Legal 500
Country Comparative Guides 2024

Belgium

Artificial Intelligence

Contributor

Simont Braun

Joan Carette

Partner in Digital Finance | joan.carette@simontbraun.eu

Philippe De Prez

Partner in Digital Finance | philippe.deprez@simontbraun.eu

Thomas Derval

Counsel in Digital Finance | thomas.derval@simontbraun.eu

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 are your countries legal definitions of “artificial intelligence"?

AI has not received any legal definition under Belgian law yet. This will change with the future entry into force of the AI Act, a regulation adopted (but still to be published) at the European level. The future Regulation laying down harmonised rules on Artificial Intelligence, or the AI Act, defines , an 'AI system' as “*a machine-based system designed to operate with varying levels of autonomy, that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, 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?

In March 2019, the Belgian government launched AI4Belgium in cooperation with private stakeholders of the industry to develop different work groups around the use of AI. This initiative aims at providing support to politics in the area of ethic and regulations, boost cooperation with the sector in Belgium, develop an ecosystem around the use of AI, propose concrete actions to be taken and foster innovation in the field of AI.

In addition to this national initiative, the federated regional entities have each adopted a strategy for AI:

- In Brussels: the Brussels government adopted an AI policy and created FARI, an institute to boost research around AI.
- In Flanders: the Flemish government adopted the Flemish AI plan in March 2019.
- In Wallonia: the Walloon government created the DigitalWallonia4.ai programme in July 2019 and the Agence du Numérique (AdN) in 2015, which leads or coordinates operational or communication actions, based on the Digital Wallonia strategy.

In addition to those, at the end of 2022, the Belgian government defined a national convergence plan for the development of AI. This national strategy focuses on 9 objectives and recommends around 70 actions:

- Promote a trustworthy AI.
- Ensure cybersecurity.
- Strengthen Belgium's competitiveness and attractiveness through AI.
- Develop a data economy and a high-performance infrastructure.
- AI at the heart of healthcare.
- AI for a more sustainable mobility.
- Preserve the environment.
- Better, lifelong training; and
- Provide better services and protection to the citizens.

3. Has your country implemented rules or guidelines (including voluntary standards and ethical principles) on artificial intelligence? If so, please provide a brief overview of said rules or guidelines. If no rules on artificial intelligence are in force in your jurisdiction, please (i) provide a short overview of the existing laws that potentially could be applied to artificial intelligence and the use of artificial intelligence, (ii) briefly outline the main difficulties in interpreting such existing laws to suit the peculiarities of artificial intelligence, and (iii) summarize any draft laws, or legislative initiatives, on artificial intelligence.

At national level, there are currently no rules, laws or guidelines specifically applicable to AI in Belgium. This will change with the entry into force of the future AI Act, a regulation adopted (but not yet published) at the European level and which, once entered into force, will be directly applicable in all EU member states.

The AI Act establishes a legal framework based on a risk-based approach. The higher the risk associated with the AI systems operated, the stricter the obligations that apply to their providers. The AI Act categorises AI systems into different risk levels:

- Unacceptable risk: this category includes AI systems that pose a threat to individuals. Examples of such systems include social scoring systems and real-time and remote biometric identification systems. These types

of AI systems will be prohibited.
- High risk: this category includes all AI systems that, without being considered as high risk, have a significant impact on safety or fundamental rights. High-risk AI systems will be regulated and will have to undergo a thorough assessment before they can be introduced on the market. Once on the market, they will be subject to continuous monitoring.
- Limited risk: this category encompasses AI systems that do not qualify as high—risk AI systems. The AI Act introduces transparency requirements towards users, ensuring that they are clearly informed that they are engaging with AI systems, that they are being exposed to a biometric categorisation or emotion recognition system or that are interacting with image, audio or video contents manipulated or generated by AI systems. After being informed that they are interacting with a machine, users are free to choose whether they continue using them or step back.

