Legal 500
Country Comparative Guides 2023

The Netherlands
Artificial Intelligence

Contributor

NautaDutilh

Joris Willems

Partner and Head of Technology Group | joris.willems@nautadutilh.com

Sarah Zadeh

Senior associate | sarah.zadeh@nautadutilh.com

Eva Reinders

Senior Associate | eva.reinders@nautadutilh.com

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

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

The Netherlands: Artificial Intelligence

1. What are your countries legal definitions of "artificial intelligence"?

The Netherlands has no official legal definition of artificial intelligence ("**AI**"). However, in March 2018, the Governement submitted a request for advice to the Scientific Council for Government Policy (Wetenschappelijke Raad voor het Regeringsbeleid, "**WRR**") [1] on the impact of AI on public values. The document 'Mission AI: The New System Technology' is part of that advice, and in the document the WRR uses the definition of AI put forward by the EU's High-Level Expert Group on AI:

> *"Artificial intelligence refers to systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals."* [2]

EU-wide, there is also no official legal definition of AI. However, this will change due to the Artificial Intelligence Act ("**AI Act**"), of which the draft text has been approved by the European Parliament on 14 June 2023 and which will now further be negotiated and finalized. The purpose of this horizontal AI regulatory framework is to set harmonized rules at the European level for the development, placement on the market, and use of AI systems as well as to address the risks brought out by AI. The latest amendment of the AI Act proposes the following definition of AI:

> *''Artificial intelligence system' (AI system) means a machine-based system that is designed to operate with varying levels of autonomy and that can, for explicit or implicit objectives, generate outputs such as predictions, recommendations, or decisions, that influence physical or virtual environments"* [3]

Considering the fast technological and market developments related to AI, the definition aims to be as technology-neutral and future-proof as possible. To provide the needed legal certainty, Annex I of the AI Act contains a detailed list of approaches and techniques for the development of AI to be adapted by the European Commission in line with new technological developments. If the AI Act is adopted, the Netherlands will implement the provisions into national laws and regulations. This includes the definition of AI as set forth in the AI Act.

Footnotes:

1. The WRR is an independent strategic advisory body for government policy in the Netherlands and advises the Dutch government and Parliament on long-term strategic issues that are of great importance to society.
2. https://www.wrr.nl/publicaties/rapporten/2021/11/11/opgave-ai-de-nieuwe-systeemtechnologie
3. Amendment 165, article 3 (1) (1) of the Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts.

2. Has your country developed a national strategy for artificial intelligence?

There are currently no laws in the Netherlands regulating AI. However, in October 2019, the Dutch government published its Strategic Action Plan for Artificial Intelligence [1], outlining goals and actions for the Netherlands to take advantage of the social and economic opportunities offered by AI. More specifically, the Dutch government described its intentions to accelerate the development of AI in the Netherlands and to raise its international profile. To achieve its goals, the government cooperates with the Dutch AI Coalition. Companies, government agencies, knowledge institutions, and educational institutions will collaborate in this Coalition to implement new AI actions that help specific domains and sectors. For example, the government states that AI will be of huge importance in solving societal issues, such as the ageing of the Dutch population, climate change, food safety, and health care. At the same time, the government mentions that it should not turn a blind eye to challenges such as protecting fundamental rights like privacy, non-discrimination, and autonomy.

Pursuant to its Strategic Action Plan, the government focuses on the following three 'tracks':

 © 2024 Legalease Ltd

- Track I is to seize societal and economic opportunities. This goal requires intensive public–private partnerships, which will enable the Netherlands to stand out on the European playing field and in global markets. It will be companies, from start-ups and scale-ups to small and medium-sized enterprises and large corporations, that will make the difference in terms of innovation and competitiveness.
- Track II intends to put in their place the required conditions for a fruitful AI climate for the economy and society. These conditions include the necessary knowledge, skills, and training; top-quality scientific AI research, as well as applied research the results of which are useful to businesses and professionals. They also include access to usable data as well as high-quality and smart connectivity.
- Track III is about "Strengthening the foundations". This track concerns the protection of citizens' fundamental rights, as well as appropriate legal and ethical frameworks. As a result, people and companies can feel confident that AI will be used responsibly. It is also important that markets remain open and competitive, and that national security is safeguarded with all AI developments.

Footnotes:

1. https://www.digitaleoverheid.nl/wp-content/uploads/sites/8/2019/11/RapportSAPAI.pdf

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.

AI and ethical principles

The Dutch government is increasingly encouraging the deployment of innovative technologies, such as AI. However, the deployment of these new technologies can have a major impact on public values, such as privacy, non-discrimination, and autonomy. This became painfully clear in September 2018, when the Dutch childcare benefits scandal was brought to public attention. [1] In short, the scandal involved thousands of parents which were falsely accused of fraud by the Dutch Tax Administration (*Belastingdienst*) due to discriminative self-learning algorithms while attempting to regulate the distribution of childcare benefits. The scandal led to great controversy and since then there has been an increasing focus by the Dutch government and within the public sector as a whole on the supervision of AI.

This is also reflected in a parliamentary letter on AI, public values, and human rights, in which the Dutch government discussed the opportunities and risks of AI, as well as existing general policies in which AI occurs. [2] This mainly involves self-regulation of AI by the market and maintaining a dialogue between government, citizens, and business. The government specifically emphasizes and supports a "human-centered approach" to AI. This approach means that respect for public values based on human rights is the starting point behind a purpose, design, and use of AI. AI should reinforce public values and human rights rather than weaken them. [3] In another parliamentary letter, the government mentions that existing regulations are insufficiently focused on AI to adequately mitigate its risks [4].

