Technology Law: five things you need to know in 2023

In 2022, companies continued their efforts following the covid-19 pandemic to adapt their organisational and business processes to allow for up-to-date and secure digital tools and technologies. We have identified the following five main developments in the area of technology and their legal aspects, which will shape your agenda in the coming year. By anticipating these developments, you can use them to your advantage and prepare for their impact.

Development #1 - Continued focus on IT resiliency

In December 2022, the Official Journal of the EU finally published both the adopted Digital Operational Resiliency Act (**DORA**) and the NIS2 Directive (**NIS2 Directive**). The legal landscape for IT resiliency is now more complete (and busy!) than ever.

DORA establishes a set of requirements for the financial sector, from risk management to operational resilience testing, through incident management and reporting. DORA also regulates the contents of contractual arrangements concluded between financial entities and ICT service providers. DORA's requirements are pervasive and the act applies to the financial sector at large (with an impressive list of no less than twenty-one different categories of entities in scope, from credit institutions to ICT third-party service providers, through crypto-asset service providers and insurance intermediaries!).

The significant amount of work required to comply with DORA from an operational point of view is likely to involve a broad range of services provided by the in-scope entities, making the effective date of 17 January 2025 relatively short notice. Considering DORA in processes and contract negotiations with providers over the course of 2023 seems essential to ensure timely compliance.

Still in the financial sector, the deadline for adoption of the EBA guidelines on outsourcing (for credit institutions, investment firms and payment service providers) was, in principle, 31 December 2021 according to these guidelines. However, in Luxembourg the CSSF, the financial sector regulator, has set this date at 31 December 2022, although for most financial institutions this is a work in progress. We expect this topic to remain high on the agenda of many institutions for part of 2023.

The NIS 2 Directive (a remodeling of the original NIS Directive) is a further source of information for standards to adopt in terms of IT resilience for a list of (highly) critical sectors (most utilities sectors, credit institutions, space operators and manufacturers of important products). Aimed at the improved harmonization of requirements within the EU, the NIS2 Directive sets specific minimum rules (and ensures consistency with DORA, where needed) in terms of ICT risk-analyses and security policies, incident handling, business continuity and crisis management, as well as supply chain security and security in network and information systems acquisition, development and maintenance. Hence, it constitutes an interesting and useful baseline for future compliance projects.

Luxembourg has until October 2024 to adopt, publish, and apply measures in line with NIS2. Some member states are likely to adopt requirements that are higher than the minimum rules of the NIS2 Directive. From a practical point of view, for certain multinational undertakings with establishments across various EU member states, the higher standard adopted by one of those member states that have separate and concurrent jurisdiction is likely to become the new *de facto* standard for the whole group of undertakings. Closely following parliamentary progress on the transposition of the NIS2 Directive (in Luxembourg, but also in each member state where a business is active) will be essential to the improved planning of compliance programmes and initiatives for the 2024 deadline.

In parallel, a Proposal for a Regulation on cybersecurity requirements for products with digital elements (**Cyber Resilience Act**) is at advanced stages of discussion, aiming to improve cybersecurity in technological products (including hardware and software) designed, manufactured, imported, or otherwise distributed within the EU, by establishing minimum cybersecurity requirements for such products. This new initiative demonstrates the degree to which cybersecurity must be an essential consideration in the design process of new technological products (and in the review process for importers and distributors), even for consumer-grade products.

Also in the area of cybersecurity, by the end of 2023 the European Commission is to have carried out its first assessment of the Cyber Security Act (**CSA**) to determine if any ICT products, processes or services are to be covered by mandatory certification. The CSA lays down the main requirements for European cybersecurity certification schemes in the ICT field. Initially, certification pursuant to the cybersecurity schemes has been voluntary, but the possibility of it gradually becoming mandatory for critical products or activities had already been envisaged.

The European Commission's assessment is to be carried out by 31 December 2023 at the latest, and businesses designing, manufacturing or implementing ICT products, services, or processes should monitor the outcome to see whether it affects any of their provisions.

Development #2 - Shift in platform relations and Bigtech regulation

In -mid 2023, the Digital Markets Act (**DMA**), which entered into force early November 2022, will start to apply. By July 2023, the largest platforms (both EU and non-EU based) must have notified the European Commission of their core platform services. No later than 6 September 2023, the European Commission will have designated which of these qualify as gatekeepers, following which these platforms will have six months to comply with the obligations in the DMA (*i.e.* by 6 March 2024 at the latest). For some, the DMA may have far-reaching consequences for their innovation efforts and business models, while for others it may offer opportunities to benefit from a more innovative and competitive business environment.