In addition to those rules on AI systems, the AI Act introduces rules applicable to general-purpose AI (GPAI) models. GPAI models are AI models that display significant generality and are capable of performing a wide range of distinct tasks regardless of the way the model is placed on the market and can be integrated into a variety of AI systems or applications. They do not constitute AI systems on their own. Large generative AI models are a typical example of a general-purpose AI model, given that they allow for flexible generation of content (such as in the form of text, audio, images or video) that can readily accommodate a wide range of distinctive tasks. Under the new AI Act, GPAI systems, in particular large generative AI systems, such as ChatGPT, must comply with transparency requirements (obligation to inform the user that the content is generated by AI) and must be accompanied with measures preventing the generation of illegal content. Finally, their providers are required to publish summaries of copyrighted data used for training.

The AI Act is expected to be published in the Official Journal of the European Union in July 2024. Twenty days later the AI Act will enter into force. Once in force, it will become applicable in distinct stages. Provisions relating to prohibitions on unacceptable risks will be applicable six months after it enters into force. The governance rules and the obligations for general-purpose AI models will become applicable after twelve months and the rules for high-risk AI systems – embedded into regulated products – will apply after thirty-six months. The rest of the provisions of the AI Act will be applicable after 24 months.

Aside from the AI Act, specific non-contractual liability rules governing AI systems are currently being discussed at the EU level (see in particular the proposal for a directive on adapting non-contractual civil liability rules to artificial intelligence ("AI Liability Directive")). If adopted, the AI Liability Directive will impose new tort liability regime and AI-dedicated rules on liability in tort throughout the EU, including new rules in terms of disclosure of evidence, burden of proof, and presumption of causal link adapted to damages resulting from the use of AI systems.

Other more specific legislative initiatives are currently ongoing at the European level, but they regulate more specific uses of AI. In March 2024, a provisional agreement was reached on a proposal for a Directive that aims to improve working conditions for individuals who perform work through a digital labour platform on the basis of a contractual relationship between the individual and the digital labour platform or intermediary (platform work). Amongst others, the proposal regulates the use of algorithms in the context of worker management by digital labour platforms.

In addition to those specific legislations, the laws that could potentially apply to AI can take many forms. In general, and in the absence of a specific definition of AI, when applying existing laws and qualifying AI products or services, AI will be considered as a software or more generally a digital service (see Q4 on conformity of digital services).

4. Which rules apply to defective artificial intelligence systems, i.e. artificial intelligence systems that do not provide the safety that the public at large is entitled to expect?

While the future AI Act (Regulation adopted at the European level, still to be published, and which will be directly applicable in all EU member states once in force) does not directly address the question of defective AI systems, it creates a legal framework ensuring that AI systems put on the market are safe for the public to use. Failure to comply with the AI Act requirements may lead to national supervisory authorities imposing fines, issuing binding orders up to ordering certain AI practices to be stopped entirely.

In addition to those considerations, general rules governing defective products or services may be relevant to AI systems. These may be summarised as follows:

