THE GLOBAL LEGAL POST

NETHERLANDS

Astrid Sixma

Kennedy Van der Laan

This chapter forms part of:

Artificial Intelligence

Law Over Borders Comparative Guide 2022

www.globallegalpost.com/lawoverborders

INTRODUCTION

The adoption of AI is widespread; from medical diagnosis, to fraud detections in bank transfers, to online profiling. The Netherlands aims to keep its position as a front runner in inventing technologies, and is currently a top-10 country for AI technology development, both within large established enterprises and as part of a thriving start-up scene.

In the legal field, there are discussions about the application of traditional legal doctrines on AI and at the same time there are calls for new or modified legal frameworks to deal with this relatively new and complex technology. Guidelines, reports and policies covering many legal fields have been introduced, and a proposal for an EU Artificial Intelligence Act was published last year. It is safe to say that the legal framework in the Netherlands is in full swing.

1. CONSTITUTIONAL LAW AND FUNDAMENTAL HUMAN RIGHTS

The adoption of AI is impacting society as such and introduces new challenges regarding fundamental human rights, such as the right of equal treatment, protection against bias and discrimination (covered below in Section 4: Bias and discrimination), the right to privacy, freedom of speech and the right to a fair trial.

These human rights are safeguarded in the Netherlands by domestic laws, in the first place the Dutch Constitution (Grondwet), and international treaties such as the European Convention on Human Rights (ECHR) and the Charter of Fundamental Rights of the European Union (Charter).

Fundamental rights apply primarily in a vertical relationship between the government and citizens, but may also have an effect in horizontal relationships between citizens and companies. Governments do not only merely have a negative obligation to refrain from unlawful interference with an individual’s human rights, but also have a positive obligation to safeguards these rights.

1.1 Domestic constitutional provisions

Considering the overriding principle of international treaties, the domestic constitutional provisions will be discussed below in Section 1.2 by topic.

1.2 Human rights decisions and conventions

Right to privacy

The right to privacy is protected by Article 10 of the Dutch Constitution, Article 8 ECHR and Article 7 of the Charter. It has a broad scope and encompasses the right to personal autonomy, respect for private and family life, home and correspondence. Interference is allowed, namely in the interests of national security, public safety or the protection of the rights and freedoms of others, provided it is in accordance with the law or prescribed by law and necessary in a democratic society for the protection of one of the aforementioned objectives.

Through the use of data, including big data, in algorithm-driven technologies, detailed profiles can be obtained on the private lives of individuals. The increased use of smart devices connected to the internet that collect and share data (Internet of

Things (IoT)), can lead to increased surveillance of citizens, by both governmental bodies (i.e., IoT applications in smart cities, security cameras) or by the private sector (i.e., use of a smart watch that transfers collected data to employer, video-monitoring of employees). The Court of Justice of the European Union (CJEU) has ruled in several instances that government surveillance can be considered an infringement of the right to privacy. The same applies to monitoring and surveillance, including monitoring of electronic communications through the use of AI, by employers (ECrtHR 5 September 2017, no. 61496/08, *Bărbulescu v. Romania).*

In the Netherlands, a law was passed allowing for digital welfare fraud detection (SyRI), including through the use of deep learning algorithms. The district court of The Hague ruled that considering the gravity of interference with the private life of citizens and the lack of foreseeability and transparency, SyRI infringed Article 8 ECHR (Court of The Hague 5 February 2020, ECLI:NL:RBDHA:2020:865).

Another element of the right to privacy that is at odds with the use of AI is the right to be forgotten (established in the case CJEU 14 May 2014, C-131/12, *Google v. Spain*, and later codified in the GDPR), considering the longevity of the use of personal data in AI-systems.

Freedom of expression

Freedom of expression, including access to information, is protected by Article 7 of the Dutch Constitution, Article 10 ECHR and Article 11 of the Charter. The freedom of expression can only be restricted by formal legislation, and there is a far-reaching prohibition of preventive restrictions/censorship.