Additional safeguards need to be put in place and therefore the Dutch government has drafted guidelines, which were published in March 2021, for the application of algorithms and data analysis by government agencies. [5] The purpose of these guidelines is to provide tools for developing and using algorithms by government agencies and to give guidance to educate the public about the governmental development and use of algorithms. All in the context of transparency, explainability, validation, responsibility, and verifiability.

Toolbox for Ethically Responsible Innovation

In 2019, a Toolbox for Ethically Responsible Innovation has been developed by the Ministry of the Interior and Kingdom Relations. This toolbox helps developers to innovate in an ethical manner, and to prioritize important public values and fundamental rights. Based on seven core principles, the toolbox provides advice for each principle, each with references to certain 'tools' (*e.g.* models, methods and guidelines, and practical examples). These offer a starting point for anyone developing or applying new technologies in the public sector. [6] The seven core principles are:

 © 2024 Legalease Ltd

1. put public values at the centre;
2. involve citizens and other stakeholders;
3. respect relevant laws and regulations;
4. ensure quality of data, algorithms, and analysis;
5. be transparent and accountable;
6. monitor, evaluate and adjust if necessary; and
7. pay attention to the safety of technology.

AI guidelines for the financial sector

In July 2019, the Dutch Central Bank (*De Nederlandsche Bank*, "**DNB**") published guidelines containing general principles for the use of AI in the financial sector.11 These guidelines serve as a discussion paper and contain DNB's preliminary views on the responsible use of AI in the financial sector. According to DNB, financial institutions increasingly make use of AI to enhance their business processes and improve their product and service offerings. Although AI enables these financial institutions to enhance their business processes, at the same time AI may also cause incidents that can harm a financial institution and/or its customers and can have serious reputation effects for the financial system as a whole. For this reason, DNB believes that a responsible use of AI in financial services entails that financial institutions should pay due attention to the soundness, accountability, fairness, ethics, skills, and transparency aspects of the AI applications that they develop.

Footnotes:

1. https://www.dutchnews.nl/2021/11/highest-dutch-court-apologises-to-childcare-benefit-scandal-victims/; https://www.tweedekamer.nl/sites/default/files/atoms/files/20201217_eindverslag_parlementaire_ondervragingscommissie_kinderopvangtoeslag.pdf; https://eulawenforcement.com/?p=7941; https://www.theguardian.com/world/2021/jan/14/dutch-government-faces-collapse-over-child-benefits-scandal
2. https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2019Z19125&did=2019D39850
3. https://magazines.rijksoverheid.nl/bz/veiligheidsdiplomaat/2022/04/04
4. https://zoek.officielebekendmakingen.nl/kst-26643-641.html
5. https://open.overheid.nl/documenten/ronl-1411e45f-b822-49fa-9895-2d76e663787b/pdf
6. https://www.dnb.nl/media/voffsric/general-principles-for-the-use-of-artificial-intelligence-in-the-financial-sector.pdf

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?

As mentioned before, the Toolbox for Ethically Responsible Innovation wishes to ensure that during the development and implementation of AI systems public safety and fundamental rights are being prioritized. One of its core principles focuses on the need to give due attention to the safety aspects of technology. It explains that adequate safety measures are about protecting against malicious actors, addressing deficiencies in security processes, and promoting security awareness amongst employees. Therefore, it is crucial to implement security measures at the organizational level, within work processes, technical infrastructure, and software when processing personal data or information.

Furthermore, the guidelines containing general principles for the use of AI in the financial sector12 provided by DNB also address the handling of AI systems that fail to meet the security expectations of the general public. DNB acknowledges that AI can potentially cause incidents that can harm financial institutions and their customers. In doing so, DNB notes that the financial sector is commonly held to a higher societal standard than many other industries, and incidents with AI could have serious reputation effects for the financial system.

Footnotes:

1. https://www.dnb.nl/media/voffsric/general-principles-for-the-use-of-artificial-intelligence-in-the-financial-sector.pdf

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

Civil liability rules

In the Dutch Civil Code (*Burgerlijk Wetboek*, "**DCC**") there is no specific regulation on AI. In essence, the DCC incorporates numerous open standards and should therefore be future-proof. [1] As a result, multiple grounds for liability may be applicable to AI. Under Article 6:185 DCC, the manufacturer is liable for damage caused by a defect in its product. A product is defective if the product (in this case an AI system) does not offer the safety that one may reasonably expect thereof, considering all circumstances. [2] A preliminary question that arises in the light of an AI system and product liability is whether software can be regarded as a product. However, it is

 © 2024 Legalease Ltd

assumed that software included in a tangible product and which serves the functioning of that product, falls under the product liability regime. This does not answer all conceivable questions about the scope of the product liability regime with respect to software in AI systems. After all, the manufacturer can also put the software that determines the functioning of an AI system into circulation without being incorporated into the system. This could include non-embedded software or over-the-air updates. [3] The EU Expert Group on Liability and New Technologies has flagged this ambiguity and believes that when (essential components of) a product takes a digital form, the product liability regime should apply. [4]

Article 6:173 DCC may also be a relevant ground for liability. The article states that the possessor of a tangible product is liable if the product poses a special hazard to persons or property and does not meet the requirements that may be imposed on the product under the given circumstances, and this hazard occurs. Any act of fault in the form of insufficient maintenance or careless use is not required, and the possessor will not be able to defend himself by arguing that he was unaware of the defect. [5]

When the previous two grounds for liability do not apply, fault-based liability (unlawful act), as defined in Article 6:162 DCC, can offer a solution. For example, it is illegitimate to put into circulation a product that is not 'fit-for-purpose'. Fault-based liability may require users to take reasonable care when using an AI system. However, fault-based liability may encounter problems, especially for AI systems for decision aid, which are designed to interfere with human decision-making. If AI systems are supposed to enhance human decision-making and we do not understand how they do this, the question is whether humans can be considered negligent for relying on the AI system when it leads to harm. Therefore, the complexity of an AI system can make an injured party's burden of proof disproportionately complex and expensive.

