Managing artificial intelligence: how companies can keep up
July 15, 2020

In their recent master class, our experts Axel Arnbak, Oscar Lamme and Ties Boonzajer Flaes looked at the various aspects of dealing with the ever-changing AI landscape, including EU and Dutch regulatory developments in this area.

Regulatory focus is split between adjusting existing regulatory frameworks and developing new ones on the one hand and ensuring that AI systems conform with current legal requirements on the other. Taking both a data protection and an intellectual property (IP) rights perspective, our experts underscored the importance of following a multidisciplinary approach to the development and governance of AI systems. This article highlights the key trends in EU and Dutch regulatory policy and enforcement strategies, civil litigation exposure when using AI systems and the most suitable IP rights strategies to help businesses protect AI systems.

Hot-button topic
Artificial intelligence (AI) has become a hot-button topic for governments, businesses and regulators alike. Governments compete for dominance in mastering this technology and grapple with the geopolitical challenges it brings. For their part, businesses increasingly employ AI to gain a competitive edge, increase efficiency and improve safety and compliance, while using exclusive rights to protect proprietary use of the technology. With these changes, regulators face the daunting task of shaping a legal framework that protects individual rights against the risks of AI while also stimulating AI development.

Regulatory horizon on AI: European perspective
The new European Commission’s digital strategy until 2024 has, as its top priorities, enhancing global leadership and creating a legal framework to ensure that AI is grounded in European values and fundamental rights. In February and March 2020, the Commission published several policy documents outlining the EU’s vision on the regulatory framework on AI, data governance and retaining and strengthening its technological and digital sovereignty. These include a White paper on AI, a European strategy for data, and A new industrial strategy for Europe. While the white paper recognises the General Data Protection Regulation (GDPR) as an important piece of legislation in regulating certain aspects of AI, it suggests that new AI-related legislation will probably be needed. The Commission recommends that AI regulation be founded on a risk-based approach. It envisions introducing mandatory requirements for data sets used to train AI systems – and for the development, fine-tuning and application of such systems – only when those AI systems are “high risk.” Although it remains unknown which sectors will be considered high risk in the future regulatory framework, the Commission has indicated that healthcare, automotive and logistics, finance, energy and parts of the public sector are the most likely candidates. The Commission has also formulated policy proposals on adjusting the scope of European product safety legislation and product liability rules.

The European Data Protection Board (EDPB), which comprises the national data protection authorities (DPAs), and the European Data Protection Supervisor (EDPS), which oversees data protection compliance by EU institutions, are currently actively involved in policy discussions about the regulatory framework on AI. While skeptical about needing a new regulatory framework, the EDPB is framing issues arising in the context of development and use of AI as data protection problems. This ties into the European tradition of using data protection legislation in response to legal challenges created by technological development. Regulating AI solely through a data protection framework is, however, problematic for several reasons. The most relevant of these being that such a framework would not account for all aspects of discrimination that could result from applying AI and, with an individual rights framework purportedly being at its core, would only indirectly address the negative impact of AI on communities and society at large.

While there is disagreement on how to regulate AI, all European stakeholders agree that AI should be ethical. In order to comply with the general principles of the GDPR, companies should identify, observe and substantiate ethical choices made in the course of the development of an AI system.

The Dutch perspective
Similarly, AI features prominently in Dutch policy, as demonstrated by AI being one of the Dutch DPA’s three priority enforcement areas for 2020-2023 (see our previous article). This year alone, the DPA has already published two guidance documents on using AI in the automotive and supermarket sectors: the March 2020 guidance on connected cars and the June 2020 letter on the use of facial recognition in supermarkets.

It’s clear that the DPA is transitioning from explaining when GDPR rules apply, to actually carrying out AI enforcement actions. For now, we are aware of several AI-focused enforcement actions, but given the vast political attention AI is receiving, enforcement actions in other sectors may quickly follow.

Finally, AI is being increasingly used by the Dutch police, as well as by supervisory and enforcement agencies, such as the Dutch Tax Authorities. In this context, members of the Dutch parliament are currently calling for the creation of general AI guidelines for government bodies and for the establishment of an independent supervisor.

Practical steps for complying with current rules on AI
While regulators grapple with setting up a future-proof legal framework for AI, many companies are already implementing (or thinking about implementing) AI solutions in their business. To ensure that these AI systems are in line with current legislation, including the GDPR, anti-discrimination laws and other sectoral requirements, companies should think beyond tick-box compliance. For many DPAs throughout the EU, the
approach is no longer enough to demonstrate compliance with the GDPR framework for AI as a whole. In particular, the Information Commissioner’s Office (ICO) in the UK has developed extensive and high-quality guidance on how to approach AI governance and compliance with the GDPR (see ICO’s page on AI Auditing Framework and Explaining decisions made with AI). Therefore, to minimise enforcement risks companies should approach AI development from broader corporate governance and project management perspectives. Here are some of our recommendations on how to deal with GDPR compliance in this process.

**Key recommendations**

- Before starting a project, it is important to get a multidisciplinary team on board that consists of all relevant stakeholders, including the AI development team; the Data Protection Officer; and representatives from senior management, the legal department, the compliance team and teams responsible for securing IP rights within the company.
- Before starting a project, project leaders should be clear about the purposes of the project; whether the use of personal data is necessary and to what extent aggregated or anonymised data can suffice. It is possible that some of these roles (controller, joint controller or processor); distribution of responsibility with external parties involved in the project; IP rights aspects of protecting the AI system and its output as well as the data used in training the AI system. These are just a few items that need to be delved into.
- These aspects should be a part of the Data Protection Impact Assessment, which is compulsory for all AI development projects involving personal data.
- It is essential to be as transparent as possible to users about the purposes and how the AI system functions, and to be clear about inherent biases in the system and possible unintended consequences. Individuals should be made aware of these issues and of their rights, and any explanation to individuals must be made in a manner understandable to a lay person.
- Any ethical choices made in the course of developing the AI system should be explained and documented.