The government has an obligation to ensure that people have access to diverse and impartial information. The use of AI in information gathering, for example through online search engines or social media platforms, may limit that. For example, algorithms used in a news and current affairs context tend to show information to users that the AI believes they would like to see, based on their search history and other available data, creating so-called "filter bubbles and rabbit holes". This limits ones access to diverse information. In 2019 research was conducted on behalf of the Dutch Media Authority (Commissariaat voor de Media) on the existence of filter bubbles in the Netherlands. It was concluded that the online news taken in by the Dutch was largely not recommended to them by any algorithm and that they had a very diverse range of news and information at their disposal, even within algorithmic filtering systems. The Media Authority continues to monitor the development of the information and news provision in the Netherlands in connection with AI (see *www.cvdm.nl/sites/default/files/publication-Filter-bubbles-in-the-Netherlands.pdf).*

AI can also be used by search engines and social media platforms to recognize and automatically ban unwanted, dangerous or suspicious content, which can be considered a form of censorship (although not directly covered by the ban on censorship by governments). Although legitimate goals may be achieved by this — i.e., protection against discrimination by filtering and banning hate speech — it may also censor legitimate expressions that may be controversial, but should not be deemed illegal (i.e., a shocking piece of art).

Right to a fair trial
The right to a fair trial is laid down in Articles 6 and 13 ECHR and Article 47 of the Charter. The right to a fair trial includes that proceedings should be fair and open, judges should be independent and impartial and rulings must be duly motivated. Those principles may be affected when AI is used by judges in the preparation of a judgment, when the functioning of the AI is not entirely transparent or known ('black box') and may encompass bias.

The use of AI for court judgments is also considered a high risk application under the proposed Artificial Intelligence Act (see Section 6. Domestic legislative developments).

2. INTELLECTUAL PROPERTY

Intellectual property rights are relevant to AI from different perspectives: AI technology itself can be protected by an intellectual property right, and the output of AI may in its turn be protected by intellectual property rights.

2.1 Patents

Patent applications for AI have increased significantly over the past decade, according to the European Patent Office and the WIPO, notably in the fields of image and voice recognition.

Patent law 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. 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 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.

The European Patent Office has refused patent applications indicating an AI-system as the inventor on the ground that the EPC requires the inventor to be a natural person (EPO Legal Board of Appeal in oral proceedings on 21 December 2021, cases J 8/20 and J 9/20).

2.2 Copyright

A work of literature, science or art is protected under Dutch Copyright Act (Auteurswet) if it is original in the sense that it is its 'author's own intellectual creation' (a principle harmonized by the CJEU in CJEU 16 July 2009, C-5/08, *Infopaq*). Elements of AI systems may or may not be eligible for copyright protection, as illustrated below:

- An algorithm or a trained machine or deep learning model itself is unlikely to be eligible for copyright protection, as it is not the result of 'free and creative choices', but is dictated by technical and functional considerations (similar to what was ruled regarding database protection in CJEU 1 March 2012, C-604/10, *Football Dataco v. Yahoo!*).

- Software that implements the algorithm or AI can be protected by copyright. Computer programs are explicitly covered by the Copyright Act, following the implementation of the EU Software Directive 2009/24/EC. However, the underlying ideas and principles of a computer program are explicitly not protected by copyright under that Directive, and the same applies to the functionality in itself of the software (CJEU 2 May 2012, C-406/10, *SAS Institute*).
- The structure of databases (i.e., training sets) may be eligible for protection under the copyright regime. Also considering the originality requirement, database protection under copyright law seems of limited relevance for AI.

On the other hand the question arises whether a work produced with the aid of AI (AI-assisted output) is protected under copyright law. It is broadly argued in the literature that the work in question must be the product of (at least some) human intellectual effort, and that output without any human intervention is excluded from copyright protection.

