Artificial Intelligence and the Law - practical measures to mitigate legal risk

18 October 2021
By: Phillip Kelly | Marcus Walsh | Sofia Wyzykiewicz | Simone-Young Alls

In its National AI Strategy published last month, the UK Government vowed to make the UK a "global AI superpower"[1]. This renewed focus on AI only increases the importance for businesses to address the novel legal issues raised by such technologies.

In the first two articles in this series we looked at (1) the approach which the courts have taken when faced with AI issues to date, and (2) some of the key legal issues and risks which are likely to arise in relation to AI.

In this final article in the series, we outline some of the important practical measures businesses can adopt to help safeguard their position when entering into AI-related supply contracts.

We have divided these into the three phases of commercial contracting: (i) pre-contract considerations; (ii) construction of contractual terms; and (iii) operational measures.

We have focussed primarily on the considerations for suppliers and customers, however we recognise that the contractual supply chain may well be more complex, and many of the practical measures outlined here will equally apply where there are multiple contracting parties.

Finally, we discuss what the EU Commission's new draft regulations on AI might mean for parties entering into AI contracts.

We will talk through these practical considerations using a case study example in our live webinar on Wednesday 20 October 2021, at 2-3pm UK, with 4 Pump Court.

Click here for more details and to register.

Pre-contract considerations

Thorough and extensive due diligence will be a key pre-contractual concern. From the customer's perspective, this should involve:

- considering exactly how the AI process will work
- how any software and training data used in that process has been sourced

For example, where training data is derived from other customers or third parties, the customer will need to ensure that the supplier has obtained the necessary licences and consents to enable it to use that data for the intended purpose. This will assist in assessing the overall litigation risk posed by the supplier's practices.

The supplier should have robust policies in place to mitigate the risk of (i) personal data breaches (where customer

information is to be used in the AI process), and (ii) bias and discrimination in the output. Just as the UK's National AI Strategy recognises that progress in AI is "best achieved through broad public trust"[2], so too should businesses be wary of the potential reputational risk where these controls are not in place.

Ultimately, at the pre-contract stage, both customer and supplier must assess the level of risk that entering into the contract poses. One way that both parties can help each other in this process would be by cooperating in the production and testing of a prototype of the supplier's AI. Using a prototype has the dual benefit of removing customer uncertainty about how the AI will function during the contract, and reducing the risk for the supplier that the customer will allege at a later stage that the AI does not meet its expectations.

Construction of contractual terms

If the parties are satisfied with the results of their respective due diligence exercises, the next task is to ensure that an agreement is put in place which provides for adequate contractual safeguards in relation to the AI. Again, there will be novel issues for both the supplier and customer to address here.

Considerations for the supplier

On the supplier side, limiting the scope of its liability to the customer will be crucial (particularly because of the distinct nature of the risks presented by AI). Firstly, AI processes are dependent on their training data set, and it may be difficult in the early stages of a project to predict how the AI will ultimately perform. Secondly, the autonomous nature of AI processes means that even minor deviations in how it is intended to perform could have significant ramifications; consider the potential consequences of a malfunctioning autonomous vehicle, for example.

The negotiation of strict caps and limitations on liability is an obvious starting point. In addition, the supplier should seek to define, in clear terms, the precise scope of the AI's performance (so that the customer is clear on what can and cannot be expected from the AI, and the circumstances in which it can be deployed). This may involve a reconsideration of the usual contractual obligation on the supplier to conduct its services with "reasonable skill and care"; where the AI process is largely autonomous, a supplier may not be able to make such guarantees on behalf of the AI, and this should be reflected in the drafting.

Both parties will need to consider how liability for breach is to be allocated. This is complex even in a simple two-party customer/supplier context, as there is much academic debate around whether an AI system can (or should) be held legally liable for its own errors[3]. The contractual arrangements become even more complicated when other parties are involved, for example, where the AI being supplied is produced by a third party, or the AI system in question uses the data of a third party or parties.The allocation of risk may be relatively straightforward from a drafting perspective, but much more difficult in negotiating which party/parties should bear the risk (and in what proportions). The complexity posed by such arrangements has led the European Commission to suggest that contractual risk may be better allocated by the provision of robust insurance provisions rather than seeking to make any one party[4] wholly responsible.

Considerations for the customer

On the customer side, a key concern will be its remedies in the event of breach of contract. While the supplier is likely to seek strict limitations on its liability, these should be closely scrutinised by the customer: do they accurately reflect the true level of potential damage that could result from an AI fault? If the AI process has the potential to cause significant harm, then attempts by the supplier to impose broad exclusions or limitations of liability may be inappropriate. As mentioned above, the allocation of risk is likely to be a key negotiation point.

