A-Team Insight

Top 6 Use Cases for AI in RegTech

22 March 2022

As artificial intelligence's influence on regtech continues to grow, so does the importance of minimising algorithm bias and maximising data quality.

The use of Artificial Intelligence (AI) and machine learning in RegTech is playing an increasingly important role and helping to reshape risk and regulatory compliance. It can offer many benefits and we outline the top 6 use cases below. We also explore some of the considerations around the set up and structure of models and any inherent algorithm biases, the underlying quality of the data that feeds the models, and the cyber threats that can damage the integrity of AI models.

AI Use Case 1: Regulatory Change Management

According to Yin Lu, head of product at SaaS regtech developer CUBE Global, the most valuable application of AI in regtech is at the level of regulatory change management.

"Before firms can comply with regulations in specific domains they have to understand (and stay up to date with) all the regulations that apply to them," she says. "This is an especially complex task for firms with business and product lines across multiple jurisdictions and cannot be resolved without AI as the volume and velocity of regulatory change is too immense."

Lu believes we are approaching the point where the moment a regulatory update is made regulated firms will be alerted about which of their policies and controls have to be modified – and in some cases, even how.

“What makes this application of AI all the more exciting is that ultimately it can help regulated firms influence regulation,” she continues. “Reg change software can highlight discrepancies between regulations that apply to the same business or product as well as their unexpected impact. This will help regulators build clearer and more consistent regulations.”

AI Use Case 2: Validating Regulatory Data

The potential of AI to identify the same transactions reported by firms and highlight where a firm is reporting syntactically correctly but is actually incorrect versus its peers – essentially a three-way check to validate data integrity versus a firm’s systems and the regulator – is another potential application says Jethro MacDonald, product manager AI & ML/innovations lab at SmartStream Technologies.

AI Use Case 3: Trade Surveillance

Independent regtech advisor David Cowland references potential benefits in the trade surveillance or communications surveillance space, which are plagued by false positives that account for up 99% of alerts.

Adrian Tam, director of data science at digital transformation consulting firm Synechron reckons the industry should be looking at introducing more robotic process automation before thinking about introducing anomaly detection technology to flag suspicious transactions.

“This is where AI can play a role, but it is also an arms race that we need to continuously invest in since there are new ways to circumvent the monitoring emerging every day,” he adds.

AI Use Case 4: Testing

The key factor in successful implementation of AI in a regulatory context is testability suggests Kyle Hansen, head of AI engineering at data software firm Kingland.

“It is very important to have clear insight into the distribution of your training data and how well your model represents those various scenarios,” he says. “This is also important for regression testing, where we make sure changes to the model did not damage its effectiveness.”

AI Use Case 5: Managing Data Quality

Fiona Browne, software development & ML team manager at data quality specialist Datactics recommends measuring and addressing data quality such as completeness, accuracy and representativeness; using clearly documented methods and processes for the identification and management of bias in inputs and outputs; and having governance in place to ensure accountability.

“AI must successfully establish an understanding of the causality in the data and demonstrate the ability to perform inductive and deductive reasoning,” says Danny Butvinik, chief scientist at financial crime, risk and compliance solutions provider NICE Actimize. “It must also address inconsistencies within regulation across different jurisdictions as well as dynamic and evolving rules.”

Cowland notes that firms have no defence if the software misses or omits something that is a regulatory necessity. “Technically, they must demonstrate how the AI makes adjustments (model drift) or how it is using real time data to make adjustments,” he says. “It shouldn’t require an army of people to make it work in the background and business leaders must be able to understand and explain it.”

AI Use Case 6: Analysis by Regulators

Tobias Adrian, director of the monetary and capital markets department of the IMF has highlighted a number of examples of the use of AI by supervisory authorities.

These include the ECB using machine reading of the ‘fit and proper’ questionnaire to flag issues and to search for information in supervisory review decisions to identify emerging trends and clusters of risks. Bank of Thailand is using AI to analyse board meetings minutes of financial institutions for regulatory compliance and De Nederlandsche Bank uses AI data analytics to assess the exposure of financial institutions to networks of suspicious transactions.

Managing Embedded Bias

An October 2021 IMF research paper referred to discussions around the risk of embedded bias creating differentiation in pricing or service quality, warning that effectiveness of AI/ML-driven supervision depends on data standardisation, quality and completeness.

Harish Doddi, CEO of machine learning specialist Datatron acknowledges that creating an unbiased algorithm is difficult.

“During development?ML?models are bound by certain assumptions, rules and expectations but the results in real-world production can differ significantly from results in controlled development environments,” he says. “One thing all?companies can do is ensure that metrics such as the true accuracy and false positive rate are consistent when comparing different social groups.”

Key Questions to Ask When Developing AI Models

AI model governance helps introduce accountability and traceability to machine learning models by having practitioners ask the following questions:

- What were the previous versions like?
- What input variables are coming into the model?
- What are the output variables?
- Who has access to the model?
- Has there been any unauthorised access?
- How is the model behaving when it comes to certain metrics?

AI needs to be trained like a human so the more diverse data provided to the model the better it will become at making the right decisions, says MacDonald. “We can also embed AI into systems in a way where it helps users with their workload but doesn’t make the final decision, instead presenting a result for a user to validate.”

This is not simply a technology question adds Browne. “It also highlights the need for diverse representative teams to build and deploy these models and flag up potential ethical/bias issues before production,” she says.

Firms can also apply bias elimination and alleviation methods such as balanced clustering and descriptive analytics.

Protecting AI Models from Cyber Threats

Companies can protect their AI models from cyber threats by threat modelling adversarial machine learning (attempts to exploit models by taking advantage of obtainable model information and using it to create malicious attacks) explains Hansen. “We can look at ways the model could be exploited once deployed and develop filtering or other countermeasures to reduce the effectiveness of these attacks,” he adds.

To withstand cyber threats, companies need to employ privacy machine learning paradigms where differential privacy and homomorphic encryption play a central role adds Butvinik. “Another objective is to design ML algorithms that responsibly train models on private data,” he says.

Tam cautions that firms need to implement their firewall to guard against the illegitimate flow of data. “Setting up the data access mechanisms and assigning each model a role, for example, is how we can safeguard the boundary,” he says.

To ensure that models are sturdy enough to counteract cyber threats it is important that they operate within private networks and that traffic to and from these networks is strictly controlled.

“All the cloud resources involved (including data storage) need to be protected as well – they should all be part of the same private network,” suggests Lu. “Authentication and authorisation guardrails have to be put in place to ensure that only specific individuals within the business can access the resources.”

When asked if there are any risk factors around sharing knowledge institutionally, Kingland’s head of data science and analysis, Jesse Sommerfeld says there is room for conflict where ‘trade secrets’ are pitted against societal value. “Direct institution-to-institution knowledge sharing is unlikely to happen given the value each institution may place on their knowledge,” he concludes.