Legal 500
Country Comparative Guides 2025

The Netherlands
Artificial Intelligence

Contributor

Kennedy Van der Laan

Laura Poolman

Senior Associate | laura.poolman@kvdl.com

Astrid Sixma

Partner | astrid.sixma@kvdl.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"?

There is no official definition of "artificial intelligence" in the Netherlands. However, the Dutch Authority for Digital Infrastructure as "*AI is a collective term for algorithms and methods that perform tasks that were previously thought to require human intelligence. Artificial intelligence refers to systems that exhibit intelligent behavior by analyzing their environment and taking action with a certain degree of autonomy to achieve specific goals*".

In general, the Dutch government aligns the definition of artificial intelligence with that set out in Regulation (EU) 2024/1689 ("AI Act").

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

The Dutch Digitalisation Strategy (NDS), presented on 4 July 2025, is a joint initiative of the Dutch national government, municipalities, provinces, water boards, and public service agencies. It aims to accelerate digital transformation by aligning fragmented efforts under one coherent strategy — acting as one digital government. The NDS complements two other national strategies, namely the Dutch Cybersecurity Strategy (NLCS) and the digital Economy Strategy.

Artificial intelligence (AI) is one of the six core pillars of the NDS, and relates to the following focus points:

- Unified AI policy across government
  - The Dutch government commits to a coordinated national approach to AI within the public sector.
  - This includes shared infrastructure, legal alignment with the AI Act, and cross-sector governance.
- Focus on public sector AI infrastructure
  - Development of open-source, sovereign AI models (e.g. GPT-NL) to reduce dependency on non-European tech providers.
  - Promotion of high-quality public datasets to support trustworthy AI use.
  - Increased availability of compute power (AI infrastructure) for public institutions and R&D.
- Human-centric & responsible AI
  - The strategy underlines the importance of transparent, explainable, and ethical AI, aligned with EU values.
  - Public AI deployments must respect privacy, fairness, and accountability standards.
- Investment in AI talent
  - Programs for AI skills development and retraining of public servants.
  - Dedicated tracks for attracting AI researchers and engineers into the public sector.

Alongside AI, the NDS outlines five other strategic priorities, namely:

- Cloud technology: a shared public cloud marketplace aligned with European standards.
- Data sharing: creation of a federated data infrastructure with domain-specific data hubs.
- Digital services: simplified, proactive, and user-friendly public service delivery for citizens and businesses.
- Digital resilience: enhanced cybersecurity, quantum-safe cryptography, and vendor independence.
- Digital skills and tools: investing in modern digital work environments and public sector digital literacy.

The NDS has not been implemented yet. It is not sure when this can be expected, but it is high on the Dutch government's agenda.

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.

The Netherlands has implemented a mix of binding regulations, voluntary guidelines, and ethical principles related to AI. These are based on both European Union legislation and national initiatives.

- **Binding regulations**: as an EU Member State, the Netherlands has adopted the AI Act, which came into force in August 2024. The Dutch government is currently preparing an AI Implementation Act to establish the national enforcement architecture and clarify responsibilities among supervisory authorities under the AI Act.
- **National guidelines and ethical principles:**
  - **The Dutch Algorithm Register**: public authorities are required to register algorithms used in decision-making processes for promoting transparency and accountability.
  - **Guidelines for transparent and responsible algorithms:** developed by the Dutch Ministry of the Interior and the Dutch Data Protection Authority in its capacity as "AI supervisor" (Algorithm Coordination Department) to cover risk assessments, fairness, explainability, and human control.
  - **Dutch AI coalition:** the *AI Coalitie voor Nederland* (AIC4NL), a national public-private partnership promoting trustworthy, human-centered AI, which has developed practical tools, like the AI Impact Assessment and sectoral ethics guides.
- **Voluntary standards and toolkits:** g., the "Ethics by Design" toolkit, for developers of AI in the public sector, impact assessments for human rights, fundamental freedoms, and societal impact and open-source Dutch-language AI models (e.g. GPT-NL) that meet EU ethical standards.