In addition to liability, the usage of AI will raise other novel issues for how traditional contract terms are to operate on a practical level. For example, contractual audit rights would need to be adapted where an AI system is in scope. The customer is not so concerned with monitoring human processes, but rather with the performance of an automated, computerised process (for which traditional methods of auditing will be largely inappropriate). Instead, it would be much more desirable to ensure that (contractually) the customer can engage a forensic IT expert to conduct (or supplement) any necessary audits.

Finally, and crucially, is the question of who will own the fully trained model at the conclusion of the contract. The more successful the project, the more valuable the fully trained model (which will have learned and adapted from all the data and use cases it has been exposed to) at the conclusion of the project. If you are the customer, would you want the

supplier to be able to market the fully trained AI model to other businesses (including your competitors)?

Operational measures

Once the contract has been signed, all parties will want to continue to monitor the performance of the AI, and ensure that it is achieving the purpose for which it was agreed. Ongoing monitoring is particularly important in an AI context given the evolving nature of AI due to machine learning capabilities. It will also be important to the customer in verifying that the supplier's representations around performance or output are holding true, and that the terms of the contract are not being breached.

The supplier may also want to engage in ongoing monitoring to protect its own position, particularly if the parties have negotiated a continuous improvement clause, which may require the supplier to improve the service to the customer in alignment with advancements in the AI technology. Given the fast-paced and changing nature of AI, this will require close attention by the supplier (and close consideration should be given to any clauses concerning ongoing monitoring in drafting the contract).

Conversely, the supplier will also want to ensure that its own interests are being protected in the post-contractual phase (for example by ensuring that the customer does not breach intellectual property rights concerning the AI, or act in such a way that could lead to a data breach risk for the supplier where third party or customer data is used on an ongoing basis in the AI process).

Regulatory considerations

To date there has been minimal regulation of AI supply contracts at UK or EU level. However the European Commission has been working to establish a consistent approach to AI regulation and has recently published Draft EU Regulations on AI[5]. There are two key points that businesses should be aware of in light of the Draft Regulations.

- The Draft Regulations define an "AI system" as including software using "logic- and knowledge-based approaches". This would allow the Regulations to capture most computerised processes, which would give the Regulations an extremely broad scope of application.
- Secondly, and crucially, the Draft Regulations employ the principle of extra-territoriality, and so would extend the scope of the Regulation to outputs deployed in the EU *even if the supplier is located outside of the EU*. Therefore any contract for use of an AI process within the EU should factor in the likelihood that they will be caught by the Regulations (once finalised).

For UK businesses, there is an additional note of caution, as (in the aftermath of Brexit) the UK could seek to introduce its own specific AI regulations (which could add an extra layer of compliance for UK businesses operating at an international level). Indeed, the UK recently published a "Plan for Digital Regulation" in which it recognised the need for regulation (albeit in a way that does not inhibit innovation[6]).

Conclusion

Given the rapid pace at which AI is changing the world around us, it is likely that businesses entering into AI-related contracts will continue to face novel legal issues for years to come. In this series of articles we have sought to assess the current legal position and the likely areas of legal and contractual risk, and to provide practical methods for navigating this changing landscape.

Mitigation of the risks relating to AI requires early engagement with experienced lawyers who understand the cultural, legal and regulatory landscapes. To discuss the impact of AI on your business and how we can help, please do speak to any of the authors, or your DLA Piper contact.

Join the webinar

If you are interested in learning more about AI projects and the consequences for your contracts, register for our webinar on 20 October 2021, in collaboration with 4 Pump Court.

Artificial Intelligence Projects: Dispute Prevention and Resolution

Wednesday 20 October | 2-3pm BST

To register click here.

[1] National AI Strategy, HM Government, Office for Artificial Intelligence (22 September 2021).
[2] Ibid.
[3] See our second article in this series, Man vs Machine: Legal liability in Artificial Intelligence contracts and the challenges that can arise .
[4] Draft Report to the Commission on Civil Law Rules on Robotics, EU Parliament, 2015/2103 (INL).
[5] Draft Regulation laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative Acts, European Commission, 2021/0106 (COD) .
[6] Digital Regulation: Driving growth and unlocking innovation, HM Government, Department for Digital, Culture, Media & Sport (6 July 2021).

AUTHORS

Phillip Kelly
Partner
Birmingham | T: +44 (0)20 7349 0296 [UK Switchboard]
phillip.kelly@dlapiper.com

Marcus Walsh
Senior Associate
Dublin | T: +353 1 436 5450
marcus.walsh@dlapiper.com

Sofia Wyzykiewicz
Associate
Sheffield | T: +44 (0)20 7349 0296 [UK Switchboard]
sofia.wyzykiewicz@dlapiper.com