

Legal 500

Country Comparative Guides 2026

Belgium

Artificial Intelligence

Contributor

LAWTREE Advocaten

Nicolas Wesling

partner | nicolas.wesling@lawtree.be

Luna Fasoel

Attorney-by-law | luna.fasoel@lawtree.be



This country-specific Q&A provides an overview of artificial intelligence laws and regulations applicable in Belgium.

For a full list of jurisdictional Q&As visit legal500.com/guides

Belgium: Artificial Intelligence

1. What is the legal definition of “artificial intelligence” in your jurisdiction, if any? If no definition exists, how do regulators or courts typically describe artificial intelligence?

In Belgium, the legal definition from the Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (AI Act) applies, as the AI Act is a regulation and is therefore directly applicable in Belgium.

An AI system is defined as a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment. For explicit or implicit objectives, it infers, from the input it receives, how to generate outputs such as predictions, content, recommendations or decisions that can influence physical or virtual environments.

2. Has your country developed a national strategy for artificial intelligence? If yes, what progress has been made in its implementation? Are there plans for updates or revisions?

The Belgian Government intends to develop a national AI strategy aimed at providing a comprehensive strategic and operational framework for the development and deployment of artificial intelligence in Belgium. Building on the policy recommendations of the AI4BELGIUM coalition, the strategy sets out ongoing initiatives and future policy priorities structured around three strategic pillars:

- Driving technological impact by strengthening high-quality expertise in AI and developing a responsible data strategy to support the development and use of AI;
- Delivering social and economic benefits by promoting continuous skills development in AI, fostering a strong and competitive AI ecosystem and enhancing public services through the responsible use of AI;
- Creating the appropriate conditions for an ethical, resilient and secure society by ensuring that the development and deployment of AI takes place in a responsible and sustainable manner.

The strategy is considered a “living document” that is

regularly updated based on new insights.

The transversal nature of AI and its broad impact on the Belgian economy and society require a multi-level governance approach, given the division of competences within a federal state such as Belgium. To take this into account, the Belgian AI strategy sets out policy measures at both federal and regional level, distinguishing between measures for the Federal State, Flanders, the Walloon Region, the Brussels-Capital Region and the Wallonia-Brussels Federation.

In 2022, the federal government adopted the National Convergence Plan for the Development of Artificial Intelligence. This plan sets out nine concrete objectives aimed at making Belgium a “SmartAINation” but does not impose legally binding obligations. The actions envisaged demonstrate an ambition to promote the responsible development and use of AI.

The coalition agreement 2025 – 2029 of the new federal government addresses the rise of technology across various domains. With regard to AI, it is particularly notable that the government has set ambitious objectives in the field of public health. AI will also be used to simplify administrative processes across various departments. In the field of security, the government plans to establish a testing environment in which intelligence and security services can experiment with new technologies. In addition, the existing legislation on camera surveillance will be amended to enable the use of smart camera systems.

In 2019, the Flemish Government launched a Flemish Action Plan for Artificial Intelligence, based on the Flemish Policy Plan for Artificial Intelligence. The plan focuses on research, the digitalisation of businesses and improving AI literacy among the Flemish population. As part of the Flemish AI Strategy, various guidelines and recommendations are also provided (e.g. by the Knowledge Centre for Data & Society). This Flemish Action Plan was renewed in 2024, as the importance of AI as a so-called horizontal and ubiquitous technology has only increased over the past few years. It is subject to periodic evaluation by advisory partners and independent experts in the field of digitalisation and AI.

In the Walloon Region, the Digital Wallonia strategy has, since 2015, embodied Wallonia’s digital ambitions and

provided a coherent and cross-cutting framework for the region's initiatives. One of its key initiatives is the DigitalWallonia4.ai program, which aims to accelerate the adoption and development of AI across Wallonia and was officially launched on 1 July 2019. In October 2025, the Walloon Government adopted the 2025–2029 version of Digital Wallonia, reflecting the need to update the strategy in light of major technological and societal developments, including generative AI, cybersecurity, European regulatory requirements and environmental and energy considerations. The revised strategy also introduces a more agile framework, moving away from rigid structures and overly prescriptive planning.

Aligned with the priorities of the European Digital Decade, Digital Wallonia 2025–2029 is structured around six key priorities: a connected and intelligent territory, cybersecurity, artificial intelligence, digital transformation and innovation, digital skills and data sovereignty. This strategy is also subject to periodic evaluation by relevant stakeholders.

The Brussels region adopted an AI policy and launched a wide range of initiatives in order to boost AI-related activities in Brussels. One such initiative is FARI – AI for the Common Good Institute, a joint initiative of the Vrije Universiteit Brussel (VUB) and Université libre de Bruxelles (ULB), which leverages AI, data and robotics for the common good. FARI supports citizens, public authorities and businesses in developing trustworthy and ethical technologies aimed at addressing urban and societal challenges. The Brussels Region has also published yearly updated white papers that address, among other topics, artificial intelligence.

3. Has your jurisdiction adopted any AI-specific laws, regulations, voluntary standards, or ethical guidelines? If so, please provide a brief overview. If not, which existing laws could be/applied to artificial intelligence and the use of artificial intelligence, what are the main interpretive challenges, and are there any pending artificial intelligence legislative initiatives?