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?

Dutch law (currently) does not have any dedicated civil liability legislation for defective or malfunctioning artificial intelligence systems (AI systems) causing any harm or losses. Instead, general civil liability principles apply. Below is a short overview of the most relevant applicable frameworks based on general tort law and contract law.

Under tort law, a party injured by a defective AI system can rely on both fault-based and strict liability provisions:

- **Fault-based liability (unlawful act)**: Article 6:162 of the Dutch Civil Code (DCC) is the general tort clause. It makes one liable for harm caused by an unlawful act attributable to them. An unlaw act is considered to be one of the following: an infringement of a right, an act or omission in violation of a legal duty or acting in violation of a general duty of reasonable care.
- **Strict-liability for defective products**: If an AI system or an AI-driven product qualifies as a 'product' within the meaning of Article 6:185 DCC, the producer (manufacturer/ developer) of the product can be held liable for harm based by a defect in the product. A product is considered defective if it does not offer the safety that a person may reasonably expect, taking all circumstances into account. The injured party is not required to prove fault or negligence of the producer, but only that the product (e.g. an AI-driven device or software embedded in a device) was defective and caused the damage suffered.

Under contract law, if an AI system does not meet the standards set out in an agreement or is defective, contract law remedies may apply:

- **Attributable breach**: If a contracting party fails to fulfill its obligations under an agreement, it becomes liable for the resulting damage, unless the failure is not attributable to that party (Article 6:74 DCC). For a breach to be established, it must generally be proved that the breach is the debtor's responsibility (by fault or law). The latter is not the case if the debtor can, for example, prove force majeure.
- **Use of defective tools**: If a party uses a tool or auxiliary item in the performance of a contract, and that item is unsuitable or defective, the resulting failure in performance is attributable to the party who used the item as if it were their own fault (Article 6:77 DCC). This rule is relevant if a party fulfills its contractual duties using an AI system or AI-driven device, as any defects or harm caused by that AI-driven device or system is attributable to its user.
- **Requirement of conformity**: In the context of sales of AI systems or AI-driven products, Article 7:17 DCC requires that a product is in conformity with the purchase agreement. The AI system or product must have the properties and performance that the buyer, given the agreement, could reasonably expect.

5. Please describe any civil and criminal liability rules that may apply in case of damages caused by artificial intelligence systems. Have there been any court decisions or legislative

developments clarifying liability frameworks applied to artificial intelligence?

As noted under question 4 above, no AI-specific civil or criminal liability rules exists under Dutch law as of today. Instead, existing general legal frameworks apply. As far as we are aware, there have been no published Dutch court decisions to date that directly address damages caused by (autonomous) AI systems.

Criminal liability in the AI context also relies on general criminal law principles. Dutch law uses the doctrine of functional perpetration: to attribute criminal acts to those who orchestrated the criminal act or failed to prevent them. In practice, this means if someone deploys an AI system as a tool to commit an offense (for instance, using an autonomous drone as a weapon), that person can be deemed the offender even though the AI performed the act. The criteria are that the person had power over the AI's actions and accepted or consciously allowed the wrongful outcome.

Similarly, if an AI's malfunction causes harm due to gross negligence, a responsible individual might face charges such as negligent homicide or recklessness, provided the legal elements (culpability and foreseeability of harm) are met. As far as is known, no criminal case in the Netherlands has dealt with AI-caused harm, and it remains to be seen how far prosecutors and courts will apply existing law to cover highly autonomous AI behavior. The new Dutch Code of Criminal Procedure (expected in 2026) does not contain special provisions on AI either, indicating that AI has not yet been explicitly addressed in criminal legislation.

The Netherlands is closely following European initiatives on AI regulation. At the EU level, the AI Act imposes strict requirements on high-risk AI systems to prevent harm. In parallel, EU product liability rules are being updated to clarify that software and AI are 'products' and to ease claimants` burden of proof for AI-related damage. As an EU member, the Netherlands will implement these changes in its civil liability regime.