Considering all of the above, in September 2022, the European Commission presented a proposal to revise the Product Liability Directive. This proposal was published simultaneously with the proposal on adapting non-contractual civil liability rules for AI (the "**AILD**"). [6] Both proposals are aimed at creating legal certainty and legal protection in the digital economy. [7] The revised Product Liability Directive aims at modernising the existing EU harmonised regime on no fault-based liability for manufacturers of defective products. The revised Product Liability Directive regulates, among others, that AI systems and AI-based goods are "products," and fall within the scope of the directive. According to the European Commission, no overlap is intended between claims brought under the proposed no fault-based Product Liability Directive and the fault-based AILD. [8] The proposal is also complementary to existing EU liability and EU safety legislation.

Criminal liability rules

AI could be used as a tool to facilitate actions against real-world targets: (i) predicting the behaviour of people or institutions in order to discover and exploit vulnerabilities; (ii) generating fake content for use in blackmail or generation of phishing material, info stealer payloads and binary scripts for DDoS and ransomware; and (iii) performing feats that human perpetrators are unable or unwilling to do themselves. Although the methods are new, the crimes themselves, such as theft, intimidation, and terror, are not. Alternatively, AI systems may be the target of a criminal activity themselves: circumventing protective systems that present obstacles to a crime; evading detection or prosecution for crimes already committed; making trusted or critical systems fail or behave erratically in order to cause damage or undermine public trust. [9] AI, however, is not explicitly mentioned in Dutch criminal law and criminality depends on the crime committed with the use of an AI system.

Even though AI can also be used to commit crimes, it can also be leveraged for crime prevention or to solve crimes. For example, AI can also be used for law enforcement purposes by the police, legal jurisdictions, and public authorities. Since AI can process vast amounts of personal data and analysis, it is necessary to ensure that the privacy and personal data rights of data subjects are respected. Therefore, in October 2021, the European Parliament adopted a report on *Artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters*. [10] It outlines European views and recommendations on the processing of AI data by public authorities in law enforcement and the judiciary. Among other things, the report mentions that the use of AI not only helps to improve working methods in law enforcement and judicial authorities, but is also useful to fight certain types of crime more efficiently (e.g. money laundering and terrorist financing, online sexual abuse, etc.). [11] In doing so, the report also points out the dangers of AI and calls for more algorithmic transparency, accountability, traceability and verification to ensure AI systems are compliant with fundamental rights. [12]

Footnotes:

1. T.F.E. Tjong Tjin Tai, Aansprakelijkheid voor robots en algoritmes, NTHR 2017.

 © 2024 Legalease Ltd

2. Article 6:186 BW; the presentation of the product, the reasonably expected use of the product and the time from when it was put into circulation should be taken into account. In addition, other circumstances, such as, for example, the availability of alternatives, the seriousness of the hazard and the likelihood that the hazard will occur, and a weighing of the advantages and disadvantages of a product may play a role
3. https://zoek.officielebekendmakingen.nl/blg-942365.pdf
4. Expert Group on Liability and New Technologies – New Technologies Formation 2019, p. 6, 28 and 42-43.
5. https://zoek.officielebekendmakingen.nl/blg-942365.pdf
6. https://commission.europa.eu/business-economy-euro/doing-business-eu/contract-rules/digital-contracts/liability-rules-artificial-intelligence_en
7. https://zoek.officielebekendmakingen.nl/kst-22112-3548.pdf
8. https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/739341/EPRS_BRI(2023)739341_EN.pdf
9. https://crimesciencejournal.biomedcentral.com/articles/10.1186/s40163-020-00123-8
10. https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_EN.html
11. https://eucrim.eu/news/ep-resolution-on-ai-in-criminal-law-and-policing/
12. https://eucrim.eu/news/ep-resolution-on-ai-in-criminal-law-and-policing/

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?

The allocation of liability cannot be fully predetermined, as it may shift depending on the specific circumstances of the case. For example: for the possessor of an AI system a (presumably) important possibility of liability exculpation lies in the second paragraph of Article 6:173 DCC. This provides that the possessor is not liable for the damage caused by a defective good if a defective good also qualifies as a defective product within the meaning of Article 6:185 DCC. This directs liability to the producer of the AI system; if the defect already existed when it was put into circulation by the producer, liability rests on the producer (and not also on the possessor).

As a defective good within the meaning of Article 6:173 DCC will always result in a defective product within the meaning of Article 6:186 DCC, it is quite conceivable that producer liability will become the main rule considering AI systems. [1] However, it will further depend on the specific circumstances of the case, such as the claim(s) involved and the applicable Dutch case law.

Footnotes:

1. A.I. Schreuder, 'Aansprakelijkheid voor 'zelfdenkende' apparatuur', AV&S 2014/20, p. 135.

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

The Dutch Code of Civil Proceedings (*Wetboek van Burgerlijke Rechtsvordering*) provides for, in addition to the basic rules on how court proceedings are conducted, the rules on (civil) evidence. The main rule is set forth in Article 150 of the Code of Civil Proceedings, which states that the plaintiff must prove its assertion and its claim. It is up to the defendant to dispute these assertions with reasons. Regarding AI, however, this burden of proof can make it impossible for the plaintiff to prove liability, or to get compensation. After all, because of the specific characteristics of AI, such as complexity, autonomy and opacity of AI, it can be increasingly difficult for the party that suffered damages from an AI system, to prove either the damage, a fault of the liable person, and a causal link between that fault and the damage, or to prove the damage, the defect and the causal link between the damage and the defect. [1] There are, however, possibilities to ease the burden of proof of the plaintiff. An example is the so-called evidentiary presumption. This means that an assertion is presumed to be proven unless the contrary is proven. Proving the contrary rests with the defendant. Evidentiary presumptions have several purposes, including protecting the injured party in the case of product liability.