For instance, we can expect (i) the end of platform monopolies (*e.g.* in hotel booking or car rental markets) because sellers will be free to offer their product elsewhere, and (ii) a better competitive position for non-gatekeeper businesses, now that gatekeepers can no longer rank their own products and services above those of other providers. For companies that offer services on the gatekeepers' platforms or competing digital platforms, it may be worthwhile analysing the DMA in more detail to see if the new regulatory framework provides a legal basis for a broader provision of services.

The Digital Services Act (**DSA**), which is part of the same set of new rules that aim to create a safer and more open digital space, entered into force on 16 November 2022. It applies to various online intermediary services, including platforms. The liability exemptions for intermediary service providers (**ISPs**), introduced by the e-Commerce Directive, will remain in the DSA. However, in order to avoid liability under consumer protection laws, the providers of online B2C marketplaces will have to ensure that an average consumer does not believe that the information or product is provided by the online marketplace itself, rather than the professional trader using the marketplace.

In-scope ISPs will have to comply with specific information and transparency obligations and may have to amend their terms and conditions accordingly. Due to the DSA's extraterritorial scope, ISPs established outside the EU that offer services in the EU must appoint a legal representative in the EU for compliance and supervision purposes. Hosting service providers (even when they are not an online platform or online marketplace) will have to put in place electronic reporting tools allowing users to report any illegal content, and are subject to specific additional transparency obligations towards users as well as notification obligations towards law enforcement and judicial authorities.

With the exception of micro and small enterprises, online platforms will additionally have to provide users with access to internal complaint-handling systems and certified out-of-court dispute settlement bodies for disputes relating to decisions of the online platforms to, for instance, suspend services or a user's account. They will also have to prioritise notices submitted by so-called "trusted flaggers", a status awarded by the supervisory authorities, and comply with enhanced transparency obligations.

The European Commission has published a useful overview of obligations per different type of online service. Based on the number of active end-users, the European Commission will determine whether a platform belongs in the 'very large' category, subject to stricter obligations. Platforms have until 17 February 2023 to report the number of end-users on their website. On 17 February 2024, the DSA will become fully applicable to all entities in scope, with the exception of an anticipated application from four months after their notification for platforms assigned to the 'very large' category. Apart from a safer and more transparent digital space, the harmonisation of these rules should make it easier for online platforms to start and grow in the EU.

The further development of the metaverse may also cause a shift in platform relations. In 2023 we expect that many more business will follow companies such as HSBC, JP Morgan, Nike and Gucci to establish a presence in the metaverse. Unlike social media and search engines, which seem pretty well covered by giants such as Google and Meta, there is still everything to play for in the metaverse.

2023 is likely to bring further interesting developments in that area, as the EU will also present an initiative to address virtual worlds, such as the metaverse. The initiative was qualified as "key" by European Commission President Ursula von der Leyen, in the latest State of the Union letter of intent.

Development #3 - Increased focus on Environmental, Social & Governance (ESG)

The amount and depth of sustainability reporting is likely to further increase in 2023. At European level, the most recent examples are the newly published Corporate Sustainability Reporting Directive (**CSRD**) and the proposed Corporate Sustainability Due Diligence Directive (**CSDD**).

These rules force companies to extend their understanding to their supply chains to analyse potential impacts for sustainability (human rights and environmental impacts). Examples of ESG-issues in the technology sector are energy consumption (*e.g.* data centers), staff working conditions (IT service desks, low-wage countries) and risks associated with big data / smart technology and facial recognition / surveillance technology, to name a few.

Although the larger parts of the relevant EU legislation target public interest / listed companies and other companies that meet certain thresholds (relating to net-turnover, number of employees or business sector), we expect many tech companies to be directly or indirectly affected by the new rules. If not driven by their own intrinsic desire to meet ESG standards, then by their customers' due diligence requirement or ethical consumerism.

Development #4 - Progress on Artificial Intelligence (AI) legal framework

Since the first introduction of the EU's Proposal for a Regulation on Artificial Intelligence (**AI Act**) in 2021, the text was significantly amended and discussed. We expect work on the AI Act to continue to intensify in the first few months of 2023, with the ultimate goal of having it on the books by the end of the year. The main impact of the AI Act would be on AI systems classified in the regulation as "high-risk".

