Tech & Data Law: 5 trends for 2025

By Vincent WELLENS & Ottavio COVOLO, avocats à la Cour, NautaDutilh Avocats Luxembourg S.à r.l.

The year 2024 was notably significant for advancements in regulations governing technology and data. We believe that the key trends in this area of the law for 2025 will be building upon such regulatory initiatives with the aim of providing further legal certainty, especially in light of the industry responses (and push-back) seen in certain fields.

#1 Regulating AI

The year 2024 was marked by the continuing growth and integration of AI systems, and more specifically generative AI tools, by both business and individuals alike. 2025 will see the first sections of Regulation (EU) 2024/1689 (the "**AI Act**") entering into application on 2 February 2025. As a reminder, the AI Act aims at regulating the use and development of AI through a "risk-based approach". AI systems are categorised as presenting a "limited risk", "high-risk", or "unacceptable risk" to fundamental rights, democracy, and the rule of law. According to the level of risk, AI systems must comply with appropriate obligations such as carrying out mandatory fundamental rights impact assessments; creating a robust cybersecurity framework; or implementing human oversight.

The first wave of applicable provisions concerns the prohibition of certain AIs which, due to their inherent risk, cannot be released nor deployed onto the European market. Such AIs are listed in art. 5 of the AI Act, under the reservation that other EU law texts may set out further prohibitions. Prohibited AI practices include "*subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques, with the objective, or the effect of materially distorting the behaviour of a person or a group of persons by appreciably impairing their ability to make an informed decision*", which may cover certain forms of dark patterns, or even "*AI systems to infer emotions of a natural person in the areas of workplace and education institutions, except where the use of the AI system is intended to be put in place or into the market for medical or safety reasons*", which would in any case be precluded on the existing privacy framework concerning the surveillance of employees in the workplace.

In addition, an often overlooked section, also entering into application on 2 February 2025, is a general requirement for both providers and deployers of AI to take measures ensuring "AI literacy", defined as skills, knowledge and understanding to allow providers, deployers and affected persons (i.e., any end-user of the AI, including both internal staff and external end-users) to "*to make an informed deployment of AI systems, as well as to gain awareness about the opportunities and risks of AI and possible harm it can cause*". In practice, it is expected that entities implement mandatory trainings on AI, although there is still some uncertainty about the exact scope of such training (in terms of level of detail, or tailoring to the AIs in use or to AI in general for instance) and whether this also means putting out resources for external end users of such AI deployed by said entity (e.g., users of a AI-powered customer support chat bot).

The second wave of requirements under the AI Act will enter into application on 2 August 2025 concerning the notifying authorities and notified bodies, the governance of supervisory authorities and the penalties, and general-purpose AI models ("**GPAI**").

Due to the rapid developments in the field of GPAI, the AI Act introduces a two-tiered approach, namely GPAI with or without '*systemic risk*'. The categorisation depends on the computing power of the GPAI, referred to as floating-point operations per second or '*Flops*' and used to measure the computational complexity of training and running AI models. While all providers of GPAI systems will have to comply with transparency obligations, such as providing technical documentation; providing details about the training data; and complying with EU copyright laws, providers of GPAI systems with 'systemic risk' will have to comply with additional requirements, such as implementing appropriate cybersecurity measures, but also reporting obligations on energy efficiency and in the event of serious incidents.

The main impact of the AI Act would be on AI systems classified as "high-risk", triggering an important number of documentation and assessment related obligations to ensure that the deployment of the AI follows a risk-based approach. These requirements will only enter into application from 2 August 2026. It is recommended for suppliers and users of AI systems to anticipate on the implementation of the regulation all the more so as this regulation is unprecedented and is not based on a pre-established framework. This being said, the GDPR remains an important piece of legislation, given notably the recent EDPB Opinion 28/2024 of December 2024 on data protection aspects related to the processing of personal data in the context of AI models underlining in particular the ability of controllers to evidence the anonymisation of personal data used in the training of the AI, and the designation of the CNPD as the competent supervisory authority for the purposes of the AI Act (pursuant to bill of law n°8476).