As mentioned, the revised Product Liability Directive regulates that AI systems and AI-based goods are "products," and fall within the scope of this proposed directive. [2] Product liability is also known as 'strict liability', which means that the injured party can make a claim for damage suffered, irrespective of any fault. However, the burden of proof remains with the injured party, who must prove that the product was defective, that they suffered damage, and the causal link between the damage and the defect. [3] Article 8 of the Product Liability Directive obliges the manufacturer to disclose necessary information in court when the injured person has presented facts and evidence sufficient to support

 © 2024 Legalease Ltd

the 'plausibility of the claim for compensation'. In addition, Article 9 of the Product Liability Directive eases the burden of proof for the injured person by establishing a presumption of defectiveness and causal link under certain conditions.

The AILD, however, will harmonise certain rules for claims outside of the scope of the Product Liability Directive, in cases in which damage is caused due to wrongful behaviour. [4] The AILD would create a rebuttable 'presumption of causality', which should make an injured party's burden of proof less complicated. For instance, Article 4 of the AILD proposes rules about the presumption of evidence and a causal link. If an injured party can show that a) the defendant breached a duty of care, b) it is reasonable to assume that as a result, the operation of the AI system was affected, and c) this gave rise to the damage, then the causal link between the operation of the AI system and the damage should be assumed. The new rules aim to ensure that persons harmed by AI systems enjoy the same level of protection as those harmed by other technologies. The AILD would furthermore give national courts the power to order disclosure of evidence about high-risk AI systems suspected of having caused damage.

Footnotes:

1. https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/739342/EPRS_BRI(2023)739342_EN.pdf
2. https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/739341/EPRS_BRI(2023)739341_EN.pdf
3. https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/739342/EPRS_BRI(2023)739342_EN.pdf
4. https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/739342/EPRS_BRI(2023)739342_EN.pdf

8. Is the use of artificial intelligence insured and/or insurable in your jurisdiction?

Dutch Insurance Law forms part of the Dutch Civil Code and covers as such all areas of insurance, as well as the general rules for insurers and their obligations towards policyholders.

In the Netherlands, different types of insurance coverages are being offered, which can protect various business activities. Also, when certain risks arise in society, insurers may have an incentive to offer products that cover such new risks. The development of digitization and the associated resilience of companies is no exception in this regard, and has been the reason why more insurers have been offering cyber insurances in recent years. [1] There is not a uniform definition of the term 'cyber insurance'. A cyber insurance may cover direct or indirect damage that the policyholder incur to or through digital components of the company. For instance, if the policyholder become a victim of ransomware or theft of company or customer information, but while little is known about this as of yet, it could also involve risks that arise from using an AI system.

Prior to entering into an insurance contract, the policyholder must disclose to the insurer all information which he knows or ought to know and which may be material to the decision of the insurer to underwrite the risk or to underwrite it on particular terms. With respect to AI, this may pose problems. For instance, the complexity of AI makes it difficult to fathom the logic involved, which makes it is difficult for the policyholder to determine what risk the use of AI compromises, let alone to value that risk. It will also be difficult to deflect that risk by entering into an insurance contract or by factoring the potential loss into the cost of the product or service for which AI is used. [2]

Footnotes:

1. https://business.gov.nl/running-your-business/business-management/cyber-security/cyber-insurance/
2. R.E. van Esch, 'De contractuele aansprakelijkheid voor schade als gevolg van het gebruik van kunstmatige intelligentie bij de nakoming van een financiële overeenkomst', FR, afl. 1-2, p. 19.

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

Patent law in the Netherlands is governed by the Dutch Patents Act (*Rijksoctrooiwet*) and the European Patent Convention (**"EPC"**). Patent protection can be obtained for technical entities or processes that are new, inventive, and susceptible to an industrial application. [1] Dutch patent law does not protect AI systems as such, but several aspects of an AI-system can fall within that scope, including inference models, network architectures, and training methods.

The European Patent Office has indicated in their Guidelines for Examination that the algorithms and models are per se considered of an abstract mathematical nature, and mathematical methods are

 © 2024 Legalease Ltd

excluded from patentability when claimed as such. However, this exclusion does not apply when they are included in, for example, a computer program or implemented in a computer. [2] Obviously, there will be a challenge what an applicant actually would want to include in a patent application and therefore disclose to the public.

Whether AI can be named as an inventor in a patent application process, has been addressed by the European Patent Office ("**EPO**"). The EPO refused two applications which extended inventorship to AI, finding that an inventor designated in the application has to be a human being, not a machine. [3] In its decision, the EPO noted that there appears to be an internationally applicable standard that the understanding of the term inventor refers to a natural person, and that numerous courts have issued decisions consistent with this understanding. [4] These decisions were appealed, but by decision in December 2022, the Board of Appeal dismissed the appeal, confirming that the EPC required the inventor to be a person with legal capacity. Legal capacity means the ability, according to a source of law, to be the subject of rights and duties. Whether this legal capacity exists is not governed by the EPC but by national law. Consequently, the Board of Appeal states that against this background, allowing the applicant to designate an entity without legal capacity as inventor would require going beyond the wording of the applicable rules. [5]

Footnotes:

1. Article 2 (1) of the Dutch Patents Act (Rijksoctrooiwet).
2. D. Visser, 'Robotkunst en auteursrecht', NJB 2023/454, afl. 7, p. 504-515.
3. https://www.epo.org/news-events/news/2019/20191220.html
4. https://www.epo.org/news-events/news/2020/20200128.html
5. https://www.epo.org/law-practice/case-law-appeals/communications/2021/20211221.html

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?