- Product liability (Law of 25 February 1991): defective AI systems can be subject to product liability laws in Belgium. Under that law, manufacturers may be held liable for the damage caused by a defect of their products. If an AI system qualifies as a product and is defective (which may be the case if it is incorporated in a tangible good), the manufacturer may be held liable for any harm or damage caused to individuals or property (see also Q5). In March 2024, the EU Parliament formally endorsed a new directive on liability for defective products. The directive will now also have to be formally approved by the Council before it will be published. Under the current draft, the notion of product is not limited to tangible goods but also includes digital manufacturing files as well as software. It is therefore expected that AI systems will also qualify as a 'product' (even without being incorporated into a tangible good) and will fall within the scope of the new product liability directive once adopted.
- The failure or malfunctioning AI systems intended to be used as safety components in the management and operation of critical digital infrastructure, may be subject to Directive (EU) 2022/2557 on the resilience of critical entities. Their failure or malfunctioning may put at risk the life and health of persons at large scale and lead to appreciable disruptions in the ordinary conduct of social and economic activities. By 17 October 2024, Member States should have transposed this Directive (EU) 2022/2557.
- Consumer protection and legal warranty: defective AI systems may also be handled from a consumer protection perspective. In particular, Belgian law has transposed EU Directive 2019/770 on certain aspects concerning contracts for the supply of digital content and digital services and EU Directive 2019/771 on certain aspects concerning contracts for the sale of goods within Article 1649bis to 1649octies and Book III, Title VIbis of the Belgian Civil Code. Under these provisions, conformity of digital content or services (including AI systems) is assessed under an objective conformity criterion (i.e. comply with what the public at large is entitled to expect from AI systems of the same nature) and a subjective conformity criterion (i.e. comply with what has been specifically agreed upon with the consumer). If an AI system is considered to be in non-conformity, consumers may seek remedies (e.g. having the AI system brought in conformity, price reduction, or contract termination).
- Privacy and Data Protection: AI systems often process personal data, and their defects may result in privacy breaches or data protection violations. In Belgium, the EU General Data Protection Regulation (GDPR) applies and imposes obligations on organisations handling personal data. If a defective AI system leads to unauthorised access, data breaches, or other privacy violations, individuals may seek compensation or other remedies under the GDPR.

5. Please describe any civil and criminal liability rules that may apply in case of damages caused by artificial intelligence systems.

Under Belgian law, there are no specific civil or criminal liability rules governing AI systems. Both the law of contract and the law of tort was recently reformed in Belgium, but no specific attention was given to AI-related liability. Only provisions of general law apply, and it remains to be seen how the courts will handle damage caused by AI systems.

At this stage and from a civil liability standpoint, there seems to be a general understanding amongst scholars that the following sources of liability would be the most relevant (this may however not be exhaustive):

- **Manufacturer's liability**: the Law of 25 February 1991 on product liability (soon replaced by Articles 6.41 to 6.53 of the Civil Code), transposes the EU Directive 85/374/CEE into Belgian law. Under this regime, the manufacturer of an AI system could be held liable for the harm or damage caused to a person or to goods by a defect in its product (the notion of which covers tangible goods and software).
- **Seller's liability and warranty regime**: under Belgian law (Article 1582 et seq. of the former Civil Code), the seller is expected to deliver goods that conform with the agreement. A seller may be found liable for hidden defects and issues of non-conformity. The seller's duties are further increased in the case of a B2C sale as consumer protection rules may further apply and prevent the seller from limiting its liability (Article 1649*bis* of the former Civil Code).

- **User's liability in tort**: the user of defective things may be held liable for the damage caused by the thing's defect (Article 1384 of the former Civil Code, soon replaced by Article 6.16 of the Civil Code), even if the user did not commit any wrongdoing as such. In principle, the notion of "thing" only covers tangible goods, but this could apply in the case of damage caused by a tangible good incorporating an AI system (e.g. a physical machine controlled by AI). An AI user may also be held liable if he/she wrongfully uses a (non-defective) AI system to cause damage (Article 1382 of the former Civil Code, soon replaced by Article 6.5 et seq. of the Civil Code).
- **User's liability in contract**: under general contract law rules (Article 5.230 of the Civil Code), the person using a thing/item to carry out a contractual duty is contractually liable for a breach caused by a defect in the thing/item 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 addition, in specific cases (e.g. damage caused by autonomous vehicles), other more specific provisions will apply.

Aside from those national rules, specific non-contractual liability rules governing AI systems are currently being discussed at the EU level (proposal for a directive on adapting non-contractual civil liability rules to artificial intelligence ("AI Liability Directive")). If adopted, the AI Liability Directive will force EU Member States (Belgium included) to adapt their tort liability regime and implement AI-dedicated rules on liability in tort. The AI Liability Directive could lead to brand new rules in terms of disclosure of evidence, burden of proof, and presumption of causal link.