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

Under Dutch law, responsibility for harm caused by an AI -system is determined by the legal regime applied to the case. If product liability (Article 6:185 DCC, see question 4 above) is applied, a manufacturer is to be held liable if the criteria for product liability are met. Under some circumstances, even a distributor or importer may be held liable, if for example the manufacturer is unknown or the distributor or importer branded or marketed the AI system under its own name.

If product liability is not applicable, an injured party may fall back on general tort law. In such case, it must be assessed which party failed to meet the duty of care in the specific case, and on that party the liability will rest. This could be the developer/provider of the AI system (if the algorithm or training data was handled without due care), or the deployer/user of the AI (if it was implemented or supervised negligently). For instance, the deployer/user of an AI-driven system might be held responsible for not preventing foreseeable harm. It is not possible to define a general rule, so any liability must be assessed and allocated on a case-by-case basis.

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

Under Dutch law, the claimant generally bears the burden of proof for the facts that underlie its claim (Article 150 Dutch Civil Procedure Code).

For a typical claim under tort law seeking damages, the claimant has to prove five key elements. These are: (1) that the defendant committed an unlawful act (breach of a right, statutory duty, or unwritten duty of care); (2) that the act is attributable to the defendant (the defendant's fault or responsibility); (3) that the claimant suffered actual damage; (4) a causal link between the act and the damage; and (5) that the violated norm was intended to protect against the type of harm suffered.

In case of a claim based upon strict liability, the law eases the claimant's burden of proof. For example, under Dutch product liability law (Article 6:185 DCC), a producer is liable for damage caused by a defective product even if negligence or fault is missing. In that case, the injured party does not have to prove the producer's fault or negligence, but only that (1) the product was defective, (2) that the claimant suffered damage, and (3) that the damage was caused by the defect.

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

The use of AI is insurable in the Netherlands, but AI-specific policies do not yet exist. Instead, AI-related risks are typically covered under existing insurance categories,

provided that the use of AI complies with applicable legal and regulatory standards (e.g., GDPR, product liability, AI Act).

AI systems can cause material, financial, or data-related harm. In the Netherlands, these risks may be (partially) covered by:

- Professional liability insurance (*beroepsaansprakelijkheid*): for faulty deployment or advice involving AI.
- Product liability insurance: if an AI-driven product causes damage or injury.
- Cyber insurance: for AI-related breaches, data loss, algorithmic bias claims, or cyber incidents.
- Employer's liability: if AI systems harm employees through monitoring or unsafe automation.

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

Under Dutch patent law, artificial intelligence (AI) cannot be named as an inventor in a patent application. The Dutch Patent Act 1995 ("Rijksoctrooiwet 1995") does not explicitly define who or what may be considered an inventor, but it is interpreted in line with the European Patent Convention (EPC), to which the Netherlands is a party. Both legal systems presuppose that the inventor must be a natural person.

The Dutch Patent Office (*Octrooicentrum Nederland*) follows the practice of the European Patent Office (EPO), which has consistently held that only natural persons can be named as inventors. This was confirmed in cases like the EPO's decisions on the DABUS applications (J 8/20 and J 9/20), where it was concluded that an AI system cannot be considered an inventor because it lacks legal personality and does not possess rights or duties.

Therefore, in the Netherlands, while an invention generated with the assistance of AI may be patentable if it meets the usual legal requirements (novelty, inventive step, industrial applicability), the inventor named in the application must be a human being.

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?

Under Dutch copyright law, images generated *solely* by artificial intelligence do not benefit from copyright protection. The Dutch Copyright Act ("Auteurswet") attributes authorship exclusively to natural persons. For a work to be protected by copyright, it must be the result of creative choices made by a human author, reflecting their personal imprint.