The AI Act, published 12 July 2024, is binding and directly applicable in Belgium on its staggered timeline. It adopts a risk-based approach, dividing systems into unacceptable (prohibited), high (subject to specific requirements) and low or minimal risk (fewer or no requirements), with specific rules for general-purpose AI.

The Regulation (EU) 2023/1230 on machinery, repealing the Machinery Directive 2006/42/EC, will apply from 20

January 2027. The definition of “machinery or related product” has been broadened to include collaborative robots. The Regulation seeks to align the regulatory framework with technological developments, including artificial intelligence, new digitalisation applications and cybersecurity systems. To this end, it introduces specific requirements concerning the safety of autonomous machinery, human-machine collaboration and the safe use of artificial intelligence systems in machinery and related products.

The Belgian AI strategy highlights the importance of fostering the reliable, safe and trustworthy development and deployment of AI through a clear legal and regulatory framework that promotes innovation while safeguarding the fundamental rights and freedoms of individuals. In the regulatory field, the Belgian Government adopted for example in March 2018 the Royal Decree of 1 December 1975 governing the testing of automated vehicles. The decree facilitates the development and testing of increasingly autonomous vehicles by allowing automated vehicles to be used on public roads for testing purposes, subject to specific conditions and restrictions.

In the field of employment, adjustments have also been introduced. The regulations concerning the well-being of workers, including Article 5 of the Act of 4 August 1996 on well-being of workers in the performance of their work, impose a range of measures on employers to promote safety and health in the workplace. This legislation sets out the basic principles of risk prevention, including avoiding risks at source, assessing risks that cannot be avoided and giving priority to collective protective measures over individual protective measures. These provisions also apply to the use of work equipment, including equipment incorporating emerging technologies such as artificial intelligence. The legal framework sets out the employer's obligations regarding the provision of safe equipment, in accordance with applicable European directives and adapted to the work being performed.

In addition to the Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR) and the Act of 30 July 2018 on the protection of natural persons with regard to the processing of personal data, Belgium has a number of collective bargaining agreements (e.g. no. 39, 68 and 81) that may apply to the collection of data and the use of algorithms in the workplace.

At European Union level, on 11 November 2024, Directive (EU) 2024/2831 on improving working conditions in platform work was published in the Official Journal of the European Union. The Directive introduces a simpler

determination of the correct employment status of digital platform workers and entails the first EU-wide rules governing the use of algorithmic management systems in the workplace. This directive needs to be transposed into Belgian law.

Belgian law establishes a general principle prohibiting direct and indirect discrimination against individuals on the grounds of age, sexual orientation, race, sex or religion. Employers must ensure that the use of AI does not result in indirect discrimination or otherwise breach these rules. This prohibition is enshrined in the Act of 10 May 2007 on combating certain forms of discrimination, the Act of 30 July 1981 criminalising certain acts motivated by racism or xenophobia and the Act of 10 May 2007 on combating discrimination between women and men. The prohibition of discrimination applies in the context of employment relationships, including access to the labour market, the determination of remuneration and working conditions, promotion and dismissal.

At national level, the Charter for the Responsible Use of AI in Public Services was adopted and signed on 11 July 2025. The Charter aims to foster a climate of trust between public authorities and citizens by clearly demonstrating how AI can be used in the public interest while respecting fundamental rights. In addition, the federal government established a Data and AI Ethics Advisory Committee in 2024. The Committee provides scientifically based advice on ethical, legal, social and environmental issues concerning AI, robotics and related technologies used within the federal administration.

At European level, several ethical and voluntary guidelines have also been developed. These include the Ethics Guidelines for Trustworthy AI, the Living Guidelines on the Responsible Use of Generative AI in Research and the European Code of Conduct for Research Integrity, among others.

At regional level, the Flemish AI Playbook provides practical guidance to public authorities on the responsible use of AI. Furthermore, various professional sectors have developed specific guidance on the use of AI. For example, the Order of Flemish Bars has issued Guidelines for Lawyers on the Use of Artificial Intelligence, providing guidance on the responsible and professional use of AI within the legal profession.

4. Are there legal requirements for artificial intelligence transparency, explainability, or audits? Are there obligations to disclose the use

of artificial intelligence to customers/clients?

Yes, the AI Act establishes specific requirements depending on the risk category of the AI system.

Individuals must generally be informed when they are interacting with an AI system, such as a chatbot, unless this is already obvious from the circumstances. AI-generated or synthetic content must also be appropriately identifiable.

For high-risk AI systems, providers must supply instructions for use that enable deployers to interpret and appropriately use the system's outputs. Individuals affected by certain decisions may also be entitled to a clear explanation of the role played by the AI system in the decision. High-risk AI systems are also subject to a conformity assessment before being placed on the market or put into service. Providers must therefore establish an appropriate quality management system and post-market monitoring system to ensure continued compliance and identify potential risks after deployment.

On 20 July 2026, the European Commission adopted guidelines on the transparency obligations for certain AI systems under Article 50 of the AI Act. These obligations, which apply from 2 August 2026, require providers and deployers of AI systems (i.e. persons, companies, organisations or public authorities that use those systems) to ensure transparency regarding the use of AI in four key areas: (i) direct interaction with individuals; (ii) AI-generated content; (iii) emotion recognition and biometric categorisation and (iv) deepfakes and AI-generated text concerning matters of public interest. Although these guidelines are non-binding and any authoritative interpretation may ultimately rest with the courts, they are nevertheless expected to serve as the primary reference for national authorities when interpreting the transparency obligations.

