BCLP. Client Intelligent

Insights

MANAGING LITIGATION RISKS OF ARTIFICIAL INTELLIGENCE

Dec 02, 2024

SUMMARY

Artificial Intelligence ("AI") use in business has proliferated in recent years; risks arising from this therefore must be managed. Whilst the use of AI can drive significant efficiency gains for most businesses, the characteristics of machine learning mean that there is the potential for data protection and discrimination claims to arise (amongst others). We explore some of the potential litigation risks in the UK arising and how these risks can be managed.

Whilst algorithms have been used to replace human processes for decades, AI integrates machine learning, which is intended to mimic human learning and enable systems to perform tasks commonly thought to require human intelligence. This can bring significant efficiency gains for companies; from analysing data and streamlining processes, to making decisions. However, the ability of AI to "learn" increases the litigation risk for businesses when systems go wrong. We focus on three of the key considerations that businesses must manage when using AI systems, which are:

- Data Protection
- Input Data; and
- Liability Issues.

DATA PROTECTION

For most AI systems, a critical issue will be personal data input into the data set used to train the AI or which is later utilised in the AI tool. Within a business context, this application of AI models may be integrated into decision making processes, such as:

- An AI system designed to asses and filter CVs in a job application process. Personal data, such as age, gender, ethnicity, qualifications and address are amongst the data likely to have been fed into the model for assessing whether candidates would be suitable for a particular role.

The model will be trained by reference to the historical performance of candidates meeting certain data points. It will then produce an output using these factors to assess who may in future perform the roles most effectively. With recent figures suggesting a 300% increase in the use of AI tools in HR between 2023 and 2024, the data used to train the AI tools are of critical importance.

- A similar assessment of characteristics might be used in credit applications. Credit risk and borrowing suitability of previous applicants could be used to model the suitability of future borrowers.

For AI systems which analyse personal data in this way, a key source of litigation risk is in the form of UK GDPR and the Data Protection Act 2018. UK GDPR contains restrictions in Article 22(1) on the automation of business processes and contains stringent restrictions on the use of personal data, including how this data must be handled. This creates the risk of infringing multiple principles in Articles 5(1) and 5(2) of UK GDPR, including the fairness principle and accountability principle when using AI systems.

- The fairness principle means personal data should only be used in ways people would reasonably expect and should not be used in ways that might have unjustified or adverse effects on them.

- The autonomous and adaptive nature of AI systems could lead to infringements of the accountability principle. Where systems are able to train themselves to generate recommendations or decisions, the developers themselves may not fully understand how the system has reached a particular conclusion, creating a gap in accountability when the company cannot explain why a particular decision has been taken, and exposing the company to a potential litigation risk.

INPUT DATA

Use of input data such as age, gender, ethnicity, qualifications and address can create further risks around how algorithms have been trained. An AI system which is trained on discriminatory data could embed further discrimination in its outputs, leading to risk arising under both the Equality Act 2010 and the European Convention on Human Rights.

Based on its input data, an AI system – particularly where it is used in decision making, such as filtering CVs for a job application or assessing credit risk of bank borrowers – might appear to discriminate against applicants on the basis of protected characteristics, for example gender, age or ethnicity. Some such claims have already begun to come through to the Employment Tribunal. A recent indirect discrimination claim based on the use of facial recognition software argued that the software was less accurate in relation to non-white employees.

LIABILITY ISSUES

The case of *Tyndaris SAM v MMWWVWM Limited (VWM)*, involved assertions of liability around reliance on an AI system. Tyndaris sued VVM for unpaid fees but VVM counterclaimed for the fall in the value of their investment due to the performance of the algorithm. VVM had invested, at its peak, US$2.5bn with Tyndaris. The investment was managed by an algorithm which applied machine learning to predict market sentiment. However, the system was said to have failed to work as intended and VVM alleged that this caused it losses of around US$20m.

A number of issues arise from this case, the most significant being who is liable for a system failing to perform as intended. Whilst *Tyndaris* settled, there are substantial issues of law regarding whether the risk lies with the user, or whether the developer is liable. Under the EU's AI Act, the provider and deployer of an AI tool in the EU may be liable for failure to comply with certain regulatory obligations to perform conformity assessments and meet certain transparency thresholds.

The risk is that AI systems can be fallible and, when this results in losses, there may well be difficulty in apportioning and establishing liability.

MANAGING THE RISK

Governments are attempting to make strides in the regulation of AI. The EU's AI Act, the recent Convention on AI signed by the Council of Europe on 5 September 2024, and the 2023 Bletchley Declaration on AI Safety being examples. The UK's new government is now also considering legislating to place requirements on parties working to develop the "most powerful artificial intelligence models", but as yet no government Bill has been tabled. There is also a separate private members' bill currently at second reading stage in the House of Lords, to regulate the use of automated and algorithmic tools in decision-making processes in the public sector.

In contracting for any services involving AI, it is important to understand the potential data protection and discrimination risks. Companies must consider (amongst others) the following:

- Compliance with regulatory requirements (such as the need to conduct data protection impact assessments, maintain AI inventories and embed AI governance policies)
- What data (personal data or otherwise) has been used to train the AI system and its source;
- How the AI system has been trained, and what instructions it has been given;
- How the AI system will be integrated into the business;
- How personal data is assessed by AI and what weighting is given to characteristics;

- How the requirement for human oversight and the necessary redress mechanisms will be implemented;
- Whether any third party claims have ever been made against the system; and
- How liability for any failures of the AI system is to be apportioned.

In managing liability, companies should be cognisant of contractual clauses which may intend to confer or limit liability. The current absence of ”market” clauses on apportioning liability means that companies should regard the negotiation of such clauses as key whenever an AI system is involved.

Whilst a comprehensive analysis of all the risks arising from the use of AI systems is beyond the scope of this insight it is intended to highlight some of the key litigation risks that may well arise from the use of AI. Our message for businesses is that delay may well be expensive and it is never too soon to ensure that you are aware of the potential risks and take steps to put in place adequate systems and processes to address your potential future risks in this fast-evolving area.

This blog was written with BCLP trainee, Calum Paton.

RELATED PRACTICE AREAS

- Litigation & Dispute Resolution

MEET THE TEAM

Georgia Henderson-Cleland

London

georgia.henderson-cleland@bclplaw.com
+44 (0) 20 3400 3714