The Dutch Copyright Act (*Auteurswet*) automatically protects the copyright of works of literature, science, and art from the moment the work is created, under the condition that the work in question is an original work. The product must bear the personal mark of its creator, which means that it must be a form that is the result of creative human labour, and thus of creative choices, and thus the product of the human spirit. This excludes, in any case, everything that has a form so banal or trivial that no creative work of any kind can be identified behind it. [1] However, the increasing use of generative AI imposes legal challenges in this regard. Generative AI can produce output consisting of works of literature, science, and art. As the output is created by an AI system, the immediate output lacks the creative choices of a human being, and in general such output will not receive any protection under Dutch copyright law. [2] But if the human intervention is concrete and detailed and the AI system created the output under human direction and supervision, there may be protection available for the output. [3] Thus, copyright protection depends entirely on the circumstances in which the output was created.

The foregoing shows that the Dutch Copyright Act and the Dutch Patents Act can most likely only protect certain elements of AI systems. However, there seems to be an option that could protect all elements. The Trade Secrets Directive protects against the unlawful use, acquisition, and disclosure of trade secrets. Most of the Trade Secrets Directive are implemented in the Dutch Trade Secrets Protection Act (*Wet bescherming bedrijfsgeheimen*), while the procedural aspects are regulated separately in the Dutch Code of Civil Procedure (*Wetboek Burgerlijke Rechtvordering*). Based on the broad definition of a trade secret, an AI system probably can be considered to be a trade secret if (i) it is secret due to the fact that is not generally known or accessible; (ii) has a commercial value because it is secret; and (iii) the rightful owner has taken reasonable measures to keep the information secret. [4] Time will tell to what extent this option will indeed provide the necessary protection.

Footnotes:

1. HR 30 May 2008, ECLI:NL:HR:2008:BC2153 C07/131HR (Zonen Endstra/Nieuw Amsterdam).
2. https://www.europarl.europa.eu/news/en/headlines/society/20200827STO85804/what-is-artificial-intelligence-and-how-is-it-used
3. D. Visser, 'Robotkunst en auteursrecht', NJB 2023/454, afl. 7, p. 504-515.
4. Article 1 (a) – (c) of the Dutch Trade Secrets Protection Act (Wet bescherming bedrijfsgeheimen).

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

 © 2024 Legalease Ltd

AI already has been very beneficial for modern-day businesses. But while the benefits of AI in the workplace are extensive, it also poses serious challenges. One challenge of implementing AI in the workplace is that it can sometimes be difficult to find AI experts who can help to deploy and manage the technology. Companies also should ensure that employees are properly trained on how to use AI technology and are made aware of the benefits it can provide, but also for the risks it can cause. Another challenge of implementing AI in the workplace is that it can be expensive. Organizations should carefully consider the cost-benefit of implementing AI and make sure that the benefits outweigh the costs. Data Security is another challenge. Companies should ensure that their data is secure and that AI technology is properly integrated into their existing IT infrastructure. Finally, AI-related data collection can cause implications regarding the privacy of employees (*e.g.* AI-enabled workplace monitoring).

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

For the development, training and use of AI, the input (namely quantitative and qualitative data) is of great importance. Where personal data is processed by an AI system, this is carried out in two distinct phases: the algorithmic training phase and the use phase. During the training phase the AI's algorithm is trained on a set of data, allowing it to create a model by identifying patterns and connections between different data points. In the use phase, this model is applied to the particular use case that the AI was designed for, in order to provide a prediction or classification, assist a human decision or make a decision itself.

As the foregoing shows, personal data is a vital component for the full life cycle of an AI system. [1] And when an entity established in the Netherlands processes personal data or when an entity processes personal data of data subjects located in the Netherlands in relation to the offering of goods or services, or in relation to the monitoring of these data subjects, both the European General Data Protection Regulation ("**GDPR**") and the Dutch Implementation Act of the GDPR (*Uitvoeringswet Algemene verordening gegevensbescherming*, "**UAVG**") apply. Therefore, companies using AI must ensure that they follow the principles of the GDPR. There is, however, a tension between the use of AI and several of these principles, including:

- Processing needs to be transparent (Article 5(1)(a) of the GDPR); controllers are obliged to process personal data lawfully, fairly and transparently. Articles 13 and 14 of the GDPR also contain various notification requirements that specify what individuals must be informed about before their personal data are processed. In the context of the use of AI, these notification requirements include the obligation to inform data subjects about the purposes of processing, their rights in relation to their personaldata and the existence of automated decision-making, including meaningful information about the logic involved and the significance and intended consequences of such processing. However, transparency is a challenge in the context of AI, as the information provided to the data subject must remain simple to be meaningful and context-appropriate. Algorithms, the processing activities and the decision making processes behind the algorithms are by definition complex and will evolve over time. [2]
- Processing needs to be fair (Article 5(1)(a) of the GDPR); this principle covers a number of processing practices and overlaps with the requirement for transparency. It also implies an analysis of whether the processing will impact adversely and unjustifiably the individuals involved. Fair processing requires that controllers consider the likely impact of their use of AI on individuals and continuously reassess it. In particular, fair processing requires that AI systems do not produce bias. It has also been highlighted by the AP that the question of whether or not the output of an AI is "fair" is inextricably linked to both the circumstances at hand and subjective views on justice. According to the AP, "*[a] controller must actively account for and justify why an algorithm is fair and the use of the chosen algorithm does not lead to inappropriate results.*" [3]
- Purpose limitation, data minimisation and storage limitation (Article 5(1)(c) of the GDPR); This principle requires personal data to be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed". By definition, AI systems need large amounts of data to work effectively, especially during the training phase. As such, AI systems may not be able to perform without first being trained on a large data set. While this can be seen as a tension between the use of AI systems and data protection law, as it cannot always be predicted which data