In addition to these guidelines, the AI Office has also overseen the development of the voluntary Code of Practice on Transparency of AI-Generated Content. This document, which is open to organisations across the EU, sets out practical technical and operational measures for the marking, labelling and watermarking of AI-generated content, with a particular focus on the obligations under Article 50(2) of the AI Act. Adherence to the Code of Practice can provide organisations with a practical means of demonstrating compliance with these transparency obligations, while the AI Office has indicated that signatories may benefit from a presumption of conformity with the relevant requirements.

At regional level, the Flemish Government has adopted specific guidelines on transparency in the use of AI, both for its own internal operations and to assist Flemish and local public authorities in interpreting and practically applying Article 50 of the AI Act. These guidelines require, among other things, that employees be transparent about their use of generative AI and that AI-generated content be appropriately identified. The Flemish Government also emphasises that AI-generated content must be checked for accuracy, completeness and reliability before being used or communicated.

The legal requirements relating to AI transparency and explainability under the AI Act interact with obligations arising from other areas of legislation, e.g. the GDPR (and the Act of 30 July 2018 on the protection of natural persons with regard to the processing of personal data) and the Belgian Code of Economic Law.

The GDPR (and the Act of 30 July 2018 on the protection of natural persons with regard to the processing of personal data) already imposes transparency obligations on organisations processing personal data, requiring individuals to receive clear information about which information is collected, for what purposes it is used, how AI systems generate or derive new information. In addition, Article 22 GDPR provides specific safeguards in relation to automated individual decision-making. Where a decision is based solely on automated processing and produces legal effects or similarly significantly affects an individual, specific conditions and safeguards apply, including information about the logic involved.

In our view, the Belgian Code of Economic Law is also relevant, as it contains provisions on fair commercial practices, consumer protection and copyright, containing rules that may require businesses to provide consumers with clear and transparent information, including, where applicable, about the use of AI in commercial practices.

5. Are there legal requirements or best practice expectations for human oversight and human-in-the-loop in artificial intelligence systems?

Human oversight is mandatory for high-risk AI systems under Article 14 of the AI Act. Its purpose is to prevent or minimise risks to health, safety and fundamental rights. Human oversight may be built into the system itself, for example through a stop button or exercised by the deployer through appropriately qualified personnel. For certain biometric identification systems, the AI Act additionally requires verification by at least two natural persons.

As indicated above, where AI systems process personal data, the GDPR also applies. In particular, Article 22 GDPR provides safeguards in relation to automated decision-making, including the right to obtain human intervention.

In Belgium, various actors have also adopted recommendations and guidance on the responsible use of AI and the need to ensure effective human oversight. For example, the federal Charter for Responsible AI Use in Public Services explicitly requires human control over high-risk AI systems and provides that citizens should be able to interact with a human instead of an AI system. In addition, the Federal Advisory Committee on Data and AI Ethics has highlighted the importance of maintaining human oversight and human expertise when AI is used within public administration. Furthermore, the Institute for the Equality of Women and Men has also issued recommendations on the use of AI in recruitment and selection processes. Its 2026 recommendations emphasises the importance of human oversight to mitigate bias and ensure inclusive recruitment practices.

6. Are there specific legal or regulatory requirements addressing algorithmic bias, discrimination, or fairness in AI systems (including gender bias)?

Discrimination and algorithmic bias are addressed under the AI Act through several mechanisms. Risk management requirements require high-risk AI systems to be assessed and tested for potential discriminatory effects. Data governance requirements further require training, validation and testing datasets to be sufficiently relevant, representative and appropriately managed in order to reduce the risk of bias and errors. In addition, the AI Act prohibits certain practices, including social scoring and certain forms of biometric categorisation based on sensitive characteristics, such as race or political beliefs.

These requirements are complemented by national guidance. In particular, the Institute for the Equality of Women and Men has issued recommendations addressing the risks of gender bias and discrimination in AI-assisted recruitment and selection. The Institute recommends, among other measures, strengthening the legal framework, increasing awareness and training among employers and recruitment professionals, establishing internal policies governing the use of AI and incorporating the principle of "Equality by Design" into the development and deployment of AI systems.

More generally, the initiatives and regulatory frameworks referred to above in Question 3 are also relevant and may apply, depending on the specific context and use of AI.

7. What legal frameworks apply to AI-related harm and defective artificial intelligence systems? Who can be held liable (developer, deployer, victim of the damage, others), how is liability allocated, and what burden of proof applies to victims?

Belgian law does not currently provide for a specific civil liability regime dedicated to damage caused by artificial intelligence systems. Liability for AI-related harm is therefore assessed under the existing rules on product liability, contractual and non-contractual liability, consumer protection and data protection, depending on the nature of the harm and the relationship between the parties.

Where an AI system qualifies as a product, the Belgian product liability regime applies. The concept of "product" expressly includes software and is adapted to digital technologies, including AI-enabled products. Providers are primarily responsible for the conformity of the system. Deployers must follow instructions and exercise oversight. Where a distributor, importer or user makes a substantial modification to a high-risk system, that party is considered the new provider and assumes all associated obligations. For the burden of proof and the allocation of liability in the event of damage, the national liability rules continue to apply.

