


How to mitigate risk in disputes arising from AI use in technology projects

 17 November 2023

Businesses are increasingly adopting AI tools to carry out functions traditionally performed by humans and/or non-AI tech. IT suppliers are no different and are offering AI solutions that increase productivity and add new proficiencies.

Notwithstanding these benefits, the use of AI 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.

AI disputes in technology projects

Technology projects invariably involve participation from multiple stakeholders (the relevant Authority and the different teams within the IT supplier, contractors, subcontractors, etc.). Within the context of the overall project, there will be different contractual arrangements in place that govern the various relationships, for example the Authority will have a contract in place with the IT supplier who in turn will have contracts in place with sub-contractors. The use of AI adds another layer to this contractual matrix and introduces an additional party to the chain – namely the AI developer.

The question of who is liable when technology projects go wrong is ultimately a factual one, but the introduction of AI makes answering this question far harder due to the inherent complexity of AI tools. The difficulties in assessing who is responsible for the failure of a project that uses AI means that a whole range of time-consuming and expensive disputes can be triggered. For instance, did the project ultimately fail because of the data used by the AI developer to train the AI tool or was it because the training methodology used by the AI developer was flawed or inadequate or was the failure due to an underlying issue with the hardware used in the tool itself? Moving higher up the chain, IT suppliers could be held liable for a failure to exercise sufficient oversight over the outputs that the AI tool produces before submitting outputs to Authorities, who in turn could be held liable for failing to properly implement the AI output. It is also possible that one or more AIs could be used by different stakeholders for their workstreams on the project or some or all of the stakeholders may be providing inputs / contributions to the operation of the different AIs on the project. Accordingly, AI use increases the number of potential disputes associated with one project, but it is important to bear in mind that the nature of these disputes largely depends on the project itself, what specifically goes wrong, and what is stated in the various liability and risk provisions of the relevant contracts.

How to manage AI risk

It is crucial that the various stakeholders are clear about the primary objectives of the project, and the ways in which AI will be used to achieve these objectives. Government bodies and local authorities should ensure that there are comprehensive agreements in place at each stage of the contractual chain to provide certainty in the event that something goes wrong, in particular in relation to any warranties and limitations of liability.

It is essential that the roles, responsibilities, expectations and risks of the various parties are contractualised and defined in detail from the outset of the project, so as to apportion liability throughout the chain with maximum clarity. This includes drafting very detailed and bespoke specifications for the AI tool along with the related customer services requirements (e.g. Statement of Works) and any

corresponding supplier solution responses that must be met by the relevant parties, which should be contractually tied into clearly identified timelines in a comprehensive implementation/project plan.

In the event that a technology project runs into difficulty, then it is likely that there will be a cascade of claims, with stakeholders seeking to recover their losses from the party next in the contractual chain. The claims will typically be for breach of contract arising from a failure to provide services in accordance with the express terms of the contract (e.g. by missing contractual milestones, or by the AI producing results which do not meet the contractual specifications for the AI tool itself or the operational use requirements for that AI tool), and/or with reasonable care and skill. Such claims may give rise to damages, termination rights and/or other contractual remedies specified in the contracts, such as delay payments.

The use of AI means that typical liability frameworks may not be suitable. Parties contracting to use an AI tool 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 will be deployed and should be based on standards that are clearly measurable. This will likely involve drafting warranties which, whilst based on common service standards such as reasonable care and skill, respond to the fact that an AI tool is being utilised. Examples of this type of warranty are 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; its outputs will be monitored and reviewed by a suitably qualified human and the AI developer uses a suitably diverse team to design and develop the AI software. Where the AI's outputs are subject to human oversight, the scope of such obligations should be clearly drafted, including identifying the required skills/experience of the individuals concerned, the nature of any training required, and the processes to be followed in testing, monitoring and reviewing the AI's outputs (e.g. testing and analysis of the AI outputs are to be carried out on a monthly basis for the duration of the project). Record-keeping in relation to the review of decisions made by AI solutions can also be helpful in managing the risk associated with their use.

Notwithstanding the merits-based challenges in establishing the causes of the failure of an AI tool, given the complexity of the development of the tool it is also important for government bodies and local authorities to recognise and mitigate against the risk that the AI developer (often start-ups) might not have sufficient assets available or sufficient insurance coverage to satisfy a claim.

The contractual issues referred to above are highly specific to the use to which the AI will be put, and so government bodies and local authorities thinking of utilising an AI solution should engage with their stakeholders, consultants, lawyers and other experts to help them navigate this complex and evolving area.

Key contacts

Sophie Ashcroft

Partner

Sophie.Ashcroft@brownejacobson.com

+44 (0)330 045 2600

Andrew Woolsey

Associate

Andrew.Woolsey@brownejacobson.com

+44 (0)330 045 2702

Related expertise

Services

Data protection and privacy

Technology disputes