#2 Regulation of platforms and BigTech

It is interesting to note that the rules for BigTech have materialised across several new legal and enforcement initiatives and 2025 will see a continuation of this trend turning more to enforcement.

The Digital Markets Act ("**DMA**"), not to be confused with its 'sister' Digital Services Act ("**DSA**"), has come into force in March 2024. The DMA is applicable to so-called "gatekeepers" in the digital world assuring, amongst others, a higher degree of interoperability with other (smaller) players and breaking up the synergies between different business segments of BigTech conglomerates. The European Commission is expected to follow its investigation and enforcement efforts both on the ground and against the appeals filed by certain designated gatekeepers concerning their designation under the DMA.

On a related note, the EDPB adopted in April 2024 bespoke requirements for "large online platforms" in terms of valid consent or pay models (i.e., where the option is given to the user to either accept targeted advertising to pay to access the website) without however a precise alignment with the like notion of "very large online platforms" under the DSA, underlining that regulatory authorities may not hesitate to pursue new requirements instead of levying existing ones. Likewise, we expect that many of the practices that would be enforced via competition law would now be easier to enforce on the basis of the DMA. Competition law will, however, continue to play a role via the applicable merger control rules on the basis of which some BigTech acquisitions can be prohibited.

In addition, the **Data Act**, facilitating switching between cloud service providers and imposing specific obligations in terms of contractual terms and switching charges, will become applicable from 12 September 2025, impacting the negotiation and revision of contractual terms from the biggest players in the cloud service industry, and their repercussions across the chain of services relying on such cloud infrastructure.

#3 Continued focus on IT resiliency and third party risk management

The earliest development in 2025 will be the entry into force of the Digital Operational Resilience Act ("**DORA**") regulating designated critical ICT third-party service providers such as the large cloud service providers) delivering services to the financial sector. Although DORA enters into application on 17 January 2025, and in-scope entities are expected to have already prepared in advance in terms of internal governance arrangements, reporting requirements, and negotiation with third party ICT service providers, a certain grace period is likely to be expected given the important number of requirements stemming from DORA. The German BaFIN has for instance requested supervised entities to comply with the registers of information requirements by 11 April 2025, and underlined that a list of critical ICT service providers is expected to be published by European Supervisory Authorities in Q2 2025. The CSSF will disclose its target date soon.

DORA establishes a set of requirements, from risk management to operational resilience testing, through incident management and reporting in the financial sector at large with an impressive list of no less than 21 different categories of in-scope entities, from credit institutions to ICT service providers, through fund managers, crypto-asset service providers and insurance intermediaries. This regulation will thus have a significant impact on the Luxembourg financial center. DORA also regulates the contents of contractual arrangements concluded between financial entities and ICT service providers. 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 of the in-scope entities and requires the review of the most important ICT agreements of the entities concerned.

As highlighted by the EDPB in its Opinion 22/2024 adopted in October 2024 on the reliance of sub-processor, there is a key importance for controllers to be reasonably aware of the identity and activity not only of their immediate sub-processors, but also of throughout the processing chain, a position reminiscent of the requirements under the DORA RTS of sub-contracting requiring entities to be able to monitor the whole subcontracting chain of ICT services supporting critical or important functions. This parallel hints at a possible convergence between regulatory frameworks to adopt similar positions on essentially the same questions, increasing certainty for supervised entities.

In addition to DORA, the NIS 2 Directive (remodeling of the original NIS Directive) is a further legal text imposing obligations in terms of IT resilience for a list of (highly) critical sectors (most utilities sectors, credit institutions, space sector, manufacturing of important products). Aimed at improving harmonisation of EU requirements, the NIS2 Directive sets specific minimum rules (and ensures consistency with DORA, where needed) in terms of ICT risk analysis 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. The bill of law (n°8364) transposing the NIS2 Directive into Luxembourg law is yet to be voted.

