

Common AI related technology project disputes and how to prevent them

The increased use of artificial intelligence (AI) is revolutionising the way businesses operate and is having a disruptive impact in sectors that have traditionally been slow to modernise.

05 October 2022

Introduction

The increased use of artificial intelligence (AI) is revolutionising the way businesses operate and is having a disruptive impact in sectors that have traditionally been slow to modernise. In the legal sector for example, AI is being used to streamline tasks such as legal research and bundling, and in some jurisdictions is being used to assist judges in reaching decisions. The benefits of investing in AI for businesses are clear. AI can increase productivity and add new proficiencies, scalability and can be tailored to create industry specific value. Notwithstanding these benefits, the use of AI in technology projects can lead to complex and at times unexpected disputes. Technology projects are typically bespoke agreements that evolve as the project progresses. As a result, when projects run into difficulties it can be challenging to ascertain what has gone wrong and to pinpoint the role AI may have played in causing the issue(s) giving rise to the dispute. This article sets out some common AI-related issues in technology project disputes and offers guidance on how to prevent them.

The added complexity of AI hardware

Machine learning (a type of AI whereby algorithms and statistical models are used to analyse and draw inferences from patterns in data) is being utilised in a greater variety of technology projects. These systems use neural networks and require significant technical resources to run, train and generate decisions, predictions and spot analogies. Legacy systems and standard graphics processing units are unlikely to be able to keep pace with the growing demand for AI tools and services – increasing the need for customers and suppliers, who want to use AI, to invest in specially designed AI hardware, such as Graphcore's recently released "Bow" AI Chip, which has the capacity to speed performance by 40% for machine learning tasks. The need for specialist hardware can increase the costs associated with the utilisation of AI and can also increase the likelihood that a dispute will arise due to there being more opportunities for something to go wrong at the manufacturing, shipping and installation stages. This can very easily result in delays to the achievement of key project milestones, which could in turn trigger remedies such as delay payments, and in the most extreme cases, termination of the contract.

Technology projects will often involve multiple stakeholders. A consequence of the additional steps required to implement AI solutions is that it can be difficult to identify who is responsible for failures and delays, whether it be the supplier, customer, a third party or a combination. Where the parties' roles and responsibilities are not well defined from the outset, a whole range of disputes can be triggered. These will typically be breach of contract disputes relating to the agreement in place between the supplier and the customer, and the various contracts which may be in place with third parties who are contracted to manufacture, ship and install specially designed AI hardware.

Determining liability

Whilst the mapping process used by AI systems is automated, the design, the initial training data and the further data that is passed through the system to train the model, is controlled by human operators. As a result, humans have visibility over the data that the AI tool starts with (the input), as well as the results that the tool produces (the output). What happens in between is often referred to as the "black box problem" which denotes the fact that after the input data has been added, it can be very difficult to change the underlying AI system and there will often be no transparency or explanation as to how or why the model produced a specific output.

This lack of transparency can create complex liability issues, especially as the main AI tools and services that are being deployed in technology projects at present are autonomous enough to function without much human intervention. It is therefore far more difficult to determine who bears responsibility when loss occurs as a direct result of an AI system failing; the failure potentially resulting from a technical malfunction or because of human error in the way in which the model was designed and/or trained.

Human involvement in the creation of the AI tool or service means that there is a strong possibility that human bias will be reflected in the input data, the training data, and in the outputs that the AI system produces. Algorithm bias can arise in a number of different settings and can result in various forms of discrimination. In a financial services setting, bias in AI systems could lead to errors in asset valuations which could in turn lead to missed investment opportunities. There have also been several high-profile examples of discrimination arising from the use of facial recognition technology in which characteristics such as gender and ethnicity, as well as the use of social scoring systems are inherent in the use and perceived accuracy of the technology.

Managing risk in contracts for AI solutions

It is crucial that customers and suppliers are clear about the primary objectives of the project, and the ways in which AI will be used to achieve these objectives. Contracting parties should ensure that there is a comprehensive agreement in place to govern the project and to provide certainty in the event that something goes wrong, in particular in relation to any limitations of liability. At a minimum the agreement should include detailed provisions covering confidentiality, liability, data protection, and IP. In the absence of dedicated AI legislation these areas are, at present, free to be negotiated. It should be noted however that contractual standards are being created - IP clauses for instance will invariably provide that the supplier owns the IP in the AI, whilst the customer has a licence to use it.

Issues related to specially designed AI hardware can be mitigated against by ensuring that all parties are clear about their respective roles and who bears the risk. The agreement should also set out the governance structure that will underpin the project and make clear how third-party relationships and dependencies will be managed and by whom.

