THOMSON REUTERS

REGULATORY INTELLIGENCE

Deploying artificial intelligence in financial services risk management and compliance

Published 14-Feb-2020 by
Daniel Csefalvay, Siân Cowan, Jason Alvares, Bryan Cave Leighton Paisner LLP

In financial services firms, risk management and compliance functions are among the most likely to use machine learning tools, and have some of the most mature levels of deployment of the technology among regulated firms, according to a survey published in late 2019. The research was undertaken by the Bank of England and the Financial Conduct Authority (FCA).

The most advanced deployment of machine learning technology was found in the banking and insurance sectors, most commonly in anti-money laundering and fraud detection as well as customer-facing applications such as marketing.

Although use of the technology in financial services has been described elsewhere by the FCA as "nascent", artificial intelligence will increasingly be used in financial services to augment the identification of misconduct by firms' employees — misconduct that may not be detected by conventional monitoring. Electronic communication systems have long been monitored for lists of words that may indicate suspicious behaviour. Artificial intelligence and machine learning can now recognise hidden patterns in data, beyond the mere identification of a list of suspicious words.

Profiling

Artificial intelligence systems are able to detect subtle variances and patterns in the properties of electronic messages — such as timing, frequency, tone, vocabulary or recipients — that can suggest a greater likelihood of wrongdoing. These correlations can be inferred only by iterative machine analysis of large data-sets, and are unlikely to be identified by simple rules-based monitoring.

Such artificial intelligence-assisted profiling techniques are also employed by social media and adtech platforms, where their usage may be more familiar. Over time, the "data exhaust" from our electronic interactions is used to build a profile of characteristic behaviour.

When we deviate from these unconscious habits, artificial intelligence tools can also be used to flag an event of potential interest. A "human in the loop" can then assess whether the flagged events may be suggestive of rule-breaking or criminal actions. These artificial intelligence tools vastly reduce the human input required by risk and compliance teams, enabling surveillance of much larger groups of people, in much greater detail.

Bank of England, EBA and FCA

Regulators are now beginning to show an interest in how artificial intelligence is deployed. The Bank of England is working with the FCA to establish an AI Public-Private Forum to share information on the use of artificial intelligence and machine learning in financial services, barriers to deployment and potential risks or trade-offs. It will also identify areas for guidance, principles, regulation or good practice examples. The forum's first meeting will be held at the end of March 2020.

The European Banking Authority in January also published a report on "Big Data and Advanced Analytics", identifying as the main pillars: data management, technological infrastructure, analytics methodology, organisation and governance, along with "elements of trust" such as ethics, explainability, fairness, auditability and data protection.

A speech by Christopher Woolard, who was recently elevated to interim chief executive at the FCA, outlined back in July 2019 how the FCA is likely to approach the issues. Woolard pointed out that the risks of artificial intelligence need to be assessed in each specific use case for the technology. The risks of algorithmic trading are totally different to the risks of using artificial intelligence for credit ratings or to calculate an insurance premium.

High-level principles, such as transparency and accountability, are said to provide a framework for identifying the specific harms and safeguards needed. Culture and governance are called out as particular safeguards. Boards are advised to ask: what is the worst thing that can go wrong?

An opinion piece published by the FCA noted public pressure on firms to explain decisions informed by machine learning. It identified a trade-off between the ability to provide accurate artificial intelligence insights efficiently, and explaining how these insights were determined. Revealing too much information may allow the system to be gamed. To some extent, much artificial intelligence can remain an impenetrable "black box". Even the programmers cannot understand exactly how the results are determined.

Yet where insights from artificial intelligence have significant impacts on individuals, such as in risk management and compliance, individuals will demand explanations. Someone in the firm needs to be accountable for the model's decisions, perhaps a senior manager. The models need to be appropriately tested and controls need to be implemented. Regulators will expect to see evidence of effective accountability, which is likely to include a sufficient element of interpretability and explanation of the model.

ICO and CDEI

In December 2019, the Information Commissioner's Office (ICO) published a consultation on requirements for explaining decisions made with artificial intelligence. The ICO has published a wide range of documents that need to be considered when deploying artificial intelligence. Issues with artificial intelligence where the ICO has declared its interest include: artificial intelligence auditing frameworks, meaningful human reviews, accuracy and performance measures, security risks exacerbated by artificial intelligence, bias and discrimination, preserving privacy, data protection impact assessments and rights of access, erasure and data rectification. Each of these issues requires a careful balancing of the data protection risks and the individual rights at stake.

The wider framework for artificial intelligence in the UK is being led by the government's Centre for Data Ethics and Innovation, which articulates best practice. Research commissioned by the centre has noted that in police work relying on artificial intelligence technology, there is an absence of consistent guidelines for the use of automation and algorithms, which may lead to discrimination. A further report on algorithmic bias is expected from the centre in March 2020.

Closing thoughts

Artificial intelligence-enhanced risk management and compliance can spot risky behaviour early enough to intervene before significant losses are incurred. Predictive monitoring can even anticipate where the next risk or compliance incident will occur. This highlights the ethical conundrums of using machine learning with regulatory consequences; everyone wants to avoid the stuff of science fiction classic "Minority Report", where psychic foreknowledge is used to apprehend "criminals" before a crime is committed.

Although deployment of machine learning technology is still developing in financial services compliance, the outlines of the issues that need to be considered are already fairly clear.

By Daniel Csefalvay, Siân Cowan, and Jason Alvares at Bryan Cave Leighton Paisner LLP

Complaints Procedure

Produced by Thomson Reuters Accelus Regulatory Intelligence 17-Feb-2020