As for criminal liability, there are no rules adapted to criminal liability in cases of damages caused by AI systems, making it difficult to establish one's liability for this type of damages. Some scholars even argue that courts could use the theory of attribution, meaning that the person or entity liable for damages caused by AI systems is the one to whom the punishable behaviour could be objectively and subjectively attributed. However, it remains to be seen how the Belgian legislator and the courts will apply existing criminal legislation in cases involving damages caused by AI systems.

6. Who is responsible for any harm caused by an AI system? And how is the liability allocated between the developer, the user and the victim?

See Q5 for the various (most) relevant liability regimes.

Different (cumulative) liability regimes may be triggered depending on the circumstances. Some of these liability regimes trigger the user's liability, whereas others target the seller or the manufacturer (which could cover the program developer).

Normally, the victim is not liable for its own damage, with two key exceptions:

- the victim has agreed to a liability clause (it should however be noted that liability clauses are likely to be deemed abusive and void in a B2C environment).
- the victim has committed negligence (e.g. misuse of the AI system). In such a case, the victim will be solely or jointly liable with other parties, depending on the circumstances. In principle, the allocation of the liability is decided using the criterion of the contribution to the damage.

7. What burden of proof will have to be satisfied for the victim of the damage to obtain compensation?

As a rule, the party seeking compensation is responsible for bringing evidence of the conditions supporting his/her claim (Article 8.4 of the Civil Code). This principle is nuanced by the fact that, in court, all parties must contribute to the good administration of evidence (Art. 8.4, 2nd indent, of the Civil Code).

In principle, claims must be proven with a reasonable degree of certainty to be considered established.

Depending on the liability ground invoked (see Q5), the elements to prove may vary and be more or less complex to establish.

It is worth mentioning that in principle, parties may contractually reallocate the burden of proof, with the noticeable exception of B2C contracts, where such reallocation is generally deemed abusive and void (Article VI.82 et seq. of the Code of Economic Law).

8. Is the use of artificial intelligence insured

and/or insurable in your jurisdiction?

Yes, it is. Several players active in the Belgian insurance market already offer insurance products covering AI-related risks and potential damages.

9. Can artificial intelligence be named an inventor in a patent application filed in your jurisdiction?

No. The inventor named in a patent must be a human being. Currently, Belgian law is silent on AI inventions.

Before the European Patent Office, the legal concept of inventorship requiring a human being to be the inventor was challenged when two applications indicating an AI system (DABUS) as the inventor were filed. In 2019, the EPO refused these applications (EP 18275163, EP 18275174) on the grounds that the EPC requires the inventor to be a natural person. The applicant filed appeals which were dismissed by the EPO Legal Board of Appeal in oral proceedings on 21 December 2021 (cases J 8/20 and J 9/20). The Legal Board confirmed that under the EPC the inventor must be a person with legal capacity and that a statement indicating the origin of the right to the European patent must specify the inventor's successor in title.

Inventions in the field of AI may be considered computer-implemented inventions.

AI can also be used as a tool in the inventing process, but the usual legal requirements will apply when assessing the validity of a patent, notably in terms of inventiveness and sufficiency of disclosure.

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

Insofar the images fulfill the condition of originality, which means they are an intellectual creation of the author reflecting his personality and expressing his free and creative choices in the production of that image, they will benefit from copyright protection. The condition of originality cannot be fulfilled by a machine or an artificial intelligence acting alone. The authorship of the image will be attributed to the creator, who is a human being or physical person.

This matter and its consequences are of course debated in view of the technological (r)evolution.

