Upcoming EU legislation on artificial intelligence:

Importance for the Luxembourg Financial Market place and beyond

The CSSF thematic report on AI of 3 May 2023 has revealed that about one third of financial institutions that participated in a joint survey of the CSSF and the BCL[1] have confirmed to have invested in artificial intelligence technology ('AI') in 2021, and indicated a general increase of panned investments for the years 2022-2023 across all innovative technologies. In April 2023, three fourths of respondents who participated in a survey carried out by the Luxembourg Banker's Association (ABBL) considered ChatGPT as an opportunity for their business rather than a threat[2].

AI is an innovative technology that can serve to benefit the financial sector by, for example, improving fraud detection mechanisms, improving internal efficiencies, and providing for new customer insights.

As the use of AI also entails new challenges and risks, the European Commission proposed in 2021 a harmonized legal framework on AI in the EU (the "**draft AI Act**"). The European Parliament's leading parliamentary committees have now approved and adopted an amended text of that draft AI Act. "We are on the verge of building a real landmark legislation for the digital landscape, not only for Europe but also for the entire world," stated one of the co-rapporteurs ahead of the vote on 11 May 2023. We identified the following highlights to consider when preparing for the upcoming AI legal framework.

Broad scope of application and extraterritorial reach

The draft AI Act has a fairly broad material and territorial scope and applies to the development, the placing on the market, the putting into service and the use of AI. The definition of 'artificial intelligence system' has changed. AI is currently defined as a machine-based system that is designed to operate with varying levels of autonomy and that can, for explicit or implicit objectives, generate outputs such as predictions, recommendations, or decisions that influence physical or virtual environments.

Like the GDPR, the draft AI Act has extra-territorial reach and also applies to providers and users of AI systems established or located outside the EU when the output produced by the system is intended to be used within the EU. In general, the draft AI Act also resembles the regulatory framework applicable to product safety as it relies on harmonised standards and conformity assessments and provides different set of rules for providers, importers, distributors and users (i.e., 'deployers' in the draft AI Act).

Unacceptable and high-risk AI systems

The draft AI Act clearly follows a risk-based approach and classifies AI systems according to their risk level: from minimal to limited, high and unacceptable. AI systems with unacceptable risk are banned. High-risk AI systems are not prohibited per se but are subject to ample requirements with regard to risk management, data governance, technical documentation, record-keeping, transparency to users, human oversight, accuracy, robustness and cybersecurity.

The main changes to the draft AI Act relate to the AI systems with unacceptable or high-risk levels, add requirements for generative AI systems, including a transparency requirement, and add safeguards to prevent discrimination and violation of fundamental rights. The ban on remote biometric identification systems has been expanded.

Where the initial draft AI Act only banned the use of such systems for 'real-time' identification, it now also prohibits the use of such systems for 'post' remote biometric identification, unless a pre-judicial authorisation has been granted for law enforcement purposes in the context of a specific serious criminal offence.

A ban on the use of "purposefully" manipulative or deceptive techniques has been introduced. Even though any intentionality could be difficult to prove, the additional notion "purposefully" was eventually upheld. The untargeted scraping of facial images from the internet or CCTV footage has been prohibited too.

The use of AI systems for emotion recognition (including by analysing facial expressions) will be prohibited in the areas of law enforcement, border management, in workplaces and education institutions. The ban on 'predictive policing' has been extended from criminal offenses to administrative offenses. This might follow from the Dutch *'Toeslagenaffaire'* (child benefits scandal) where families were falsely accused of fraud due to a flawed algorithm.

In the initial version of the draft AI Act, AI systems listed in Annex III were automatically qualified as high-risk. The amended draft AI Act includes an additional, restrictive layer. AI systems covered by Annex III will only be deemed high-risk if they pose a significant risk of harm to the health, safety or fundamental rights of individuals. The list of AI systems covered by Annex III (high-risk) has been expanded and now also includes the use of AI systems in the recommender systems by very large online platforms within the meaning of the Digital Service Act used to recommend user-generated content available on the platform.

Generative AI systems

Concerned by the use and popularity of generative AI systems, such as ChatGPT, Dall-E or Midjourney, last-minute provisions have been added to the draft AI Act. Providers of generative AI systems will have to document and make publicly available a sufficiently detailed summary of the use of training data protected under copyright law.