If an image is generated *with the assistance* of AI—meaning that a human made creative decisions in the input, selection, or editing process—the resulting image may qualify for copyright protection. In such cases, the authorship and corresponding rights are attributed to the human who exercised sufficient creative control over the process.

Fully autonomous AI-generated works (i.e., those created without meaningful human input) fall outside the scope of copyright protection in the Netherlands, as current Dutch law does not recognize non-human authorship. This interpretation is in line with broader European legal principles and case law.

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

In the Netherlands, the use of artificial intelligence systems in the workplace — particularly for hiring, employee evaluation, and monitoring — is subject to a strict and multi-layered legal framework that combines European regulations and national data protection principles.

Under Annex III of the AI Act, systems used for recruitment, performance monitoring, promotion, or termination decisions are classified as "high-risk AI". Employers (as AI deployers) must comply with obligations including risk management systems, human oversight mechanisms, post-deployment monitoring and documentation and transparency obligations.

The AI Act explicitly bans AI systems that infer emotions or mental states through biometric data in the workplace, except for narrow safety or medical purposes. This includes tools like facial expression analyzers or stress detectors used in interviews or productivity tracking.

Under the AI Act, organisations deploying high-risk AI systems must ensure that the people interacting with or overseeing those systems are adequately trained. This includes HR staff, IT teams, and line managers involved in hiring, monitoring, or disciplinary decision-making using AI.

Employers must have a lawful basis (usually consent or legitimate interest), and meet GDPR principles such as purpose limitation (Art. 5(1)(b)), data minimisation (Art. 5(1)(c)), transparency and information duties (Art. 13–14) and fairness and non-discrimination (Art. 5(1)(a)). Automated decision-making without human review is restricted under Article 22 GDPR, and requires specific safeguards, including the right to obtain human intervention.

The *Autoriteit Persoonsgegevens* (AP) identifies many risks associated with using algorithms and AI in the workplace (link). The AP requires that employee monitoring (through AI) is necessary, proportionate and transparent, is communicated in advance to employees and avoids constant or covert surveillance unless legally justified (link).

Under Dutch labour law and EU directives, works councils (*ondernemingsraden*) may have a right to be informed, consulted or asked for consent before implementing certain AI systems, especially those affecting working conditions or employee privacy. This reinforces the principle of participation and transparency in the introduction of workplace technologies.

No new regulations have been introduced regarding AI-driven hiring, performance assessment, or employee monitoring.

12. What privacy issues arise from the development (including training) and use of artificial intelligence?

The Netherlands recognises several privacy and data protection issues related to AI development and use, based on the General Data Protection Regulation (GDPR) and specific national guidance by the Dutch Data Protection Authority (*Autoriteit Persoonsgegevens* – "AP"). The key issues are set out below:

i. Use of personal data for training AI models

- AI systems are often trained on large datasets that may contain personal data.
- The principle of data minimisation (Art. 5(1)(c) GDPR) requires that only data strictly necessary for the training purpose be used.
- Under Dutch interpretation, the use of personal data for (general-purpose) AI training often lacks a valid legal basis (Art. 6 GDPR), unless consent or demonstrable legitimate interest can be proven. According to the Autoriteit Persoonsgegevens, testing should be performed preferably with anonymized or synthetic data instead of personal data. Only when such is not possible, personal data may be used **if** a legal ground can be invoked.
- A similar issue arises when special categories of personal data are used (e.g., health data). Under the GDPR and Dutch GDPR Implementation Act there is only limited scope for invoking an exception to the processing prohibition in this case.

ii. Lack of transparency and explainability

- AI decision-making may lack explainability, which conflicts with the transparency obligations (Art. 12–14 GDPR) and the right to information for data subjects.
- The Autoriteit Persoonsgegevens emphasizes that automated decision-making with significant impact (Art. 22 GDPR) requires explicit justification and the ability to provide meaningful information about the logic involved.

