expected to establish more balanced sanction limits for SMEs (normally up to EUR 35 million or 7% of the global annual turnover) and introduces a two-year implementation grace period following its publication.

#2

↘

NIS2 provides legal measures to boost the overall level of cybersecurity in the EU. Organisations need to prepare for October 2024, taking into account other EU regulations such as the CRA, which phases in from the end of 2025.

Cybersecurity risk coverage and allocation is a major area of attention

We anticipate the focus on cybersecurity risk coverage and allocation to be a major area of attention in 2024 and beyond. Cybersecurity insurance market coverage is expanding annually, with the development of tailored products increasingly aligning with market demand. In parallel, risk allocation through the negotiation of indemnification, limitation and exclusion of liability clauses warrants careful consideration to ensure the contractual arrangement accurately reflects each party's role. Grasping and understanding risks and exposure is the preliminary step to avoiding uncertainties and unexpected costs related to managing cybersecurity incidents.

EU Member States have until October 2024 to transpose the Network and Information Security Directive (NIS2) into national law. It imposes stricter requirements on a broader range of actors, including mandatory cyber risk management measures and new incident reporting requirements, with fines of up to EUR 10 million or 2% of global annual turnover for non-compliance. There is uncertainty about the new requirements as national legislation is still evolving. Nevertheless, organisations should start preparing for October 2024 now.

In addition, a provisional agreement was reached on the EU Cyber Resilience Act (CRA) on 30 November 2023. The CRA

complements the NIS2 and phases in from late 2025. It aims to protect consumers and businesses using digital products or software, establishing a framework of cybersecurity requirements and a duty of care for the lifecycle of such products. Upon enforcement, connected software and products will carry the CE mark, indicating compliance with the new standards.

#3

IT resilience becomes a statutory requirement for all financial institutions

↘

With the first set of rules for ICT and third-party risk management and incident classification published on 17 January 2024, timely preparation is essential for financial market participants to promote operational resilience and ensure compliance with DORA as of 17 January 2025.

While NIS2 focuses on supply chain cybersecurity, the Digital Operational Resilience Act (DORA) creates a regulatory framework on digital operational resilience across the EU's financial sector. DORA provides a single set of rules for the use of ICT systems by financial entities, focusing on ICT risk management, security and business continuity, resilience testing and contracting with ICT service providers. DORA also establishes an oversight framework for critical ICT service providers. Both NIS2 and DORA impose stringent requirements for the identification, assessment and reporting of IT security incidents. These obligations are based on mandatory cybersecurity policies, especially those managing third-party risks including outsourcing. Entities are also encouraged to collaborate with third parties in cybersecurity, such as participating in the DORA information-sharing arrangements.

As Member States and local regulators are set to transpose the NIS2 Directive and implement the DORA Regulation, with the first set of Regulatory Technical Standards (RTS) published on 17 January 2024, entities and service providers should monitor these developments for potential contractual negotiations due to these changes.

#4

New EU regulations to ensure fair competition, user security and privacy

↘

While the DMA aims to ensure contestable and fair markets in the digital sector, the DSA regulates the obligations of digital services, including marketplaces, that act as intermediaries in their role of connecting consumers with goods, services, and content.

In the dynamic landscape of European regulatory developments, new regulations have been implemented to effectively govern digital platforms. Together, these efforts represent the legal strides towards an innovative and secure digital ecosystem that balances the challenges of innovation, competition and user privacy. However, these (proposed) acts also highlight the ongoing challenges in balancing innovation, competition, and user privacy within the digital landscape.

The Digital Markets Act (DMA) - The DMA aims to promote fair competition by preventing anti-competitive practices and ensuring a level playing field, and came into force on 1 November 2022. The Act sets out criteria for the qualification of large online

platforms as ‘gatekeepers’. A company may be designated as a gatekeeper for multiple core platform services. Designated gatekeepers must comply with obligations such as allowing third parties to interoperate with their own operating services and prohibiting their own products or services from being ranked more favourably than those of third parties. The European Commission has designated Alphabet, Amazon, Apple, ByteDance, Meta and Microsoft as gatekeepers, covering 22 ‘core platform services’. These gatekeepers have until 6 March 2024 to comply with the DMA requirements. Non-compliance can result in a fine of up to 10% of the company’s total turnover, rising to 20% in the case of repeated infringements.

The Digital Service Act (DSA) - The DSA focuses on improving the accountability of online platforms, strengthening user security and enhancing content moderation to balance freedom of expression with responsible online behavior. It includes obligations such as transparency, notice-and-action, and bans on targeted advertising to children. It came into force for very large online platforms and online search engines on 25 August 2023. All online players, except small and micro-enterprises, must comply with the general obligations by 17 February 2024. Which obligations apply depends on whether the online actor qualifies as a (very large) online platform (at least 45 million active users per month in the EU), an intermediary or a hosting service provider. On 25 April 2023, the European Commission designated 17 platforms as ‘Very Large Online Platforms’ and two search engines as ‘Very Large Online Search Engines’. Three adult content websites were designated as ‘Very Large Online Platforms’ on 20 December 2023. These platforms and search engines must comply with the DSA obligations within four months after the designation.

ePrivacy Regulation - This proposed regulation will replace the ePrivacy Directive. It aims to strengthen users’ control over their online information and to maintain the confidentiality of electronic communications. The proposal was presented in January 2017 and is ‘lex specialis’ to the General Data Protection Regulation (GDPR). The proposal includes new obligations on tracking technologies such as cookies and wishes to establish legislative harmonisation and coordinated enforcement. However, the legislative process turned out to be very difficult and lengthy, and there have been no new legal developments in recent months.

#5

eIDAS 2.0 and digital ID become key enablers for secure cross-border transactions

The EU is revising the Regulation on electronic identification and trust services (eIDAS), in order to extend its application to the private sector and promote an EU digital identity framework. The EU legislator aims to achieve a shift from the reliance

↘

The EU Digital Identity will be available to EU citizens, residents, and businesses who want to identify themselves or provide confirmation of certain personal information. It can be used for both online and offline public and private services.

on national digital identity solutions only, to the provision of electronic attestations of attributes valid at EU level. The EU legislator recently reached a political agreement on the main topics of the legislative proposal. During the negotiations, the Dutch representation focused on prohibiting the use of data from the digital ID wallet for commercial purposes, advocating the use of open source software, and ensuring the voluntary use of the digital ID wallet. The proposal now accommodates national digital IDs within the EU, alongside the European digital ID. Initial communications indicate that these concerns have been addressed. Given the substantial debate on the legal and practical implications of the revised 2021 proposal, the final text of this revision is eagerly anticipated.

About the team

Our multidisciplinary Information & Communication Technology Group excels in navigating the legal complexities of new technologies. We combine deep sector knowledge with a pragmatic approach, focusing on simplicity where possible and innovative solutions where necessary. Recognised for our swift, practical advice, we take ICT legal challenges 'back to the basics', ensuring effective, client-focused outcomes.

Contact

For further information on these developments and their implications, please contact:

Joris Willems The Netherlands
T: +31 6 5 20 50 390
joris.willems@nautadutilh.com

Vincent Wellens Luxembourg/ Belgium
T: +352 621 15 61 78
vincent.wellens@nautadutilh.com

Contributors

Aline Bleicher | Cyril Christiaans | Ottavio Covolo | Garance Diacono | Inger van Dijkman | Danique Knibbeler | Matthieu Pierre | Tom de Smet | Sarah Zadeh