THOMSON REUTERS

REGULATORY INTELLIGENCE

Legal liability for financial institutions and financial services firms when using artificial intelligence and machine learning

Published 20-Mar-2020 by
Charlotte Walker-Osborn, Eversheds Sutherland

Recent advances in the development of artificial intelligence (AI), coupled with the availability of sufficient computing power to enable the effective use of AI, have made its application to the financial services sector a reality. Robotic process automation (RPA) is being used to handle repetitive tasks, removing the need for human effort. Machine learning (ML) tools can identify connections within data sets and AI-based reasoning can be deployed to extrapolate to previously unknown connections.

There has been a recent surge in activity by the sector to apply ML and AI to various problems including fraud detection, anti-money laundering (AML), process automation, decision-making and personalised financial planning. In the banking sector, firms are expecting their number of applications to triple in the next three years, according to the Bank of England and Financial Conduct Authority's (FCA) joint report on machine learning in UK financial services, published in 2019. Some recent examples include:

- BNY Mellon announced in May 2017 that it had rolled out more than 220 bots developed by Blue Prism to handle repetitive tasks that are normally handled by staff, e.g., "data requests from external auditors" and "funds transfer bots" which help "correct formatting and data mistakes in requests for dollar funds transfers". It is estimated that the activity of its "funds transfer bots" alone is responsible for $300,000 in annual savings (source: Thomson Reuters).
- In June 2019, HSBC signed a collaboration agreement with Canadian AI firm Element AI to help the bank develop capability to analyse data from clients of its global banking and markets unit. The data analysis aims to help the bank meet worldwide regulatory requirements such as AML rules more efficiently, as well as allowing it to predict what services and product solutions its clients may need in the future (source: Finextra).
- It has been reported that JPMorgan Chase increased its technology budget to more than $10 billion in 2019 and the organisation introduced its Contract Intelligence (COiN) platform to help review 12,000 annual commercial credit agreements, reducing time down from 350,000+ hours to seconds or minutes (source: JPMorgan Chase).

Leading financial services firms and companies are data-rich and already have the requisite know-how and rules to make decisions based on data. While many financial services companies already have sophisticated ML and RPA tools at their disposal, in future the leaders will be working heavily with AI companies to allow the AI to be able to analyse these vast data sets, including natural language documents, against these rules. Given that backdrop, it was inevitable that the two would come together to deploy leading-edge AI to the sector. The approach and outlook of the parties will have a significant impact on the structure of the collaboration and the legal implications.

Legal and liability considerations

There are some important liability considerations for the sector in adopting these forms of technology or even marketing itself as a provider of this sort of information.

Data and data privacy

Consents/right to use the data

Clearly, there must be a right to use the data in the way envisaged both now and in the future. This becomes more problematic where data involves the personal data of individuals, particularly where firms need either to gain specific consent for usage or find another legitimate reason under the law to be able to utilise that personal data.

Getting the right data and ensuring there is no bias

Forms of rtificial intelligence technology evolve through use. Iteratively training an AI system using a new data set gives rise to a new model whose properties and behaviour are modified by that training data. The trained model embodies the training data. There are a number of high-profile examples where either insufficient data, the wrong data (including historical data) or the wrong training of that data has led to the wrong decisions and introduced bias. It is therefore imperative for financial services firms that these elements of the project are carefully thought-through.

The implications of being challenged on a decision are arguably largely the same as for decision-making which does not use AI, but it will be very important to be able to understand what data was used, how it was tagged, how it was trained and, increasingly, to be able to justify how the decision was arrived at.

There has been a huge push, both in the UK and the EU, to introduce laws (and consequential liability) specifically regarding AI in this area (see, for example, the European Commission's recently published white paper on artificial intelligence). At the heart of much of the AI-specific legislation is human agency/oversight, robustness and safety, privacy and data governance, transparency, diversity, non-discrimination and fairness, and societal and environmental wellbeing. Compliance with these areas should in future be factored into projects, to avoid falling foul of the law or incurring liability as a result of non-compliance.

As an overarching point in relation to data, intellectual property law struggles, in many countries, to deal with AI forms of technology. New laws will, therefore, emerge in a number of countries in the coming years. Firms should ensure their legal teams look at intellectual property carefully when working on any collaboration deal and, in the absence of clarity in some areas, utilise the contract carefully to ensure liability for breach of intellectual property is in the right place.

Privacy and personal data

As with any activities involving personal data, a data protection impact assessment should be performed, and firms should ensure their contracts with the AI provider allow them to allocate and/or discharge their regulatory and transparency obligations fairly. Depending on the collaboration, it may be possible to ensure anonymised or pseudonymised data sets are utilised. Even then, there are data privacy issues to address, including the need to ensure that a data subject cannot be re-identified.

There is a plethora of guidance and blogs emanating from the the UK privacy regulator, the Information Commissioner's Office (ICO), including an auditing framework for AI. Firms ignore these at their peril, as arguably one of the largest areas of risk for companies adopting or offering out these services will be failure to comply with legal obligations under privacy laws, with the potential for resulting fines in the region of tens to hundreds of millions of pounds and/or potential criminal liability.

AI and cyber security

Ultimately, forms of AI technology reside on servers, whether the firm's own, the AI provider's or in the cloud. Data and technology inevitably bring cyber risk. A cyber breach could lead to financial loss for the business and a risk of non-compliance with law (including privacy laws and cyber security-specific laws) with, again, the potential for resulting fines and even criminal liability. It is therefore critical that firms address this in their contracts with their AI providers and with their customers. It is also crucial that a detailed analysis takes place early on regarding the technology set-up, the data flows and the security. The analysis is, largely, the same as for other technology projects.

Where AI meets financial regulation

Firms will be familiar with the strong emphasis the regulator places on technology projects and, again, in this respect AI projects should be looked at with the same rigour, otherwise there will be similar consequences for non-compliance.

For example, there may be a requirement for authorisation. Activities could result in the business carrying out a regulated activity, and this includes where an algorithm is performing investment management or dealing activities. This brings a need to factor in all the usual prudential requirements required by the FCA.

Critical analysis at the outset is vital, given the nature of AI solutions, the regulator's focus on human agency/oversight and the privacy, data governance and transparency considerations. Firms must also determine how they will deal with, and allocate, risk, and how they will factor in oversight and governance. They must also assess the potential implications of failure, both for individual customers and in terms of the company's liabilities. Early engagement on the legal issues is paramount, and the author strongly recommends that such considerations should be set out carefully in any collaboration agreement/contract.

Please note that the information provided above is for general information purposes only and should not be relied upon as a detailed legal source.

By Charlotte Walker-Osborn at global law firm Eversheds Sutherland

Complaints Procedure

Produced by Thomson Reuters Accelus Regulatory Intelligence 23-Mar-2020

THOMSON REUTERS™