The existing framework is primarily set out in the Belgian Code of Economic Law, which implements the EU product liability rules. Under this regime, producers may be held strictly liable for damage caused by a defective product, without the injured party having to prove fault. The claimant must generally establish the existence of a defect, the damage suffered and the causal link between the two. Depending on the circumstances and the role of the parties concerned, liability may also extend to importers, distributors or other economic operators in the supply chain. At EU level, Directive (EU) 2024/2853 on liability for defective products introduces a revised product liability framework, concerning the disclosure of evidence and the burden of proof in technically complex cases. Member States are required to transpose the Directive into national law by 9 December 2026, with the new rules applying to products placed on the market from 9 December 2026 onwards. Belgium is currently in the process of transposing the directive into national law.

Outside the product liability regime, AI-related harm may also give rise to contractual or extra-contractual liability under the Belgian Civil Code. Developers, providers, deployers, operators or other persons involved in the design, development, deployment or use of an AI system

may incur liability where the applicable conditions for contractual or extra-contractual liability are met.

In case of non-contractual liability, book 6 of the Belgian Civil Code requires, in principle, a fault (an act or omission), a damage and a causal link between the fault and the damage. More specifically, the user of a defective object may be held liable for damage caused by the defect, even without personal fault. This may apply to tangible products incorporating AI, such as an AI-controlled machine. An AI user may also incur liability where they wrongfully use a non-defective AI system and thereby cause damage. More specifically, this means that a victim of harm caused by an AI system may be liable for its own damage where the victim has acted negligently (e.g. misused an AI system). For damage caused by autonomous vehicles we refer to our answer to Question 3.

In contractual relationships, liability is assessed in accordance with the parties' contractual obligations and the general rules of book 5 of the Belgian Civil code or the Belgian Code of Economic Law regarding B2C and B2B rules. A contractual party may, to the extent permitted by law, have excluded or limited its liability. If a victim of harm caused by an AI system has agreed to such a liability clause, it may have to bear the resulting damage itself. In a B2C relationship, however, such clauses may be considered unlawful and therefore void.

More specifically, the person using an object to carry out a contractual duty is contractually liable for a breach caused by a defect in the object used. This provision is particularly relevant in cases where contractual services are rendered with the assistance of a (defective) AI system (e.g. automated asset management services). Parties may contractually depart from this principle.

In the case of a sale of goods or a contract for the supply of digital content or digital services to a consumer, the seller or supplier is generally required to ensure that the goods or digital service conform to the agreement. The seller or supplier may be held liable for hidden defects and lack of conformity.

In principle, the party seeking compensation bears the burden of proving the facts giving rise to liability, the damage and the causal link, subject to the specific rules and presumptions provided for by law (e.g. a reasonable degree of certainty). The parties may, in principle, contractually agree to modify the burden of proof. However, this is generally not permitted in B2C contracts, where such clauses may be considered unlawful and void under the Belgian Code of Economic Law.

Where AI systems involve the unlawful processing of personal data, the GDPR and the Act of 30 July 2018 on the protection of natural persons with regard to the processing of personal data also applies. Controllers and processors may incur liability for infringements of data protection legislation, while data subjects may be entitled to compensation for material or non-material damage in accordance with Article 82 GDPR.

The AI Act itself does not establish a general civil liability regime or determine the right to compensation for damage caused by AI systems. Instead, it imposes regulatory obligations on providers, deployers and other relevant actors concerning the development, placing on the market, putting into service and use of AI systems. Non-compliance with these obligations may nevertheless be relevant when assessing liability under the applicable product liability, civil liability, consumer protection or data protection rules.

At the moment, Belgium is establishing the national governance and enforcement framework for the AI Act, including the designation of competent authorities and the applicable administrative enforcement mechanisms and sanctions. These measures do not create a separate AI-specific civil liability regime but complement the existing Belgian framework within which claims for compensation arising from AI-related harm may be brought.

It should further be noted that, at EU level, no AI-specific civil liability regime has been established. The proposed AI Liability Directive, which was intended to introduce specific rules on the burden of proof in relation to AI-related damage, was withdrawn by the European Commission. AI-related liability therefore continues to be addressed primarily through the existing and evolving rules on product liability, contractual and extra-contractual liability, consumer protection and data protection.

8. What cybersecurity obligations apply to AI systems?

High-risk AI systems must ensure an appropriate level of cybersecurity throughout their entire lifecycle. They must be resilient against attempts by third parties to manipulate their use or performance. Specific AI vulnerabilities such as data poisoning or adversarial attacks must be addressed through appropriate technical solutions.

These requirements apply in addition to the obligations arising under Directive (EU) 2022/2555 on measures for a

high common level of cybersecurity across the Union (NIS2) and, where applicable, the Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA). The interaction between these frameworks is particularly relevant for regulated entities subject to cybersecurity governance and supply-chain requirements, as well as for economic operators that qualify as providers under Article 25 of the AI Act.

NIS2 and the Belgian Act of 26 April 2024 establishing a framework for the cybersecurity of networks and information systems of general interest for public security require companies and public authorities falling within scope to adopt stricter measures to prevent and manage cyber incidents and threats, including appropriate risk-management measures for network and information systems. NIS2 is also relevant to the use of AI from a cybersecurity perspective. The risk-based approach in NIS2 encourages organisations to deploy appropriate and state-of-the-art technologies to strengthen the cybersecurity capabilities of AI and machine learning. AI and machine learning can therefore form part of an organisation's broader cybersecurity strategy, for example for threat detection, monitoring and incident response. At the same time, where AI systems themselves form part of an organisation's network and information systems, their security and associated risks should be incorporated into the organisation's overall cybersecurity risk-management framework.