The use of AI means that typical liability frameworks may not be suitable. Parties contracting to use an AI tool or service in a technology project should ensure that from the outset, the agreement includes AI specific warranties, indemnities and limitation provisions. These terms should be tailored to the specific context in which the AI tool or service will be deployed. The more general the term, the harder it will be to determine whether a particular standard has been met and establish liability. Common service standards, such as reasonable skill and care, are unlikely to be sufficient where AI is involved due to the output being too dissociated from the initial human input (the black box problem referred to earlier). Contracting parties will therefore need to draft inventive warranties stipulating, for example, that the AI tool should behave in the same way as a suitably capable and experienced human who is exercising reasonable skill and care in providing the service. Likewise, a buyer of an AI solution may wish to include warranties that the dataset used to train the AI is not discriminatory, does not breach data protection principles, or that the AI will not infringe third party IP rights. Limitation of liability and indemnity provisions should be given close scrutiny at the stage of contract negotiation, to ensure that one party does not bear disproportionate liability in the event of a catastrophic failure of the AI giving rise to significant third-party claims. These issues are highly specific to the use to which the AI will be put, and so contracting parties should engage with their stakeholders, consultants, lawyers and other experts to help them navigate this complex area.

Contracting parties also need to be aware of the risks associated with algorithm bias and should look to establish internal guidelines, processes and controls that minimise and address the discrimination and data privacy risks that may result from biased AI systems. An effective internal governance framework can assist in identifying any unjustifiable biases from initial data sets and may also flag any discriminatory outputs.

The changing regulatory landscape

Whilst there is general agreement that AI regulation is required, there is not, as of yet, a broad consensus on how this should be achieved.

On 21 April 2021, [the European Commission published the Draft AI Regulation](#). Instead of opting for a blanket regulation covering all AI systems, the EU chose to adopt a risk-based approach which differentiates between unacceptable risk, high risk, and low risk uses of AI. The level of regulatory intervention varies depending on which category of risk the AI tool or service falls into. Both customers and suppliers should familiarise themselves with the Draft Regulation and determine whether they are using, or intend to use, AI which carries an unacceptable risk (therefore prohibiting use of the AI tool or service), or whether they are likely to be impacted by the requirements for the provision of high-risk AI systems. Failing to account for the Draft Regulation could result in penalties for noncompliance, which are up to 6% of global annual turnover or EUR 30 million, whichever is greater.

The territorial scope of the Draft Regulation centres on whether the impact of the AI system occurs within the EU – not on the location of the AI provider or user.

On 18 July 2022, the UK Government published a policy paper titled 'Establishing a pro-innovation approach to regulating AI'. This paper builds on the UK's National AI Strategy and sets out the Government's proposals on the future regulation of AI in the UK. The UK approach to AI regulation seeks to demonstrate the Government's pro-innovation regulatory position post-Brexit, as it aims to be proportionate, light-touch and forward-looking, with the hope that this will drive the development of innovation and investment. Whilst the EU's Draft AI Regulation categorises AI use on risk level, the UK is not seeking to group specific uses of AI, instead choosing to rely on six "core principles" that will require AI developers and users to:

- ensure that AI is used safely;
- ensure that AI is technically secure and functions as designed;
- make sure that AI is appropriately transparent and explainable;
- consider fairness;
- identify a legal person to be responsible for AI; and
- clarify routes to seek redress or for contestability.

Moreover, in contrast to the centralised approach adopted by the EU, the UK's proposal will allow different regulators, such as Ofcom, the Competition Markets Authority (CMA) and the Information Commissioner's Office (ICO), to interpret and implement the six core principles, and adopt a tailored approach to the growing use of AI in a range of sectors.

Developers and suppliers of AI systems should also be aware of the Digital Regulation Co-operation Forum's (DRCF) recently published paper on algorithmic processing (which includes AI applications, such as those powered by machine learning). The paper notes that whilst algorithmic processing has the potential to deliver significant benefits, it also poses several risks if not managed responsibly. To manage these potential harms, the DRCF suggests that a more hands-on cooperative intervention strategy could be achieved through the increased use of regulatory sandboxes, such as the [Financial Conduct Authority's \(FCA\) Digital Sandbox](#). Where this strategy proves ineffective, the paper suggests that regulators can resort to use of their powers to take enforcement action against those who have not complied with the regulations and caused harm.

Parties contracting to use an AI tool or service in a technology project, should therefore endeavour to keep abreast of the latest AI regulatory developments to ensure that they understand their roles and responsibilities, and are aware of the level of regulatory intervention that they might face.

Conclusion

Customers and suppliers who recognise and mitigate against the potential risks of AI use in a technology project, by taking the steps outlined above, are likely to be the ones who reap the many benefits that AI offers. Those who fail to take early action to protect themselves contractually against AI risks could easily find themselves in a technology dispute over issues similar to the ones that we have identified in this article, as well as more project specific disputes.

Likewise, it is essential that parties consider the various proposals for AI regulation outlined above at the early stages of the project, to determine the applicable regulatory framework and to assess whether contractual changes are needed to account for developing regulation of AI.

If you need advice in relation to the issues discussed in this article, please contact Sophie Ashcroft.

Contact

Mark Hickson

Head of Business Development

onlineteaminbox@brownejacobson.com

Related expertise

Dispute resolution and litigation

Technology disputes