2.3 Trade secrets/confidentiality

The protection of trade secrets is governed by the Dutch Trade Secrets Protection Act (Wet bescherming bedrijfsgeheimen), implementing the EU Directive 2016/943/EU. Information is considered a trade secret if:

- it is not public in the sense that it is not generally known to the public or known by or easily accessible to persons who normally deal with that type of information;
- it has commercial value because it is secret; and
- is subject to reasonable measures to keep it secret.

Inference models can fit into this category.

Unlike a patent right, a trade secret does not grant an exclusive right. Further, reverse engineering of a lawfully acquired product is allowed, unless this has been contractually prohibited.

3. DATA

Data is relevant on many levels to AI: from the protection of training sets by a database right, to restrictions on the use of personal data, to having access to big data sets from the government.

3.1 Domestic data law treatment

A collection of data can be protected by a *sui generis* database right under the Dutch Database Act (Databankenwet). The content of a database can be protected if a substantial financial, material or human investment has been made in obtaining the verification or the presentation of the content. Creating training databases will generally require such a substantial investment, and subsequently such training datasets would be protected as a database. Investments made regarding the creation of data (i.e., data augmentation) itself can however not be taken into consideration.

The maker of the database can prevent the extraction and/or reuse of the whole or a substantial part of the database's content.

3.2 General data protection regulation

Relevant principles of the GDPR

The collection and processing of personal data is governed by the General Data Protection Regulation (GDPR) and the Dutch Implementation Act (Uitvoeringswet Algemene verordening gegevensbescherming).

There is a tension between the use of AI and several principles of the GDPR, including:

- Purpose limitation, data minimisation and storage limitation (Article 5 GDPR).
- Transparency and accountability (Article 5 GDPR); data subjects must be informed about the processing of their data and, when AI is used, meaningful information about the logic involved should be provided.
- Restrictions regarding profiling and automated decision making (Articles 21 and 22 GDPR); this is especially relevant in the context of AI and deserves a further elaboration.

Profiling means any form of automated processing of personal data in order to evaluate certain personal aspects relating to a natural person. This includes, for example, the creation of online profiles and use for direct marketing, or profiling in the context of a credit check in order to decide whether an applicant is granted a loan. The latter is considered automated decision making, provided there is no meaningful and substantive human involvement in the decision making process. Restrictions apply when an AI-system makes a decision that has legal effects or similarly significantly affects an individual. This is only allowed if:

- it is necessary for entering into or the performance of a contract between the parties involved;
- is authorised by law; or
- is based on the data subject's explicit consent.

In any event, meaningful human intervention must be provided upon request of a data subject, including to contest the decision. The use of special categories of data, including biometric data (Article 9 GDPR) in automated decision making is further restricted.

Dutch Data Protection Authority ruling

The Dutch Data Protection Authority (Autoriteit Persoonsgegevens) fined the Dutch Tax Authority (Belastingdienst) in 2021 for the use of a risk-classification model, which included a self-learning algorithm, in which the fact that a person had a non-Dutch nationality was incorporated as a risk indicator. This was considered discriminatory and unlawful (under Articles 5 and 6 GDPR). The Dutch government resigned over this scandal, known as the 'benefits affair'.

3.3 Open data & data sharing

Open data and open government

Traditionally regulations around open data and data sharing primarily address obligations of governmental bodies to do so:

- The Government Information Reuse Act (Wet hergebruik van overheidsinformatie), sets the rules under which citizens and companies can request governmental bodies to provide certain information they have for reuse. In principle, the information must be provided, unless exemptions or restrictions (i.e., GDPR compliance) apply. Data must be made available where possible in electronic form in a machine-readable and open format, together with the metadata.

- The Open Government Act (Wet open overheid) provides rules on actively making governmental information public and accessible and ensuring that it is easier to find, exchange, retrieve and archive. This act is however more focused on transparency of the government than on the (re-)use of data.