11. What are the main issues to consider when using artificial intelligence systems in the workplace?

AI raises important risks in terms of:

- **Human rights**: especially in the domain of privacy, non-discrimination, representation and dignity.
- Biases: AI can multiply and systematise existing human biases, inequalities or discrimination by formalising rules for management processes based on them, e.g. by using insufficient representative data or outdated data in the hiring and recruitment process, leading to unfair employment decisions.
- Harassment: AI programs could make inappropriate comments about a worker's appearance, sex or race which could lead to (criminal) punishments.
- Autonomy and representation: systematically relying on AI-informed decision-making in the workplace can reduce employee autonomy and representation, especially if AI-based hiring also leads to a standardisation of employee profiles.
- **Employment law**: AI-based control and monitoring mechanisms must respect legitimate interests and fundamental rights of workers (also well-being) at work. In addition, specific HR rules can indirectly impact the use of AI, such as CLA No. 39, under which all employers with at least 50 employees must provide inform and consult its employees on the social impact of the introduction of a new technology in the working environment, before the new technology is implemented. Employers who do not respect these information and consultation procedures may not unilaterally terminate the employment contracts for reasons related to the introduction of the new technology. This sanction may be particularly relevant if the employer uses a new AI technology to measure employees' work and performance, which could influence decisions to terminate employment.
- **GDPR and privacy**: the collection and curation of data by AI systems can raise concerns in terms of privacy. In addition, under Article 22 of the GDPR, a person has the right, in principle, not to be subject to a decision based exclusively on automated processing,

including profiling, and producing legal effects concerning him or her or significantly affecting him or her in a similar way. In that case, human intervention should be provided.
- **Liability**: Belgium has a civil law liability regime under which any tort or negligence, without which the damage would not have occurred, must in principle be compensated.

For the specific situation of the use of algorithms by digital labour platforms, we refer to our answer to Q1.

12. What privacy issues arise from the use of artificial intelligence?

When they process personal data, AI systems must generally comply with Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR). Specific issues may arise due to the opacity of the processing by the AI system, with as consequence that the data subjects do not understand (nor have they consented) to the processing of their data. Another issue may arise from the ability of AI systems to identify persons through the crossing of seemingly non-personal data.

13. How is data scraping regulated in your jurisdiction from an IP, privacy and competition point of view?

Privacy point of view: Data scraping, or the technique whereby a computer program extracts data from human-readable output, like a website, and transfers to and saves this data in a structured format, such as a database or spreadsheet, is subject to both the directly applicable European General Data Protection Regulation (GDPR) and the Belgian Act of 30 July 2018 on the protection of natural persons with regard to the processing of personal data or (Act of 30 July 2018).

Processing of personal data is only permitted if you have a legal basis for doing so. Article 6 GDPR outlines the legal grounds for data processing, which include obtaining the data subject's consent, fulfilling a task carried out in the public interest, or having a legitimate interest in processing the data where such processing is necessary to achieve that interest.

In addition, the general principles relating to processing of personal data of Article 5 GDPR and Article 28 of the Act of 30 July 2018 apply to data scraping. In particular, both articles provide that the processing of personal data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation'). Gathering all personal data on a webpage without a specific purpose is therefore not compliant with this principle.

Article 14 GDPR on the provision of information to the data subject where personal data have not been obtained from the data subject and Article 37(1) of the Act of 30 July 2018 apply equally to data scraping. Article 35 GDPR prescribes that where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons, the controller must, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. This assessment should in particular be carried out when using new technologies like AI. Also, Article 59(1), 2° of the Act of 30 July 2018 provides that the controller or processor must consult the competent supervisory authority before the processing of personal data is incorporated into a new file when using new technologies.

IP point of view: In the context of data scraping, the copyright rules are also applicable to the sources the data scraper uses, like databases, provided that the source is original, i.e. through the selection and arrangement of its contents, it constitutes an intellectual creation unique to its author. The fact a lot of labour and investment went into compiling the database is not in itself enough to meet the requirement of originality. Copyright may also apply to the content (the elements) of the database, if these elements are original. The consequence of an applicable copyright is that prior authorisation of the author will be required for the source to be reproduced, for example by data scraping. This applies even for the reproduction of a sentence, if it is considered original (see the Infopaq judgement of 16 July 2009 of the Court of Justice of the EU (C-5/08), which found that even an excerpt of 11 words might be protected by copyright). The author also has a moral right to the database and the elements.