iii. Automated decision-making and profiling

- If AI is used to make decisions, including profiling, with produces legal effects concerning an individual or similarly significantly affects it, without meaningful human involvement, it may fall under the Article 22 GDPR's restriction. The processing of personal data in this context is consequently as a rule prohibited. Only in a number of exhaustive cases, an exception can be made to this rule.
- Dutch courts and regulators are strict on this point, especially after the SyRI and Toeslagenaffaire cases, where profiling and opaque algorithmic decisions caused major rights violations.

iv. Bias, discrimination, and fairness

- The use of biased training data may lead to discriminatory outcomes, especially in sensitive domains like social services, employment, or policing.
- Dutch interpretation of the GDPR (incl. case law and Autoriteit Persoonsgegevens' guidance) links discrimination risks to unlawful data processing and violations of Art. 5(1)(a) GDPR (lawfulness, fairness, transparency).

v. Purpose limitation and function creep

- Reuse of personal data beyond the original purpose (e.g. using healthcare related data for commercial AI training) is generally not allowed without a new legal ground for such processing activity. Such processing is typically not considered as 'further processing' in terms of Article 6(4) GDPR, but instead a new processing purpose for which a separate legal ground

is required.
- The Autoriteit Persoonsgegevens warns against "function creep," e.g., when datasets collected for public interest are silently reused for AI model training.

13. How is data scraping regulated in your jurisdiction from an IP, privacy and competition point of view? Are there any recent precedents addressing the legality of data scraping for AI training?

Intellectual Property

- **Copyright (*Auteurswet*).** Scraping copyrighted content (e.g., texts, images, source code) without permission is prohibited unless a legal exception applies (e.g., quotation right, parody, or research exemption under Art. 15o Auteurswet for TDM — text and data mining).
- **Database right (*Databankenwet*).** If the scraped source qualifies as a protected database (with substantial investment), scraping may violate the *sui generis* database right. The Dutch Supreme Court (*Hoge Raad*) has ruled that even partial extractions may be unlawful if they interfere with the normal exploitation of the database (Hoge Raad, 17 April 2018, ECLI:NL:HR:2018:856.).
- **TDM exceptions**. EU Directive 2019/790 (*DSM-richtlijn*) implemented in the Netherlands in 2021, allows text and data mining (i) for research purposes (Art. 15n/15o Auteurswet) and (ii) for general commercial use, unless the rightholder explicitly opts out (via metadata or terms). AI training by private entities is only lawful if the scraped content is (i) not protected, or (ii) covered by the TDM exception and not opted-out.

Privacy and data protection

The Dutch Data Protection Authority (AP) has issued in April 2025 updated guidelines in relation to data scraping (link). According to the AP, scraping typically involves the automated collection and storage of information from the internet, and in practice almost always includes personal data, leading to significant privacy risks. The AP states clearly that scraping by private parties or individuals is **almost never** permitted under the GDPR, unless very narrowly targeted, exceptional use cases apply.

The guidance emphasises that public accessibility does not amount to consent: just because information is viewable online doesn't mean it's lawful to scrape it. Where scraping does involve personal data, organisations must satisfy GDPR principles including lawfulness, purpose limitation, data minimisation, transparency, and human rights safeguards. The document highlights that using the legal basis of 'legitimate interest' (Art. 6(1)(f) GDPR) for scraping is usually insufficient, as it is extremely difficult to meet the necessity and proportionality requirements.

An explicit exception is noted for 'household use', where individuals performing scraping for purely personal, non-commercial hobby projects may fall outside GDPR scope altogether. The AP warns that broader or indiscriminate scraping—such as building databases of online profiles for commercial profiling or AI training—will usually breach GDPR requirements.

Organisations are urged to carefully assess the legal grounds, document their decision process, and avoid mass data harvesting unless strict conditions are met. While this guidance addresses private-sector practices, the AP notes it is working on a separate guidance for public sector scraping, recognising that public bodies face similar privacy risks.