European data strategy

As part of the EU Digital Market Strategy and the European data strategy, new regulations and directives have been proposed that apply to both public authorities and private companies:

- The Data Governance Act was adopted in May 2022. This act aims to boost data sharing in the EU, providing companies and start-ups with more access to more data that they can use to develop new products and services, including in the field of AI, where access to big data is crucial.
- The Data Act was proposed by the Commission in February 2022 to further encourage data sharing. This act includes rules regarding data access rights and the use of data generated by IoT devices.
- The EU Directive on Copyright in the Digital Single Market (Directive 2019/790, implemented by the Dutch Implementation Act Directive on copyright in the digital single market) includes provisions regarding text and data mining.

3.4 Biometric data: voice data and facial recognition data

Biometric data that allow the unique identification of a natural person are considered a special category of personal data. Processing such data is prohibited under Article 9 of the GDPR, unless specific exemptions apply or the data subject has given its explicit approval. Article 29 of the Dutch Implementation Act includes an additional exception: it is not prohibited when this is necessary for authentication and security purposes. It is understood that the necessity must also be seen to be necessary in view of a compelling interest; being an interest beyond a regular business interest.

The Dutch Data Protection Authority (Autoriteit Persoonsgegevens) gave a formal warning in 2020 to a supermarket regarding the use of facial recognition, considering that the data subjects did not give their explicit consent, nor was it necessary for security purposes, because there was no compelling interest.

4. BIAS AND DISCRIMINATION

The risk of bias and discrimination through the adoption of AI is a heavily debated topic.

4.1 Domestic anti-discrimination and equality legislation treatment

The protection against discrimination and the right to an equal treatment is laid down in Article 1 of the Dutch Constitution, Article 14 ECHR and Articles

21 and 23 of the Charter. These provisions and principles prescribe that all are equal before the law and that everyone is entitled to equal treatment. There cannot be an unequal treatment without an objective and reasonable justification.

There is national special equal treatment legislation in which several EU Directives (2000/43/EC, 2000/78/EC, 2006/54/EC and 2004/113/EC) are implemented, including the General Equal Treatment Act (Algemene wet gelijke behandeling), as well as specific acts regarding discrimination based on the grounds of age, disability or chronic illness, sex, and fixed or indefinite period of employment. These equal treatment rules apply when there is differentiation at an individual level. Discrimination can also be indirect (as confirmed by the CJEU), when an apparently neutral criterion or practice factually disadvantages a much larger number of persons with the protected characteristic, than persons without that characteristic.

The emergence of AI-driven technologies has led to a significant increase in the possibilities to differentiate between (groups of) people, by both governmental bodies and private actors, as demonstrated by the aforementioned 'benefits affair'. Such differentiation may lead to unjustified discrimination and poses a challenge to safeguarding the protection against discrimination. Considering that algorithms, and especially machine and deep learning algorithms, can be highly complex and not transparent, it may be difficult to determine whether the algorithm and/or the output is discriminatory, or if differentiation is justified. Further, datasets used in an algorithm can be biased, which bias can be self-reinforcing when used by a deep learning algorithm. Organisations should ensure that the data used is factually correct, complete and representative and they should regularly test their AI-systems to avoid discrimination and bias.

5. TRADE, ANTI-TRUST AND COMPETITION

When it comes to AI and anti-trust the discussions are primarily focused on dynamic algorithmic pricing and price discrimination. Questions are raised on how to apply the existing legal doctrine on these issues and whether the current legal framework is fit for this.

5.1 AI related anti-competitive behaviour

Algorithmic pricing

Dynamic algorithmic pricing is an automated way of setting prices based on variables such as supply and demand, availability of alternatives and prices of competitors. This could lead to automatically coordinated price setting and commercially sensible parallel conduct of competitors that can be considered tacit collusion (under Article 6 Competition Act, Article 101 TFEU). In order to qualify as concerted practices, indirect 'contact' must be established between competitors (i.e., when AI-systems communicate/interact), which may not be straight forward when dealing with AI-systems.

When AI is used to implement or monitor pricing agreements between competitors, this naturally is considered anti-competitive behaviour.