 © 2024 Legalease Ltd

elements may be relevant for the purpose of the system, the principle itself does not limit data processing by referring to a specific volume or set of data elements – it refers to what is "necessary" for the purposes of processing. What personal data is considered "necessary" varies depending on the AI system and the purpose for which it is used.

- Restrictions regarding profiling and automated decision making (Articles 21 and 22 of the GDPR); While there is a general right to object to the processing of personal data in certain circumstances under Article 21 of the GDPR, Article 22 establishes a more specific right for individuals not to be subjected to a decision based solely on automated processing, including profiling, which produces a decision that produces legal effects or has a similar significant impact on an individual. This includes, for example, profiling in the context of a credit check to decide whether to grant an applicant a loan. Automated decision-making is permitted only if: i) it is necessary for the conclusion or performance of a contract between the parties involved; ii) it is permitted by law; or iii) it is based on the explicit consent of the data subject.

Footnotes:

1. https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-hunton_andrews_kurth_legal_note_-_how_gdpr_regulates_ai__12_march_2020_.pdf
2. https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-hunton_andrews_kurth_legal_note_-_how_gdpr_regulates_ai__12_march_2020_.pdf
3. https://autoriteitpersoonsgegevens.nl/actueel/ap-legt-focus-in-toezicht-op-datahandel-digitale-overheid-en-ai

13. What are the rules applicable to the use of personal data to train artificial intelligence systems?

As mentioned, using personal data to train AI systems is subject to the GDPR and the UAVG. Under the GDPR, personal data used for preparing AI systems must be collected and processed transparently and lawfully. The data subjects must be informed about the purpose of data collection, the processing activities involved, and their rights regarding their personal data. Additionally, the GDPR requires that the processing of personal data for AI training purposes have a legal basis, such as a legal basis or the data subject's consent.

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

The AP is responsible for supervising the processing of personal data and thus the application of AI and algorithms using personal data. In 2019, the AP has published a multiple-year vision document about data protection in a digital society. [1] In this document, it describes the developments and risks it will focus on to ensure the protection of personal data. The AP believes the principles of lawfulness, propriety, and transparency provide a good basis for the development and deployment of AI and algorithms to make a positive contribution to society. In addition, the deployment of AI and algorithms must be decent. This means that AI systems are robust and accurate, deployed for the right purposes, and that they do not exclude groups of people. It is also important for oversight and data subjects to understand how data are processed and decisions are made. In that regard, the AP will focus on shaping a system of supervision of AI and algorithms in which personal data are used, which they confirmed in February 2020, in a document that explains how the AP will supervise AI and algorithms.[2]

Footnotes:

1. https://autoriteitpersoonsgegevens.nl/uploads/imported/focus_ap_202-2023_groot.pdf
2. https://autoriteitpersoonsgegevens.nl/uploads/imported/toezicht_op_ai_en_algoritmes.pdf

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

In November 2021, the AP imposed a fine of 2.75 million euros to the Dutch Tax Administration as a result of the Dutch childcare benefits scandal that was brought to public attention in September 2018. [1] As already discussed in the answer at question 3, the scandal involved thousands of parents which were falsely accused of fraud by the Dutch Tax Administration. This was the result of discriminative self-learning algorithms which were used to determine risk-profiles to regulate the distribution of childcare benefits. The AP imposed the fine of 2.75 million euros because with the use of these discriminative self-learning algorithms the Dutch Tax Administration violated several principles of the GDPR,

 © 2024 Legalease Ltd

including processing data of dual nationality. In April 2022, the AP imposed another fine of 3.7 million euros to the Dutch Tax Administration for the use of a fraud signaling system. [2]

Footnotes:

1. https://www.autoriteitpersoonsgegevens.nl/documenten/boete-belastingdienst-kinderopvangtoeslag
2. https://nos.nl/artikel/2424861-recordboete-voor-belastingdienst-vanwege-zwarte-lijst

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

In February 2020, the District Court of The Hague ordered the immediate halt of the system 'SyRI' ("System Risk Indication"), which is an instrument used by the Dutch government that used algorithms to detect various forms of fraud, including social benefits, allowances, and taxes fraud, due to the violation of article 8 of the European Convention on Human Rights ("**ECHR**"). The District Court of The Hague decided that SyRI does not strike a "fair balance" between social interests and the violation of the private life of citizens, as required under the ECHR. [1] According to Article 8 ECHR, the Netherlands also has a special responsibility when applying new technologies, as it must strike the right balance between, in this case, the benefits that algorithms may bring and the violation of the right to a private life through the use of these algorithms. In that respect, the application of SyRI is insufficiently transparent and verifiable, and thus unlawful. This ruling is comparable to the Dutch childcare benefits scandal, as both cases concern the wrongful and unlawful use of algorithms by public authorities.