In parallel, the "**Cyber Resilience Act**" has been adopted on 23 October 2024. This act aims at improving 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 that 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.

#4 The data economy: open data & data sharing

The European data strategy that was announced by the European Commission in 2020 aims to create a single market for data, in which – personal and non-personal – data will flow freely across sectors benefiting various stakeholders, boosting Europe's global competitiveness and data sovereignty. The Data Governance Act ("**DGA**") and the Data Act are pivotal in this respect. The DGA includes conditions for the reuse of certain categories of data held by public sector bodies, sets rules for the provision of data intermediation services, and introduces a framework that facilitates data altruism for objectives of general interest.

The Data Act by contrast aims to ensure fairness in the digital environment, stimulate a competitive data market, open opportunities for data-driven innovation and make data more accessible for all. It includes harmonised rules on (i) making data generated by the use of a product or related service (e.g., IoT applications) available to the user thereof, (ii) making data available by data holders to data recipients, public sector bodies and Union institutions, agencies or bodies, (iii) facilitating switching between data processing services, (iv) introducing safeguards against unlawful third party access to non-personal data, and (v) the development of interoperability standards for data to be accessed, transferred and used.

A Luxembourg bill of law (n°8395) aims at implementing both the DGA and the "once only" principle, whereby an administration cannot request a citizen to produce a document or information that is already in the possession of another administration.

Other key trends in the EU and in Luxembourg will be the creation of sectoral data sharing mechanisms is "*en vogue*", for example, with the EU legislative initiative to adopt a regulation on a European Health Data Space ("**EHDS**") for health data, now awaiting a formal vote from the Council - following a political agreement reached in March 2024 with the European Parliament - before its publication in the official journal, as well as the proposal for a regulation on a framework for Financial Data Access ("**FiDA**") facilitating the sharing of data in the financial sector beyond the existing account information access rules under the payment services regulatory framework.

These initiatives will however be subject to scrutiny from both in-scope entities and the individuals whose data will be managed under these initiatives, particularly from a privacy and data protection standpoint given such considerations may lead to the nullity of a legal provision (see for instance the ultimate beneficial owners registers' open access being shut down by the CJEU).

#5 GDPR enforcement & increased risk of privacy litigation

The GDPR as shown above still retains a particular importance and data protection authorities are increasingly seen as taking an active role beyond data protection to ensure an overall surveillance of risks posed by technology and related industries (be it in BigTech, AI or 3rd party management). Whilst the above approach will raise questions of alignment between the different regulatory regimes, the proposal for a regulation harmonizing certain aspects of GDPR enforcement remains to be negotiated between the European Parliament and the Council with disagreements remaining ahead of the trilogue, particularly on the position of the complainant.

Another trend in recent years is the award of damages for data protection related breaches, which is seeing some increase in Europe, although at a slower pace than in other jurisdictions such as with the US. The CJEU has held that even if the breach resulted in no material damages being evidenced, it does recognise the right of the claimant to receive some non-material (i.e., moral damages, even for a trivial amount based solely on the . In the recent *Bindl* case (T-354/22), the General Court of the European has ordered the European Commission to pay EUR 400 for non-material damages to a visitor of its website due to the transfer of their IP address to the website of Facebook hosted in the US following a click on the "Sign in with Facebook" plug-in. Another arguably trivial claim which may give rise to such moral damages could be the fact pattern in the *Mousse* ruling before the CJEU (C-394/23) holding that the processing of "Mr" or "Ms" is not necessary for the booking of train tickets.

It remains to be seen whether this will bolster claimants' interest in privacy litigation in the EU and reverse the general trend in Europe of seeing enforcement stemming from regulators' initiatives rather than from individual claimants, but this does send an encouraging signal to privacy claimants (especially activists) that any breach of GDPR, irrespective of its trivial importance, could lead to the award of moral damages.