In the latest proposal, such high-risk AI systems are those either:
- in themselves products, or forming part of or used as a safety component of a limited list of products, defined in other harmonisation directives and regulations (including, for instance, motor vehicles, medical devices, toys), that are required to undergo a third-party conformity assessment with a view to placing them on the market or putting them into service; or
- expressly listed in the AI Act (such as some specific AI systems used in education, employment, or law enforcement), unless AI's output is purely accessory.

The AI Act provides different obligations for multiple stakeholders: providers, importers, distributors and users. In particular with regard to high-risk AI systems, each operator in the supply chain up to and including the user will have to comply with specific regulatory obligations. Users will, for instance, have monitoring and incident reporting obligations and the obligation to ensure human oversight.

The creation of a supervisory board, the European Artificial Intelligence Board (**EAIB**), inspired by the EU GDPR's EDPB and the EU GDPR's EDPS, is also an important component of the AI Act. The EAIB would be tasked *inter alia* with contributing to the harmonised enforcement of the AI Act within the EU, providing expertise and best practices, and advising the European Commission on AI. The AI Act is without prejudice to the competences, tasks and independence of national data protection authorities, which should have access to any documentation created under the AI Act. How the EAIB would collaborate with the European Centre for Algorithmic Transparency (**ECAT**), recently created by the DSA, is not clear yet.

The AI Act was also completed with a separate (but complementary) initiative: the Proposal for a Directive on adapting non-contractual civil liability rules to artificial intelligence (**AI Liability Directive**). Where the purpose of the AI Act is to prevent harm caused by artificial intelligence, the AI Liability Directive is aimed at offering effective remedies to people having suffered damages caused by artificial intelligence.

It aims to help victims to evidence their liability claim in two ways. The AI Liability Directive introduces a rebuttable presumption of causality in case of non-compliance with a duty of care, and facilitates access to relevant evidence by enabling victims to request the court to order disclosures of information about high-risk AI systems.

Even though these proposals are still being discussed, we expect 2023 to be an important year in getting closer to final texts. The AI Act would be applicable within 36 months following its entry into force (the initial proposal has recently been amended to include an increase to 36 from 24 months, but whether such amendment will be accepted is yet to be confirmed). According to the current text, the AI Liability Directive would have to be transposed by member states within two years of its entry into force – a deadline that might be further aligned with the AI Act.

Overall, the deadlines to adapt to such significant changes to the legal framework applicable to AI would be quite short and it would be important for players in AI to monitor the legislative trends, and to consider the impacts already taking place in 2023.

Development #5 - Changes driven by foreign affairs and competition law

In many EU countries, foreign direct investments (**FDI**) screening mechanisms are being implemented (based on the EU FDI Regulation). The Luxembourg FDI screening mechanism will be introduced by the bill n°7885, and will apply to foreign direct investments made by foreign investors that effectively participate in the control of a Luxembourg company which carries out critical activities on Luxembourg territory.

Control can follow from either (i) owning directly or indirectly **25%** or more of the capital of the Luxembourg company, (ii) having a majority of the voting rights of the shareholders of the Luxembourg company, (iii) having the right to appoint or remove the majority of the members of the administrative, management or supervisory body of the Luxembourg company and being at the same time a shareholder, or (iv) being a shareholder of the Luxembourg company and controlling, pursuant to an agreement with other shareholders, a majority of the voting rights.

In the course of 2023, a new bill of law will likely be filed with a view to the introduction of a merger control regime in Luxembourg. Based on an intermediate report of the preparatory works, the Luxembourg regime will probably be aligned with and inspired by pre-existing rules and concepts used both by the European Commission and by national competition authorities of other member states. Luxembourg is the last EU member state to adopt such a general merger control regime.

Such types of controls, however, are not entirely new in Luxembourg. For instance in the space sector, since 2021, any transfer of space activities is subject to authorisation, and any change of control (exceeding certain thresholds) of space operators authorised under Luxembourg law is subject to notification and screening by the Ministry of Economy, which can object to the envisaged acquisition.

It will also be important to continue to closely follow national and international sanction regulations, including with respect to Russia, Belarus and Iran, to enable companies to respond to any changes in a timely manner.

Vincent WELLENS (picture)
Admitted Lawyer in Luxembourg and Brussels
Partner, NautaDutilh Avocats Luxembourg
vincent.wellens@nautadutilh.com

Sigrid HEIRBRANT
Admitted Lawyer in Luxembourg and Brussels
Senior Associate, NautaDutilh Avocats Luxembourg
sigrid.heirbrant@nautadutilh.com

Yoann le BIHAN
Senior Associate, NautaDutilh Avocats Luxembourg
yoann.lebihan@nautadutilh.com