In addition, the GDPR remains relevant, as it requires organisations to implement appropriate technical and organisational measures to ensure an appropriate level of security for the processing of personal data.

On 19 November 2025, the European Commission published its proposal for the so-called "Digital Omnibus", which brings together a range of amendments concerning digital technologies and seeks to simplify and harmonise key elements of the EU digital regulatory framework. The initiative primarily aims to reduce regulatory complexity and administrative burdens for businesses while increasing legal certainty.

In our point of view, the Digital Omnibus will also be relevant from a cybersecurity perspective, as it proposes amendments to existing EU rules on cybersecurity, data protection and digital technologies. In particular, the proposed changes seek to streamline and simplify compliance with overlapping cybersecurity and incident-reporting obligations. The Commission has proposed, among other measures, a single-entry point for reporting cybersecurity incidents and data breaches.

For AI systems, this broader regulatory simplification may

affect the interaction between the AI Act and other cybersecurity frameworks, including NIS2, where applicable, DORA and the Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act). The practical impact will depend on the final legislative outcome and the extent to which the proposed amendments modify or clarify the respective obligations.

9. Is the use of artificial intelligence insured and/or insurable in your jurisdiction, including with cyber policies? Are there market trends, or limitations?

The AI Act requires notified bodies responsible for carrying out conformity assessments to have appropriate liability insurance. Although the AI Act does not impose a general insurance obligation on all AI users, taking out insurance policies, including cyber insurance, is strongly recommended in practice as part of a broader risk-management strategy.

In practice, several insurance products covering AI-related risks and potential damages are available on the Belgian market. Some insurers such as Vanbreda, among others, are specifically positioning themselves in the market by offering coverage for AI-related incidents.

10. Can artificial intelligence be named as an inventor in a patent application filed in your jurisdiction? If not, what is the current legal position?

No. According to the Paris Convention of 20 March 1883 for the protection of industrial property and the Belgian Code of Economic Law, any natural or legal person, as well as any company assimilated to a legal person, may file a Belgian patent application, irrespective of their nationality or place of residence. As artificial intelligence is neither a natural person nor a legal person, it cannot file a patent application and therefore cannot be designated as an inventor. Moreover, according to Article XI.9 of the Belgian Code of Economic Law, the person applying for a patent is considered to be an inventor.

Accordingly, under Belgian law, an AI system cannot be designated as the inventor in a patent application. The inventor must be a human being, i.e. a natural person. This was also confirmed by the European Patent Office in 2021 in the DABUS case.

11. Do images or works generated by and/or with artificial intelligence benefit from copyright protection in your jurisdiction? If so, who is the authorship attributed to, and under what conditions?

Under Belgian law, only a human being, i.e. a natural person, can be considered an author (Article XI.170 of the Belgian Code of Economic Law). AI systems therefore cannot claim copyright protection for creations they have generated.

Belgian copyright law protects original "literary and artistic works". In a series of judgments, including Infopaq, Painer and Brompton Bicycle, the Court of Justice of the European Union has clarified that originality requires an "author's own intellectual creation" reflecting the author's personality. This interpretation presupposes human authorship.

For AI-generated images, copyright protection may arise where the work meets the originality requirement. This requires the work to constitute the author's own intellectual creation, reflecting its personality and resulting from its free and creative choices. An AI system acting autonomously cannot satisfy this requirement. Accordingly, authorship must be attributed to a human creator, insofar as that person has made the creative choices necessary to qualify as an author.

When assessing the copyright protection of AI-generated output, it is therefore important to distinguish between different degrees of AI involvement:

- **AI as a mere tool:** Where AI is used as a technical tool under the direct control of a human user, comparable to a camera or word processor and the creative choices are predominantly made by the human user, the resulting work may qualify for copyright protection. In such cases, the human user may be regarded as the author.
- **Human–AI co-creation:** Where both the human and the AI system make substantial creative contributions, the legal position is more complex. Copyright protection may extend to those elements of the work that result from the human creator's own creative choices, but not to elements generated autonomously by the AI system.
- **Autonomous AI creation:** Where a work is generated almost entirely autonomously by an AI system, with minimal or merely trivial human input (for example, through the use of a

simple prompt) copyright protection is considerably more uncertain. If there is no identifiable human "author's own intellectual creation", the work may fail to meet the originality requirement under EU and Belgian copyright law.

12. What are the main issues to consider when using artificial intelligence systems in the workplace? Have any new regulations, or guidelines, been introduced regarding AI-driven hiring, performance assessment, or employee monitoring?

AI raises important risks in several areas. It may affect human rights, particularly privacy, non-discrimination, representation and dignity. AI can also reproduce and amplify existing biases and inequalities, for example where insufficiently representative or outdated data is used in recruitment, potentially resulting in discriminatory (employment or financial) decisions.

AI may also contribute to harassment, for instance through deepfakes or inappropriate comments about a employees' appearance, sex or race.