Competition law

- **Digital Markets Act (DMA) & Dutch competition law.** Large online platforms (gatekeepers) cannot unjustly block access to publicly available data, but may impose fair access conditions. Conversely, smaller parties scraping data from dominant platforms (e.g., Google, LinkedIn) may still breach terms of use, and platforms may enforce contract law if not abusive. No scraping-specific case law under Dutch competition law yet, but the ACM (Authority for Consumers & Markets) monitors scraping behavior if it harms innovation or competition (e.g. training monopolistic AI models on scraped data).

Recent Dutch/European precedents and developments

- In ECLI:NL:RBAMS:2024:6563, the Amsterdam District Court ruled that an opt out from the Text and Data Mining (TDM) exception (under Article 15o of the Auteurswet, implementing the DSM Directive) must be expressed in a machine readable way, such as metadata—natural language opt outs (e.g., blocking specific bots) were insufficient.

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

In the Netherlands, a scraping prohibition in website terms of use can be legally enforceable. Website terms of use are generally binding if the user has been informed

about the terms and explicitly accepted them (e.g. through a "clickwrap" or login agreement). In cases of "browsewrap" (just by using the site), the terms may not be applicable considering that one of the constitutive requirements under Dutch law for an agreement – acceptance – may be deemed to not have taken place. It is noted though that acceptance can also be tacit, in which case the applicability depends on whether it can be constitute that the user could reasonably be expected to be aware of the terms and have agreed to them.

With automated scraping bots, it's often difficult to prove consent or that the terms were ever seen or accepted. Without a clear acceptance or contractual relationship, enforcing website terms alone becomes legally fragile. However, in such cases the IP-related prohibitions referred to under 13 may still apply.

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

The Dutch Data Protection Authority (*Autoriteit Persoonsgegevens* – "AP") has issued multiple AI-related guidelines, particularly in its role as "AI supervisor" (Algorithm Coordination Department). Key guidance publications are:

- **Report on AI & Algorithms in the Netherlands (periodically issued).** The AI & Algorithms in the Netherlands Report (RAN) examines trends, risks, and control in the use of artificial intelligence (AI) and algorithms. In this fifth edition, the AP focuses on overarching developments, fundamental rights and public values, policy, and regulations. The AP also considers the importance of algorithm registration. (link)
- **AI Literacy**. In these guidelines, the AP discusses AI literacy as a building block for the control of AI systems. Within this framework, AI literacy is also desirable for certain algorithmic processes that do not classify as AI systems. (link).
- **Tools for meaningful human intervention**. These guidelines concern meaningful human intervention, which ensures that there is no decision-making (through AI/algorithms) based solely on automated processing as referred to in Article 22 of the GDPR, and therefore no prohibition under those articles. (link).
- **AP's vision on generative AI (consultation)**. With this vision, the AP aims to contribute to the public debate on generative AI and outline what is needed for its safe and responsible use. (link)
- **Position paper on AI and supervision**. In this position paper, the AP presents ten actions to enable the value-driven use of AI in the Netherlands. These include drawing up a National Delta Plan for algorithms and AI and investing in an ecosystem for sustainable AI innovations. Representatives of the people, the government, and regulators have an important role to play in realizing these actions. (link)

16. Have the privacy authorities of your jurisdiction discussed cases involving artificial intelligence? If yes, what are the key takeaways from these cases?

The Dutch Data Protection Authority (*Autoriteit Persoonsgegevens* – "AP") has addressed two cases which relate to artificial intelligence (AI), as AI systems were used in automated decision-making, profiling, or data collection.

SyRI case (System Risk Indication)

The Dutch government used SyRI to detect welfare fraud through automated risk profiling based on large-scale data. The District Court of The Hague declared SyRI in 2020 unlawful, citing a lack of transparency, explainability, and proportionality (violation of Article 8 ECHR). While the court ruled, the AP supported concerns about opaque algorithmic profiling without sufficient justification.