Another interesting court ruling regarding the application of AI, took place in October 2022. The Trade and Industry Appeals Tribunal (*College van Beroep voor het bedrijfsleven*, "**CBb**"), the highest court in the field of economic administrative law, ruled, amongst other things, that the online bank Bunq was within its right to screen customers with the use of new technologies such as data analysis and AI. [2] The disagreement between Bunq and DNB dates back to 2018. At the time, DNB was of the opinion that Bunq needed to improve the screening of its customers and was failing in its function as a "gatekeeper" with regard to anti-money laundering checks. Bunq wanted to use data analysis and AI as part of its Know Your Customer ("**KYC**") procedure, but the DNB stated that this use not in line with DNB's requirements. With this court ruling, Bunq is able continue to make use of data analysis and AI as part of its anti-money laundering and KYC procedures. The court ruling may also affect other banks, that were obliged to hire an increasing number of employees in recent years to fulfil their gatekeeper-function, for which costs are increasingly weighing on the budget. [3]

Footnotes:

1. Rb. Den Haag 5 February 2020, ECLI:NL:RBDHA:2020:865.
2. CBb 18 October 2022, ECLI:NL:CBB:2022:707.
3. https://nos.nl/artikel/2448856-dnb-moet-inbinden-bunq-mag-klanten-screenen-via-kunstmatige-intelligentie

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

While the Netherlands has no official regulator or authority responsible for supervising the use and development of AI, the Digital Regulation Cooperation Platform ("**SDT**") was launched in October 2021 by the Dutch Consumer & Market Authority ("**ACM**"), the Dutch Financial Markets Authority ("**AFM**"), the Dutch Media Authority ("**CvdM**") and the AP to coordinate enforcement in the digital sector and combine knowledge and experience in this field.51 The SDT wishes to understand the opportunities and risks in the digital society, and put them on the agenda. Think of topics such as AI, algorithms and data processing, online design, personalization, manipulation, and deception. In addition to such studies, the SDT also wishes to be able to take advantage of those opportunities as well as deal with the risks. While doing so, the SDT will keep in mind various public interests. Furthermore, the four SDT members wish to invest collectively in knowledge and expertise, and share these with each other. Finally, they collectively wish to ensure efficient and effective supervision of (European) laws and regulations. In March 2023, it was announced that the SDT would establish, in addition to the Chamber for general consultation, two additional "Chambers" to align supervision of online platforms and AI. These Chambers will also involve other regulators than the four SDT members.

In January 2023, the AP also announced it was creating a new organizational unit: the Coordination Algorithms Directorate, which will be in charge of supervising algorithms and coordinating the work of the various agencies with competencies in supervising algorithms and AI. In the short term, the AP will begin strengthening the existing supervision of algorithms that unlawfully process personal data. The AP will monitor algorithms for

 © 2024 Legalease Ltd

transparency and arbitrary decisions. Some of the AP's duties will include identifying and analyzing cross-sector risks, promoting a joint interpretation of standards in supervisory practice, and establishing a public register for algorithms in the Netherlands. The AP will also be given the authority to impose fines and other sanctions in line with the GDPR.52 The expansion of the AP's mandate to include oversight of algorithms comes after a review of government use of algorithms in the Netherlands (following the Dutch childcare benefits scandal) found that there is often a lack of criteria to guide their development and purpose and a lack of controls in place to govern their use.

Footnotes:

1. https://www.afm.nl/nl-nl/sector/actueel/2023/maart/uitbreiding-digitaal-toezicht-sdt
2. https://autoriteitpersoonsgegevens.nl/uploads/imported/toezicht_op_ai_en_algoritmes.pdf

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

According to research of The Central Agency for Statistics (*Centraal Bureau voor de Statistiek*, "**CBS**"), a Dutch governmental institution that gathers statistical information about the Netherlands, about 45 percent of the large companies in the Netherlands used one or more AI-technologies in 2019. [1] On average, 12 percent of Dutch companies used, for example, speech recognition, machine learning, and pattern or face recognition. Machine learning for data analysis is the most widely used form of AI technology: 6 percent of companies applied this technology in 2019. Not entirely surprisingly, the use of AI increases proportionately with company size. With 8 percent, small companies (with 10 to 20 employees) used AI the least.

More recent data shows Dutch companies are leading the way in the use of AI compared to other EMEA (Europe, Middle East & Africa) countries. [2] Across EMEA, an increasing trend of non-technical users working with AI to make critical business decisions was seen, with 47 percent indicating that their non-technical users have full access to these AI capabilities. In the Netherlands, companies appear to be at the forefront of this trend, with 54 percent indicating that their non-technical users have full access to AI. [3] The survey also examined how companies view the upcoming AI Act. While there has been criticism of the potential impact of the AI Act and its effect on AI innovation, the survey found that nearly 80 percent of Dutch respondents believe the legislation would not hinder innovation, but rather will create new opportunities. The survey also revealed that Dutch companies are well prepared for the AI Act. For example, 74 percent say they are fully aware of the new requirements the legislation will bring, compared to the EMEA average of 68 percent.

Footnotes:

1. https://www.cbs.nl/nl-nl/nieuws/2021/41/bijna-helft-grote-bedrijven-gebruikt-artificial-intelligence
2. The survey, conducted in the Netherlands, the United Kingdom, France, Germany and the UAE, was conducted among more than 700 senior decision makers from companies actively using data science platforms to build and maintain AI-systems.
3. https://digitailing.nl/nederlandse-bedrijven-lopen-voorop-in-het-gebruik-van-ai/; https://industrievandaag.nl/nederlandse-bedrijven-lopen-voorop-in-het-gebruik-van-ai/; https://itexecutive.nl/artificial-intelligence/nederlandse-bedrijven-lopen-voorop-met-gebruik-ai/