Moreover, excessive reliance on AI-based decision-making may affect autonomy and representation of a person, particularly where procedures or recruitment and workforce management become increasingly standardised.

Under the AI Act, certain AI systems used for recruitment, selection, worker management and performance evaluation are classified as high-risk. In this context, the use of AI to infer emotions in the workplace is prohibited, while employers must inform employees and their representatives before deploying certain high-risk AI systems. Existing employment-law obligations continue to apply alongside the AI Act. From an employment-law perspective, AI-based monitoring and control mechanisms must respect employees' fundamental rights, legitimate interests and well-being.

The GDPR also imposes important safeguards. The collection and processing of data by AI systems must comply with data-protection principles. In particular, Article 22 GDPR provides, subject to certain exceptions, a right not to be subject to a decision based solely on automated processing that produces legal effects or similarly significantly affects an individual. Appropriate human intervention must therefore be ensured where the provision applies.

Finally, liability is also an important consideration. Under Belgian civil liability law, damage resulting from a wrongful act or negligence may give rise to an obligation to compensate. Liability arising from the use of AI is broad and may encompass, amongst others, copyright infringement, non-contractual liability, breach of contract and infringements of privacy and data protection rights.

For an overview of certain legislative initiatives relating to the workplace, such as recommendations of Institute for the Equality of Women and Men, the Act of 4 August 1996 on well-being of workers in the performance of their work, collective bargaining agreements (e.g. Nos. 39, 68 and 81) and Directive (EU) 2024/2831 on improving working conditions in platform work, please refer to our answer to Question 3. Please note that additional arrangements or agreements may have been made at sectoral level, of which we have no visibility.

13. What are the main privacy/data protection issues arising from artificial intelligence development and use (including training data)? Have data protection authorities issued guidelines or rulings on artificial intelligence, and what are the key takeaways?

When AI systems process personal data, they must generally comply with Regulation (EU) 2016/679 (GDPR). The Belgian Data Protection Authority emphasises that the GDPR and the AI Act are complementary frameworks and must therefore be applied together.

The GDPR establishes several key principles that are particularly relevant to AI. Lawfulness requires every processing activity to have a valid legal basis, such as consent or a legitimate interest. The data minimisation principle requires organisations to process no more personal data than is necessary for the specific purpose. In addition, organisations using certain high-risk AI systems may need to carry out both a data protection impact assessment under the GDPR and a fundamental rights impact assessment under the AI Act. These assessments help identify and mitigate potential risks to individuals' privacy and fundamental rights.

Several specific challenges may arise in this context. The opacity of AI systems can make it difficult for data subjects to understand how their personal data is processed, which may create challenges in complying with transparency obligations, and, where relevant, to provide valid consent. AI systems may also be capable of identifying individuals by combining or cross-referencing data that, considered separately, may not constitute

personal data. An AI-generated output may itself constitute personal data where it contains information that allows an individual to be identified, directly or indirectly. Such identification may result from the underlying dataset, the algorithm or a user prompt and may, depending on the circumstances, constitute a breach of the GDPR.

Further concerns include the use of scraped data without an appropriate legal basis, manipulation of AI systems by unauthorised persons, inadequate security measures and human oversight. Finally, AI systems may generate unintended bias and discrimination, particularly where the underlying data or algorithms contain existing biases.

14. How is data scraping regulated in your jurisdiction from an IP, privacy and competition perspective? Are there recent precedents addressing the legality of data scraping for training of artificial intelligence systems?

Data scraping refers to the automated collection and storage of information from the internet. Scraping often involves the collection of personal data, which may give rise to risks, for example, in relation to privacy, intellectual property and competition law.

Privacy perspective The legality of data scraping depends on the nature of the data collected, the source from which it is obtained and the purpose for which it is subsequently used. Where scraping involves personal data, the activity falls within the scope of the GDPR and the Belgian Act of 30 July 2018 on the protection of natural persons with regard to the processing of personal data.

A lawful basis under Article 6 GDPR is required for the processing of personal data. Data scraping is considered to be a separate processing activity under the GDPR. In addition, the principles of necessity and data minimisation apply. Organisations should therefore avoid collecting personal information indiscriminately and should be able to demonstrate a specific and legitimate purpose for the data collected. Where information is obtained from sources other than the individuals concerned, the applicable information obligations under Article 14 GDPR must also be considered. Depending on the nature and risks of the processing, a data protection impact assessment may be required, particularly where AI or other novel technologies are involved.

Intellectual property perspective Scraping can also have intellectual property implications. Copyright may protect a database where its structure reflects the author's own intellectual creation. The amount of effort or investment

involved in compiling the database is not, by itself, sufficient to establish copyright protection. Individual items contained in a database may likewise be protected where they meet the originality threshold for copyright perspective.

Where protected material is reproduced through scraping, the prior authorisation of the relevant rightsholder may be required. This can apply even to relatively short extracts where they contain sufficiently original expression, as illustrated by the Infopaq judgment of the Court of Justice of the European Union. Applicable moral rights should also be taken into account.

Even where copyright does not apply, a database may qualify for the sui generis database right where its producer has made a substantial investment in obtaining, verifying or presenting its contents. This right can allow the producer to prevent the extraction or re-use of all or a substantial part of the database. Copyright and sui generis protection may coexist where the respective requirements are satisfied.