If the database is not original, the database producer may potentially still benefit from a sui generis protection, i.e. a specific protection to prevent competitors from appropriating databases or parts thereof. The sui generis right results from the implementation of the EU Database Directive and applies to databases that are the result of a qualitatively or quantitatively substantial investment. This investment consists of the use of significant financial, technical or human resources (such as the involvement of qualified personnel or the acquisition of specific technical equipment) to create the database. The

database creator is entitled to prevent extraction and/or re-utilization of the whole or a substantial part of the contents of that database. A database can be protected by both the sui generis database right and copyright.

Articles 3 and 4 of the Digital Single Market (DSM) Directive introduce exceptions to copyright and sui generis database rights, specifically for the purpose of text and data mining (TDM). Article 3 allows research organisations and cultural heritage institutions to perform TDM on works they have lawful access to, solely for scientific research purposes. Article 4 extends this exception, permitting any individual or entity with lawful access to use TDM for any purpose. However, the exception in Article 4 is limited by the condition that the rightsholder has not expressly reserved their rights. These provisions are transposed in Belgian law through, inter alia, Article XI.190, 20°, Article XI.191/1, 7° and Article XI.191/2, 3° of the Code of Economic Law.

Competition point of view: The general Belgian rules on competition law, as found in Books IV and V of the Code of Economic Law, and the European competition rules of Articles 101-106 TFEU apply.

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

In Belgium, the general principles of contract law apply. For a prohibition to be enforceable, the Terms of Use (ToU), Terms of Service (ToS) or terms and conditions must be binding. These terms are binding if the website user had actual knowledge or at least a reasonable opportunity to have actual knowledge of the terms and accepts these terms prior to accessing the data available on the website. This implies that if the terms are only made available upon request, that they will not be binding. These terms must adhere to all applicable laws and regulations. For instance, the provisions on unfair contract terms.

Additionally, text and data mining (TDM) may be contractually ruled out by rightsholders, except for TDM conducted for scientific purposes.

15. Have the privacy authorities of your jurisdiction issued guidelines on artificial intelligence?

The Belgian Data Protection Authority (DPA) has not as such published guidelines on AI. However, it occasionally responds to questions or issues opinions and recommendations on matters involving AI and privacy.

In its 2022 annual report, the DPA recognises the growing importance of issues relating to AI and, above all, the expectations of citizens regarding the various problems that these new technologies may cause. Still in 2022, the DPA intervened in a case involving the use of AI (see Q15).

In addition, the Belgian DPA has issued a few advices on draft laws covering the use of AI, looking at them generally in light of the rules applicable to automated decision making (article 22 of the Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR)) or the proportionality of using AI systems.

16. Have the privacy authorities of your jurisdiction discussed cases involving artificial intelligence?

Yes. The Belgian Data Protection Authority (or Belgian DPA) intervened in a case in collaboration with the French Data Protection Authority (CNIL). However, this decision does not discuss as such the specific problematics linked to the use of AI.

17. Have your national courts already managed cases involving artificial intelligence?

To the best of our knowledge, Belgian courts have not yet had the opportunity to render interesting decisions pertaining to AI.

18. Does your country have a regulator or authority responsible for supervising the use and development of artificial intelligence?

There is no dedicated regulator or authority directly responsible for supervising the use and development in general of AI in Belgium. When used to perform regulated activities, AI may be subject to guidance or regulations from sector-specific supervisor such as those in the financial sector. The Belgian Data Protection Authority also indirectly supervises its use through the angle of personal data.

Moreover, the Belgian government has appointed the Federal Public Service for Strategy and Support (BOSA) to implement specific actions with regard to digitalisation.

In that context, BOSA can issue guidance and or reports that are not binding nor mandatory but are useful to understand Belgium's stance and strategy regarding AI, such as the 2022 National Convergence Plan for the Development of Artificial Intelligence. Built around 9 objectives, the National Convergence Plan aims to develop concrete actions to promote the use of AI in Belgium.