Takeaway: high-impact AI systems must meet strict standards for transparency, necessity, and fairness — especially in the public sector. (link)

***Toeslagenaffaire* (Childcare Benefits Scandal)**

The Dutch Tax and Customs Administration used automated systems to flag fraud risks among childcare benefit recipients. Discriminatory risk scoring (based on dual nationality), lack of human oversight, and denial of access to information. The AP issued a critical report in 2020, concluding systematic GDPR violations including unlawful profiling, insufficient transparency, and no valid legal basis.

Takeaway: profiling and AI decision-support tools must not result in discrimination and must respect GDPR rights like human intervention (Article 22). (link)

***Risicoscan Verblijf Buiten Nederland* (Risk Scan Stay Abroad)**

Until the beginning of 2023, the Employee Insurance Agency (UWV) illegally monitored the online behavior of people receiving unemployment benefits. Media reports

revealed that the UWV had been using cookie data on unemployment benefit recipients for an algorithm risk-scoring tool called *Risicoscan Verblijf Buiten Nederland* (Risk Scan Stay Abroad). The UWV tracked and analyzed the behavior of visitors to UWV websites to see if they were staying abroad illegally while receiving unemployment benefits. Website visitors were not informed that they were being monitored.

Takeaway: using algorithmic risk profiling without a valid legal basis, transparency, or safeguards violates the GDPR and obliges public bodies to actively remediate harms, including informing affected individuals and restoring rights. (link)

17. Have your national courts already managed cases involving artificial intelligence? If yes, what are the key takeaways from these cases?

Dutch courts have handled several cases involving AI, and they emphasize protecting fundamental rights and requiring transparency in AI systems. For example, in 2020 the District Court of The Hague struck down the government's fraud-detection AI system SyRI as unlawful, ruling it violated citizens' privacy rights under the European Convention on Human Rights. And in 2021 (affirmed on appeal in 2023) the Amsterdam court ruled in cases against Uber and Ola that the platforms violated the drivers' rights, as they were managed or even fired by algorithms. The courts ordered these companies to reinstate improperly terminated drivers and to explain their algorithms' logic (recognizing, for the first time, a "right to an explanation" under the GDPR).

Key takeaways from these cases are that AI systems must operate within existing law: fundamental rights (like privacy and non-discrimination) may not be breached by algorithms, and individuals affected by automated decisions have a right to transparency and human oversight. In short, any decisions that are made by AI must be accountable, explainable, and subject to human checks, just as any human decision-making process would be. The case law is, however, relatively scarce to date, but will probably increase as AI systems will be more generally used over time.

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

Since 2023, the Dutch Data Protection Authority (AP) has been the coordinating supervisory authority for algorithms and AI that pose risks to fundamental values and fundamental rights. To this end, the AP has set up a separate organizational unit, the Algorithm Coordination Department (DCA).

The supervisory authorities responsible for supervising and enforcing the AI Act have not yet been appointed. In the Netherlands, the government is currently working on a proposal for the supervision of the AI Act. It is expected that there will be several supervisory authorities for different parts of the AI Act. Which supervisory authority is responsible will depend on the context in which the AI system is used or developed. The division of tasks will be laid down in Dutch legislation.

The extent to which the AP will supervise the AI Act has therefore not yet been determined. As the coordinating algorithm supervisor, the AP is already contributing to the preparations together with other parties. In November 2024, the AP and the RDI issued a recommendation to the Ministries of Economic Affairs and the Interior and Kingdom Relations on how to properly organize the supervision of the AI Act. The AP is carrying out this work through its Algorithm Coordination Department (DCA).

19. How would you define the use of artificial intelligence by businesses in your jurisdiction? Is it widespread or limited? Which sectors have seen the most rapid adoption of AI technologies?

AI is increasingly being adopted by businesses in The Netherlands. Usage of (generative) AI based on LLMs is widespread in different sectors, e.g. for internal usage and chatbots. We see a rapid growth in (i) **healthcare** for diagnostics, patient data analysis and administration, (ii) **financial services** for fraud detections and risk analysis, (iii) **retail end e-commerce** for personalized marketing and customer service chatbots.