**Most suitable strategy of protecting AI algorithms and their output**

To fully benefit from the development of AI systems, and early in the algorithm development process, companies should have a clear strategy of how to protect AI algorithms and their output. The most suitable strategy for protecting AI algorithms most likely includes a mixture of patents, trade secrets and defensive disclosures. Copyright protection is of limited relevance, as it covers only the actual source code in which algorithms are expressed and does not cover the functionality of the algorithms.

At first glance, patent protection seems unavailable for AI algorithms as they constitute mathematical methods implemented in a computer program, which are explicitly excluded from patent protection by article 52(2) of the European Patent Convention. In practice, these exceptions are interpreted restrictively; obtaining a patent on an AI algorithm as well as on its output is possible if it is claimed as a part of a technical system in which it operates, and not as an abstract entity. Exponential growth of the number of AI patents is the best way to demonstrate this.

**Patents**

When considering applying for a patent, companies should be mindful of at least the following:

- Drafting patent claims in such a manner that legal hurdles for patent protection of AI algorithms imposed by the European Patent Convention are overcome and that the patent protection covers not only the AI system but also its output;
- Carefully studying and selecting the jurisdiction(s) offering the best protection. This requires careful analysis, as AI systems often operate out of several locations. For example, an AI algorithm can be deployed by a company in France, run on servers located in the Netherlands and apply to customers throughout the EU. Choose countries where you can obtain a patent strategically, taking into account the relevance of the AI system to competitors. Due to its position as a cloud data-centre hub, the Netherlands could be one of the jurisdictions where obtaining a patent may be sensible.

**Trade secrets**

Invoking trade secrets is another way to protect AI algorithms, as they can grant broad protection to anything that is kept a secret, from customer lists to methods used in chemical processes. To qualify as a trade secret, in addition to being secret (that is, not generally known/readily accessible), the information should have commercial value and be subject to reasonable steps to keep it secret. Unlike patents, trade secrets also cover AI algorithms that are not implemented in a technical system. The European Trade Secrets Directive grants protection against infringing goods: anything that was created and significantly benefited from a misappropriation of a trade secret. Remedies for trade secret infringement include injunctions and seizures.

Trade secret protection has at least four downsides as compared to patents:

- Injunctions are harder to obtain for a trade secret infringement than for a patent infringement.
- Trade secret protection does not grant exclusive rights, but only protects the trade secret from being misappropriated. This means that it cannot be invoked against the use of AI algorithm developed without the knowledge about the trade secret.
- The legal framework on trade secrets is often unclear and jurisdiction-specific.
- Reliance on trade secrets can put a company in a difficult position if a third party obtains a patent on the same AI algorithm and/or its output. The right of prior use, which could to some extent allow the company to continue using the algorithm, is often interpreted restrictively, is subject to territorial limitations and can be difficult to prove in practice.

One could also argue that the GDPR transparency requirements
in relation to the AI algorithm towards individuals could interfere with trade secret protection. If you include trade secret protection in your IP strategy, it is important to maintain an open line of communication between the relevant IP and data protection teams. From a legal perspective, the purpose of the GDPR transparency requirement is to inform individuals about the impact that using AI has on their rights and interests. It does not require the disclosure of commercially sensitive information, such as source codes or the technicalities of how the algorithm functions. It is possible to comply with the GDPR while preserving trade secret protection, if privacy statements and other communications to individuals are carefully crafted.

**Defensive disclosure**

If obtaining a patent is considered too costly or unreasonable, but there is a risk that a third party may develop the same algorithm, companies may consider making a defensive disclosure of a part of the algorithm to prevent third parties from obtaining a patent in the future. Make sure you keep proof of the disclosure.

**Protecting value created by data use**

Apart from protecting the AI algorithm itself, companies should also protect the value created by using their data to train those algorithms. In particular, if a third party vendor supplies an algorithm that is trained with your company’s data, make sure that your contract with the third party regulates whether – and on which conditions – this algorithm can be used by competitors.

**Minimising enforcement risks and private litigation exposure**

When developing an AI system and designing its legal protection and governance structure, companies should think about public enforcement by governmental authorities, such as DPAs, as well as private enforcement of data protection and IP rights. Carefully considering where the AI system is to be implemented – taking into consideration enforcement risks and IP protection in various jurisdictions – is crucial to managing exposure.

From a data protection perspective, when multiple companies are involved in the application and functioning of an AI system, such as in a joint venture, it is crucial to clearly define the roles of controllers and processors early on to avoid a situation where multiple parties are considered joint controllers. Recently, DPAs across Europe have been inclined to establish joint controllership in order to claim jurisdiction over data privacy violations.

In addition, GDPR-based damage claims litigation, especially in the form of mass claims, has become an even greater risk to companies that process personal data using AI systems, than enforcement by authorities. Using consumer data makes companies vulnerable to mass claims. Increasing involvement of professional claims funders in mass claims in Europe adds a profit-seeking component to those claims. The Netherlands is an attractive jurisdiction for bringing mass claims. The new law on mass claims – in effect since 1 January 2020 – broadens the mass claims regime by allowing courts to award damages in class action cases, where previously they could only rule on liability. Furthermore, the Netherlands Commercial Court allows litigation of complex international civil or commercial matters in English (see our previous article). We expect that the current rising trend in mass claims litigation will continue in the Netherlands for the foreseeable future.

Conversely, from an IP rights perspective, the Netherlands is a convenient jurisdiction to obtain patent protection. Because many companies use servers located in the Netherlands, the likelihood of patent infringement litigation in the Netherlands is high.