19. How would you define the use of artificial intelligence by businesses in your jurisdiction? Is it widespread or limited?

Depending on the sector, the use of AI has generally seen a steady increase in Belgium in the last few years. According to Eurostat, roughly 14% of Belgian companies already use AI, which is comparatively higher than the European average of 8%. The use is most notable in large companies (more than 250 employees), where nearly half of these companies already use AI. Overall, service sectors tend to use more AI than industrial, construction or trade sectors. AI use is important in ICT-heavy sectors, but is also prominent among publishers, providers of audiovisual services and other industries such as wood, energy, and chemical production.

20. Is artificial intelligence being used in the legal sector, by lawyers and/or in-house counsels? If so, how?

AI tools are already actively used in the legal sector, most notably for: categorising information, assisting with document drafting and text proofing, speech-to-text tools, text retrieval and case law analysis, as well as internal office administration (e.g. Henchman, ChatGPT, Microsoft Copilot). Some of these tools also integrate advanced translation tools such as DeepL to offer full-range services for document review. In addition, some law firms have developed their own AI systems and even chatbots to offer a first line of customer support to existing or potential clients.

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

Challenges:

- Data protection, privacy and confidentiality: the use of AI involves processing (large volumes of) data, which raises challenges for compliance with GDPR and the lawyers' duty to confidentiality.
- Legal responsibility: AI systems may make or suggest decisions that have ethical and/or legal consequences. Determining who bears the responsibility for these decisions and ensuring transparency and accountability can be challenging from a Belgian legal perspective.
- Data quality: access to high quality legal data with AI tools can be a challenge. Lawyers need to ensure that the data they use from AI models is accurate, relevant, and up-to-date, which can require significant effort and resources. In addition, many processes of digitalisation are not yet finetuned in Belgium, leading to incomplete or even non-existent digital databases.
- Job displacement and skill development: lawyers will need to adapt with new skills and knowledge to harness the potential of AI. In addition, new AI technology may lead to job displacement, as tasks which originally are performed by lawyers shift towards execution by AI.
- Ethics and discrimination: the use of AI can lead to legal and ethical questions, particularly when AI systems exhibit certain biases or even discrimination.

Opportunities:

- Legal research and document analysis: AI-powered tools can assist lawyers with comprehensive legal research, analysing large volumes of legal documents, and extracting relevant information, enabling more efficient and accurate legal work.
- Workflow automation and efficiency: AI can automate repetitive and time-consuming tasks, such as document generation, grammar reviews and legal document classification, allowing lawyers to focus on more complex work.
- Streamlined processes: AI can streamline contract analysis and due diligence processes, helping lawyers identify potential risks, inconsistencies, and important clauses in a more efficient and timely manner.
- Predictive analytics: AI algorithms can analyse legal data, precedents, and case outcomes, providing predictive insights to lawyers and suggesting legal sources.
- Enhanced client services: AI-powered virtual assistants, online legal platforms and chatbots

can improve access to legal services, provide basic legal information and guidance, or filtering information so clients can directly be put in contact with the right legal professionals.

22. Where do you see the most significant legal developments in artificial intelligence in your jurisdiction in the next 12 months?

There are currently no specific Belgian laws on AI. On a European level however, the EU AI Act and the Product Liability Directive will shape the Belgian regulatory AI landscape. It is expected that chapter I and II of the AI Act may already apply within the coming 12 months, depending on when the AI Act enters into force.

In addition, the Digital Operational Resilience Act (DORA) will impose additional ICT risk obligations on European financial institutions, which will cover all ICT systems used by financial entities, including AI systems. Therefore, third-party service providers who provide AI systems used by financial entities will fall within the indirect scope of the DORA and will also be impacted by the new DORA requirements.

Contributors

Joan Carette
Partner in Digital Finance
joan.carette@simontbraun.eu

Philippe De Prez
Partner in Digital Finance
philippe.deprez@simontbraun.eu

Thomas Derval
Counsel in Digital Finance
thomas.derval@simontbraun.eu