The EU rules on text and data mining (TDM) provide important exceptions. Research organisations and cultural heritage institutions may, subject to the applicable conditions, conduct TDM for scientific research purposes. TDM is an automated computer process whereby large volumes of text or data are analysed to identify hidden patterns, trends and relationships. A broader exception is available for other users, including for commercial purposes, provided that the rightsholder has not expressly reserved the relevant rights. These exceptions have been incorporated into Belgian law through the relevant provisions of the Belgian Code of Economic Law.

Competition law perspective Data scraping may additionally raise competition law concerns, particularly where access to data is controlled by dominant undertakings or where scraping forms part of an agreement or practice capable of restricting competition. In such circumstances, the Belgian competition rules in Books IV and V of the Code of Economic Law and Articles 101–106 of the Treaty of the functioning of the European Union may be relevant.

Finally, the AI Act introduces specific restrictions in this area. In particular, it prohibits the targeted scraping of facial images from the internet or CCTV recordings where this is done to create or expand facial-recognition databases. For other forms of scraping used in the development of AI models, providers must take into account any express reservation of rights or opt-out by rightsholders applicable to TDM.

15. To what extent is the prohibition of data scraping in the terms of use of a website enforceable?

In addition to the regulations listed above, the general terms and conditions, terms of use and/or licenses applicable to the websites from which data are scraped should also be taken into account. Such terms commonly restrict or expressly prohibit data scraping, for example through provisions relating to intellectual property, permitted use or automated access. Where a contractual relationship exists between the data scraper and the website operator – such as through acceptance of terms and conditions or where the data are accessible only behind a login – it is important to assess any contractual restrictions governing the extraction and use of the data.

It is therefore important to review the applicable terms of use in advance and, where necessary, obtaining the relevant licenses or permissions before carrying out any scraping activities.

However, under Belgian law, restrictions on the extraction or use of website content will generally only be enforceable if they form part of valid and binding contractual terms. Users must have been given a genuine opportunity to access and review the applicable terms and must have accepted them before obtaining the relevant data. Conditions that are not brought to the user's attention until after access or that are only available upon request, will generally have limited contractual effect. Even where such terms are binding, they must remain consistent with mandatory Belgian and EU law, including the rules governing unlawful contractual provisions.

Contractual restrictions may also be used by rightsholders to reserve their rights in respect of TDM. Such restrictions do not, however, override the statutory exception applicable to TDM carried out for scientific research where the relevant legal conditions are satisfied.

From an AI perspective, the AI Act further requires providers of general-purpose AI models to employ state-of-the-art technical solutions to identify and respect copyright holders' express reservations against the use of their works for TDM. Consequently, website operators and other rightsholders that clearly reserve their rights may have stronger practical means of preventing their content from being used for AI training or other data-mining purposes.

16. Does your country have a regulator or

authority responsible for supervising the use and development of artificial intelligence? What are its powers and enforcement tools?

Belgium does not have a single dedicated regulator or authority responsible for supervising the development and use of AI in general yet. The Belgian Institute for Postal Services and Telecommunications (BIPT), which already regulates the telecommunications and postal sectors, is expected to take on a central role as Belgium's AI supervisory authority, according to the Federal Public Service Economy, which is coordinating the implementation of the AI Act.

However, this framework is not yet formally in place, as the necessary legislation still needs to be adopted by Parliament. It also remains to be determined which authorities will supervise AI applications in areas such as education and employment, which fall partly or entirely within regional competences. The federal government and the Regions are therefore still working towards an agreement on the allocation and coordination of supervisory responsibilities. As a result, the establishment of a fully operational AI supervisory framework and helpdesk may still take several months.

Where AI is used in regulated activities, it may therefore fall under the supervision and guidance of sector-specific regulatory authorities. The Belgian Data Protection Authority also plays an important role in overseeing AI indirectly, particularly where AI systems involve the processing of personal data.

Infringements of the AI Act may result in both non-monetary and financial sanctions. Non-monetary measures may include warnings and orders to publish information concerning the infringement, among other corrective measures. The AI Act also provides for significant administrative fines, ranging from 750,000 EUR to 35 million EUR, or, for companies, 1% to 7% of their total worldwide annual turnover, depending on the nature and severity of the infringement.

17. How widespread is the adoption of artificial intelligence in businesses in your jurisdiction, and which sectors are leading?

According to Eurostat, in 2025, more than one in three Belgian companies (34.5%) used at least one artificial intelligence tool. This proportion rose to three in four among companies with more than 250 employees, confirming that AI is becoming an increasingly strategic tool for large businesses. Technologies for the automated

analysis of written language were among the most common applications, used by almost one in four companies (23%).

18. How is artificial intelligence used in the legal sector, by lawyers and/or in-house counsels? Are AI-driven legal tools widely adopted, and what are the main regulatory concerns?

AI is increasingly becoming part of the legal profession, although the extent and manner of its use vary considerably between law firms. Its applications range from legal research, case-law analysis and document review to drafting, proofreading, information classification, transcription and administrative support. Commonly used tools include LexisNexis and Microsoft Copilot, while solutions such as DeepL and ChatGPT plus may be integrated to assist with translation and multilingual document work. Some firms have also developed proprietary AI applications or chatbots to handle initial client enquiries and provide basic support.

The use of AI is particularly relevant in the context of judicial proceedings. AI systems deployed by or on behalf of judicial authorities to assist with the investigation or interpretation of facts and law are considered high-risk under the AI Act. Their use cannot replace human judgment: ultimate decision-making must remain with a human.