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

In the Netherlands, AI has found its way into supporting lawyers and/or in-house counsel with regard to multiple purposes. For example, laywers perform due diligence with the help of AI tools to uncover background information. This includes the processing of legal documents and contract review. Lawyers also use AI for automated drafting of documents, in which software templates create filled out documents based on data input. The use of AI in the legal sector has also significantly facilitated the process of anti-money laundering and KYC procedures. Yet AI also poses some challenges and risks within a professional setting, such as legal and ethical issues, quality assurance, user trust, and human-AI collaboration. For lawyers and/or in-house counsel, awareness of these challenges and risks is becoming increasingly relevant. Therefore, to use AI effectively and safely, it is crucial to understand how AI works before engaging with it. Especially in the legal sector. [1]

Footnotes:

1. https://www.nautadutilh.com/en/information-centre/news/using-chatgpt-and-other-

 © 2024 Legalease Ltd

generative-ai-tools-risks-and-challenges

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

The transformative technology of AI has the potential to revolutionize the legal profession, which presents both challenges and opportunities for lawyers in our jurisdiction.

Firstly, lawyers face the challenge of quality assurance and liability when AI is involved in legal processes. Despite their advancements, AI systems are not infallible, and the errors or biases present in their outputs can carry significant implications. Lawyers face the task of addressing the issue of liability and accountability when AI systems are utilized in legal proceedings, ensuring responsible and ethical use of AI systems.

Another challenge that lawyers face is privacy related. AI heavily relies on extensive datasets to improve its algorithms, raising concerns regarding data privacy and security. Lawyers must address the challenges of data privacy and security when handling personal data. Safeguarding confidential data from unauthorized access, ensuring compliance with data protection regulations, and managing potential risks associated with AI systems have thus become crucial tasks for legal professionals.

Additionally, the rise of AI systems raises ethical concerns. As AI systems become more advanced, there is growing apprehension about their application and the effects they may have on society. Lawyers must confront the challenge of ensuring that AI systems comply with legal standards, uphold client confidentiality and transparency, and avoid biases in AI's input.

Moreover, the need for more transparency can lead to distrust towards AI, creating challenges for businesses aiming to implement these systems effectively. Considering that it is hard to comprehend the internal mechanisms and the reasoning behind AI's decisions, lawyers must advise companies on the significance of fostering transparency in their AI systems, allowing individuals to comprehend their functioning and the factors influencing their decision-making. Finally, lawyers need to acquire a deeper understanding of AI systems to enhance their ability to provide better guidance and advice to their clients.

The challenges above emphasize the importance for lawyers to adapt and embrace the evolving landscape of AI in the legal profession. By actively addressing these challenges and keeping up with legal developments and ethical considerations, lawyers can eventually leverage AI technology to improve their services in a rapidly evolving digital era. In general, we can consider key opportunities such as document management, text editing, and translation services when utilizing AI tools. More specifically, AI-powered analytics tools can analyse large volumes of data, providing lawyers with valuable insights to enhance their case analysis. This includes identifying relevant precedents, patterns, and trends. Furthermore, AI-driven language translation tools can facilitate efficient communication and collaboration across different languages, especially in international cases or when dealing with multilingual clients.

Depending on the field of law, lawyers can employ specialized AI tools to enhance productivity, efficiency, and work quality. These tools can be tailored to address specific needs that attorneys may have within their respective practice areas. For example, in the M&A practice, lawyers can use AI for automated document processing and drafting. AI tools can streamline these tasks, saving lawyers valuable time. They can also use AI for contract review and due diligence background checks. Finally, AI can significantly reduce the time spent on repetitive and time-consuming tasks, allowing lawyers to focus on more complex and strategic aspects of their work.

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

In the next 12 months, a number of important legal developments in the field of AI can be observed in the Netherlands. One of them is the introduction of the AI Act, which, as mentioned before, aims to set out harmonized rules at the European level for the development, placement on the market, and use of AI systems as well as to address the risks brought out by AI. The draft text has been approved by the European Parliament on 14 June 2023, enabling negotiations with the Council and the European Commission to progress further. If the AI Act is adopted, the Netherlands will implement the provisions into national laws and regulations.

Another noteworthy legal development is the enactment of the Digital Operational Resilience Act ("**DORA**") [1], which came into force earlier this year. To this end, it is the first European-level legislative initiative aiming to introduce a harmonized and comprehensive framework on digital operational resilience for European financial institutions. In short, DORA will apply to almost all

 © 2024 Legalease Ltd

regulated financial entities and impose a broad spectrum of ICT risk obligations on such entities, including the risks of AI. However, the scope of DORA is not limited to financial entities. Providers of ICT services considered critical to the financial sector will also come under the direct supervision of a European regulator under DORA.

Finally, the increasing focus by the Dutch government and the public sector as a whole on the supervision of AI will continue. Part of this, as mentioned before, is the supervision of algorithms by the AP and the establishment of the Algorithms Coordination Directorate. [2] In 2023, the AP will receive one million euros for this purpose and the budget rises structurally to 3.6 million euros per year in 2026. For strengthening the existing supervision, the government has structurally reserved 2.61 million euros. Algorithms and AI are also mentioned as one of the focus areas in AP's 2023 annual plan. [3]

Footnotes:

1. Proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) NO 600/2014 and (EU) No 909/2014.
2. https://www.autoriteitpersoonsgegevens.nl/actueel/algoritmetoezicht-ap-van-start
3. https://www.autoriteitpersoonsgegevens.nl/documenten/ap-jaarplan-2023

Contributors

Joris Willems
Partner and Head of Technology Group
joris.willems@nautadutilh.com

Sarah Zadeh
Senior associate
sarah.zadeh@nautadutilh.com

Eva Reinders
Senior Associate
eva.reinders@nautadutilh.com

 © 2024 Legalease Ltd