20. Is artificial intelligence being used in the legal sector, by lawyers and/or in-house counsels? If so, how? Are AI-driven legal tools widely adopted, and what are the main regulatory concerns surrounding them?

It is our understanding that AI is increasingly used by lawyers and in-house counsel in the Netherlands, primarily to streamline regular office tasks or other routine tasks. AI may also be used for tasks like contract review, legal research, document analysis, and drafting of documents. Some general AI-tools are used (such as ChatGPT, Anthropic Claude, Microsoft Copilot), but some companies also offer specific AI-legal tools aimed at

professional legal tasks. Some law firms even develop their own (GenAI) tools. The main concerns regarding the use of AI include safeguarding confidentiality of client data when using AI, ensuring accuracy and fairness (to avoid AI errors or bias), and complying with data protection laws and the EU's new AI Act requirements (which require transparency and human oversight for high-risk AI systems).As far as we know, there is some reluctance among lawyers to use AI (tools) in their work, mostly due to concerns related to the accuracy of AI. This may however change over time as AI tools become increasingly powerful.

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

While these challenges and opportunities may vary between lawyers, we think that these 5 key challenges and opportunities raised by AI are relevant to lawyers:

Challenges

- **Confidentiality of AI tools**: Using AI (especially cloud-based generative AI) raises confidentiality concerns. Lawyers must ensure AI platforms are secure, comply with privacy laws, and maintain professional secrecy.
- **Accuracy of AI systems**: At this moment, AI may produce errors or biased outputs (such as hallucinations). Human oversight is therefore still necessary which in turn can negate the potential efficiency gains. The limited accuracy of the output makes AI at this moment not too relevant for professional legal work.
- **Adoption gap**: Many lawyers as of today will probably lack any AI training or AI-relevant skills. Adopting AI in a legal context requires new skills but may also require a new way of working and a shift in mindset.
- **Costs of AI systems**: Integrating AI into existing workflows and products may be complex and expensive. AI needs high-quality data to be trained on, which is at the moment not (freely) available. In addition, commercial tools offered on the market are relatively expensive.
- **Replacement**: One of the most debated challenges for lawyers is whether a great part of the work will be replaced by AI.

Opportunities

- **Automation of routine tasks**: AI may be able to speed up routine tasks, such as standard contract review and legal research, which increases efficiency, boosts productivity and may reduce costs for clients.
- **Improved client service**: By automating routine tasks, lawyers may be able to dedicate more time to tasks which are relevant to the client. Clients may also benefit from faster responsiveness which enhances client satisfaction.
- **Better insights and data–driven decision making**: AI may be able to uncover patterns in legal data in large datasets, that would otherwise go unnoticed or be missed, and enables lawyers to make better informed decisions using data patterns.
- **Improved legal research**: AI-powered legal research tools can provide faster, relevant results.
- **New services and area of expertise**: AI is creating demand for new legal areas like AI compliance, algorithm audits, and tech contracts. AI will therefore maybe create a new legal 'niche'-area.

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

- **Supervision and enforcement**. As the Dutch government is currently preparing an AI Implementation Act to establish the national enforcement architecture and clarify responsibilities among supervisory authorities under the AI Act.
- **AI and processing of personal data**. We expect the Autoriteit Persoonsgegevens to issue guidelines in relation to the processing of personal data through AI systems, e.g., during the training and testing phase. These guidelines would apply in addition to the guidance already provided by the European Data Protection Board in this regard. For example, see (link) and (link).
- **Liability**. With the proposal for the AI Liability Directive being withdrawn in early 2025, we are expecting developments regarding liability for faulty AI systems, initially primarily in case law.

Contributors

Laura Poolman
Senior Associate
laura.poolman@kvdl.com

Astrid Sixma
Partner
astrid.sixma@kvdl.com