For lawyers, the benefits of AI must therefore be balanced against important practical and legal considerations. Before adopting an AI tool, law firms should carefully review its terms of use, data-processing practices and security arrangements, including what data are used to train or improve the system, where information is stored and who may have access to client or other confidential information. The accuracy and reliability of AI-generated output must likewise be critically assessed, particularly where the output is used in legal advice or proceedings.

Belgian courts have already addressed the use of AI in the drafting of procedural documents, including written submissions. The relevant case law illustrates that the use of AI in legal proceedings requires careful human verification and oversight. AI systems may produce inaccurate information or “hallucinate”, for example by inventing case law. Lawyers (but also individuals who choose to represent themselves) therefore remain responsible for checking the accuracy, relevance and legal validity of AI-generated content before relying on or submitting it to a court.

19. What are the 5 key challenges and the 5 key opportunities raised by artificial intelligence for lawyers in your jurisdiction?

Challenges The increasing use of AI in the legal profession raises a number of regulatory, operational and ethical challenges. Law firms must navigate an increasingly complex regulatory landscape while ensuring compliance with data protection, confidentiality and professional secrecy obligations. At the same time, the allocation of liability between the different actors involved in the development and use of AI tools may be difficult, particularly where AI-generated outputs contribute to legal or business decisions.

Another important concern is the quality, reliability and security of data used by AI systems. Lawyers must critically assess AI-generated information and verify that it is accurate, relevant and sufficiently up to date. This may be particularly challenging where legal information has not yet been fully digitised or is spread across incomplete databases.

The adoption of AI is also likely to change the skills profile of the legal profession. Lawyers will need to acquire sufficient technical and AI-related knowledge to use these tools effectively and to identify their limitations. At the same time, automation may reduce the need for human involvement in certain routine tasks. The relationship between lawyers and their clients is also likely to evolve. Clients increasingly use AI tools to obtain preliminary answers to legal questions, which may create a risk of inaccurate, incomplete or misleading legal information. Lawyers will therefore increasingly need to assess and, where necessary, correct AI-generated information provided or relied upon by clients. This may require lawyers to take a more advisory and corrective role, while also clearly communicating the limitations and risks associated with relying on AI for legal advice.

Another emerging challenge concerns the risk of over-reliance on AI and the potential erosion of professional judgment.

Finally, AI raises broader ethical and equality concerns, including the risk that biased training data or algorithms may result in discriminatory outcomes. Ensuring appropriate human oversight and accountability will therefore remain essential.

Opportunities AI also offers considerable potential to increase efficiency and improve the quality of legal services. It can accelerate legal research by analysing extensive bodies of legislation, case law and other legal materials and identifying relevant information.

AI may also create opportunities for new business models and innovative forms of legal service delivery. Rather than relying exclusively on the traditional hourly billing model, law firms may perhaps develop AI-assisted legal products and platforms that offer clients more predictable, standardised and potentially cost-effective services.

Routine and time-consuming activities, such as document drafting, proofreading, classification and administrative work, can increasingly be automated, allowing lawyers to devote more time to complex legal analysis and strategic advice. AI can similarly facilitate contract review and due diligence by rapidly identifying relevant clauses, inconsistencies and potential risks.

AI-based analytical tools may further assist lawyers in identifying patterns in case law and legal data, generating insights and locating potentially relevant precedents. This could support, rather than replace, professional legal judgment.

Finally, AI can create new opportunities for client service and legal advice, including through chatbots, virtual assistants and digital platforms. These applications can provide initial information, triage enquiries and direct clients to the appropriate legal specialist. AI is therefore not only a tool for improving efficiency, but may also create new advisory roles, particularly in AI governance, compliance and “ethics by design”, while strengthening the competitiveness of legal service providers.

20. Where do you see the most significant legal developments in artificial intelligence in your jurisdiction in the next 12 months? Are there any ongoing initiatives that could reshape AI

governance?

Over the coming year, Belgium’s regulatory landscape for AI is likely to evolve significantly, primarily as a result of the phased implementation of the AI Act. A key priority for the Belgian authorities will be to put the necessary national supervisory and enforcement framework in place.

For organisations using or developing AI, the increasing applicability of the AI Act will require a more structured approach to AI governance and compliance. This will include identifying the applicable risk classification, determining the responsibilities of the different actors involved and putting in place appropriate procedures for documentation, risk management, transparency and human oversight. These issues will be particularly important in sectors where AI applications are likely to qualify as high-risk, such as employment, healthcare, education, financial services and public administration.

Companies and public bodies are also likely to invest more heavily in AI literacy and internal governance structures, ensuring that employees and decision-makers have sufficient knowledge to use and supervise AI systems responsibly.

Further developments are expected at EU and national level, including the continued elaboration of codes of practice for general-purpose AI models, the establishment and operation of AI regulatory sandboxes and additional practical guidance for SMEs and start-ups. These developments should provide further clarity on how organisations can meet their obligations under the AI Act in practice, including the consequences of non-compliance and the practical mechanisms through which violations may be enforced and sanctioned.

Contributors

Nicolas Wesling
partner

nicolas.wesling@lawtree.be

Luna Fasoel
Attorney-by-law

luna.fasoel@lawtree.be