FREQUENTLY ASKED QUESTIONS (FAQS)

1. Can we use all the data obtained from customers through the use of a Software as a Service (SaaS) solution to train our AI-system?
To use customer data for this purpose you generally need permission and a usage right to such data should be included in your agreements. As to the further processing of personal data the GDPR applies.

2. We use AI in our software; how can we prepare for the EU Artificial Intelligence Act?
The proposal is expected to undergo numerous changes. Taking into account general principles of fairness, accountability and transparency when employing AI in your software, will make you prepared once the Act will be nearer to finalization and adoption.

Price discrimination
AI can also facilitate price discrimination or individualised pricing based on behavioural profiling. Big Tech companies have access to extensive data sets on their customers, allowing them to play on their weaknesses, vulnerabilities and biases, and consequently enabling them to charge each customer their highest acceptable price, all through the use of algorithms. This can be considered abuse of a dominant market position.

European Commission Decision on Google
The European Commission found that Google abused its market dominance as a search engine by promoting its own comparison shopping service (Google Shopping) in its search results, and demoting those of competitors. This was accomplished by the algorithms Google used (Commission Decision 17 June 2017, Case AT.39740, and CJEU 10 November 2021, Case T612/17, upholding the EUR 2.42 billion fine).

5.2 Domestic regulation
Competition is regulated by the Dutch Competition Act (Mededingingswet) and the Treaty on the Functioning of the European Union (TFEU), which include prohibitions regarding:

- agreements (e.g., cartels) or concerted practices which may affect trade and have as their object or effect the prevention, restriction or distortion of competition (Article 6 Competition Act, Article 101 TFEU); and
- abuse of a dominant market position (Article 24 Competition Act, Article 102 TFEU).

The relevant Dutch competition authority (Autoriteit Consument & Markt) has published a position paper concerning the supervision of algorithmic applications, including guidelines for investigations into violations involving AI.

6. DOMESTIC LEGISLATIVE DEVELOPMENTS

Although guidelines have been issued at a domestic level (including 'Guidelines for the application of algorithms by governments and public information about data analyses'), most initiatives have been at a European level as part of the EU's Digital Strategy. This includes the White Paper on AI and the Report on Liability for AI, and foremost the 2021 proposal for the Artificial Intelligence Act. See the European Union chapter for further details.

Some key elements of the proposal for the Artificial Intelligence Act are:

- Scope of application: providers that put an AI-system into service in the EU, users of a system located in the EU, providers and users outside the EU when the output of the system is used in the EU. Hence, there will be a significant extraterritorial scope.
- Risk based approach; the degree of regulation depends on the risk level of the AI-system, as follows:
    - Unacceptable risk: when the application is considered an infringement of human rights (i.e., social scoring by governments), this is banned.
    - High risk: certain applications may harm health, security or fundamental rights, (i.e., CV selection tools), and strict requirements will apply regarding data and data governance, documentation and record keeping, transparency and provision of information to users, human oversight, robustness, accuracy and security.
    - Limited or minimal risk: when there is a risk of manipulation (i.e., when using chatbots), there are information obligations (such as, for example, that the user must be made aware that they are interacting with an AI-system). When there is a minimal risk, for example, when AI is used to predict your musical preferences, no restrictions apply. However, applying the restrictions for high risk AI voluntarily and implementing a code of conduct is encouraged.

AUTHOR BIOGRAPHY

Astrid Sixma

Astrid Sixma specializes in IT law, with a focus on technology projects and FinTech issues. She advises both suppliers and customers in IT projects and in drafting and negotiating various technology contracts. She also litigates in disputes concerning IT contracts, licences, failed IT implementations, and IP infringements of software. Astrid graduated from Groningen University in 2008 (cum laude) and during her master studies she also studied at McGill University, Montreal. Before she joined Kennedy Van der Laan in 2019, she worked at two big Dutch law firms and an Amsterdam niche firm.