Even though it was initially proposed to ban the use of copyrighted material for training AI systems altogether, such overall ban was abandoned in favour of the transparency requirement. Another important addition regarding generative AI systems is that they must be trained, designed and developed in such a way as to ensure adequate safeguards against the generation of content in breach of EU law in line with the state of the art, and without prejudice to fundamental rights, including the freedom of expression. This provision aims to ensure that generative AI systems will not create discriminatory results and that fundamental rights are protected.

Protection of personal data

The draft AI Act does not prejudice or derogate from the EU General Data Protection Regulation ('**GDPR**'). It merely aims to complements the existing data protection laws. Prior to putting a high-risk AI system in use, deployers will have to conduct a fundamental rights impact assessment ('**FRIA**'). Where the deployer is required to carry out a data protection impact assessment ('**DPIA**') under the GDPR, the DPIA shall be an addendum to the FRIA. When registering the use of high-risk AI system in the EU database, which is mandatory for public authorities and 'gatekeepers' under the Digital Markets Act, a summary of the DPIA carried out must be filed.

In addition to their rights under the GDPR, any persons significantly affected by a decision based on a high-risk AI system has the right to a clear and meaningful explanation from the user of the system, including information on role of the AI system in the decision-making procedure, the main parameters of the decision taken and the related input data.

Users providing such explanation must take into account the level of expertise and knowledge of the average consumer or individual. According to the joint survey of the CSSF and the BCL[3], 70% of the respondents reported a very good, or good explainability of the predictions of the machine learning solutions used, including credit scoring use cases.

Finally, the amended draft AI Act foresees that, where an AI system involves the processing of personal data, the EU declaration of conformity shall include a statement that the respective AI system complies with the GDPR.

Measures in support of innovation

To foster innovation, enhance legal certainty and remove barriers for SMEs and start-ups, the draft AI Act imposes on Member States to establish at least one AI regulatory sandbox. Such sandbox is intended to provide a controlled experimentation environment for the development, testing and validation of innovative AI systems, under strict regulatory oversight, before their placement on the market or putting into service. The fintech sector is familiar with the concept of sandboxes. They can help companies manage their regulatory risk during the development or testing phase.

Model contractual terms and unfair B2B terms

According to the amended draft AI Act, the European Commission shall develop recommended, non-binding model contractual clauses between providers of high-risk AI systems and their suppliers that provide tools, services, components or processes used or integrated in high-risk AI systems. Furthermore, the amended draft AI Act provides for the nullity of unfair B2B terms unilaterally imposed on SMEs or start-ups. It thereby defines an unfair contractual term as "a term of such a nature that objectively impairs the ability of the party upon whom the term has been unilaterally imposed to protect its legitimate commercial interest in the information in question or its use grossly deviates from good commercial practice in the supply of tools, services, components or processes that are used or integrated in a high-risk AI system, contrary to good faith and fair dealing or creates a significant imbalance between the rights and the obligations of the parties in the contract".

It also introduces a list of terms deemed unfair, such as terms that (i) exclude or limit the liability for intentional acts or gross negligence, (ii) exclude available remedies in case of contract breach, or (iii) shift the financial burden of penalties in case of non-compliance or of associated litigation costs.

Implementation and sanctions for non-compliance

EU Member States will designate one or more competent authorities for supervising the application and implementation of the upcoming AI Act. With respect to AI systems that are provided or used by regulated financial entities, the financial supervisory authorities may for instance be designated as competent authority in order to ensure a coherent enforcement of the obligations under the various applicable legislations. On EU level, an independent European Artificial Intelligence Office shall be established in Brussels.

Infringements are subject to sanctions which include differentiated administrative fines that can amount up to 40.000.000 euros or 7% of the total worldwide annual turnover of a company in case of non-compliance with the prohibition of certain AI practices.

Next steps

The draft AI Act is expected to be voted on the European Parliament's plenary session of 14 June 2023 and will then enter the last phase of the legislative process. During the so-called trilogue negotiations, the European Commission, the European Parliament and the Council will work out the final details of the AI Act. Just like the GDPR, the finally adopted regulation on AI is expected to have an impact on the regulatory approaches elsewhere in the world with regard to AI.

Sigrid HEIRBRANT
avocat aux Barreau de Bruxelles et Luxembourg (Liste IV)
sigrid.heirbrant@nautadutilh.com

Vincent WELLENS (portrait)
avocat à la Cour au Barreau de Luxembourg (Liste I) et
avocat au Barreau de Bruxelles
vincent.wellens@nautadutilh.com

NautaDutilh Avocats Luxembourg S.à r.l.