CENTRE DE DROIT
BANCAIRE ET FINANCIER

Banking group

Implementing artificial intelligence

Par Gaëlle de Cannière le 14 October 2024

ChatGPT and GenAI – these new words have been part of our daily lives since November 2022, and we no longer need to introduce them. The growing use of artificial intelligence (AI) in the banking sector raises complex legal and regulatory issues. How do you navigate the world of AI when you are active in the financial sector in Switzerland ?

The starting point is to understand the existing legal and regulatory framework. To date, there are few laws specifically governing AI. However, several projects are at more or less advanced stages in the legislative process. These include the European Regulation on AI (see cdbf.ch/1359/), which came into force on 1st August 2024, and the Council of Europe's work on a Convention on Artificial Intelligence, which is open to ratification. It is also worth mentioning the work done by UK and Canadian legislators to enact a law on AI.

When it comes to AI, most financial regulators have not waited until 2022 to set out their expectations. For example, the CSSF (Luxembourg) has already conducted a study and made its recommendations in December 2018 and notes in particular that *top management* is ultimately responsible for the use of AI and *machine learning*. The same applies to BaFIN (Germany), which is publishing its guidelines for the use of AI in June 2021. More recently, it was ESMA's turn to issue recommendations on the use of AI in compliance with MiFID II. FINMA, for its part, has identified four key areas in connection with the use of AI, which are (1) the definition of roles and responsibilities, (2) the accuracy and reliability of results, (3) transparency and explainability, and (4) non-discrimination. At the legislative level, DETEC is expected to take a position by the end of the year on whether to legislate on the subject. A regulatory watch needs to be put in place to identify these new requirements, which are published almost daily.

Overall, the regulators stress the importance of (1) implementing a strategy, (2) defining governance, (3) identifying risks and controls and (4) training employees, which are four key points to bear in mind when AI is implemented in a financial institution.

The strategy

The Board of Directors has the ultimate power to approve a strategy. Its members must therefore be trained and made aware of the issues in order to be able to define a strategy : do we authorise AI ? If so, within what framework and for what purposes ? What are the limits ? etc. These questions must be addressed and formalised, then approved by the board of

directors or the competent local body.

Governance

To implement the strategy, roles and responsibilities need to be assigned, particularly for the IT department, the IT security department or the legal department. We must not forget all the lines of defence (L1, L2 and L3), each of which has its own role to play. When the first line of defence has to implement the AI model in accordance with the defined strategy, the second line of defence will have to monitor compliance with the rules by the first line and finally, the third line will have to audit it. It is therefore important to involve the various competent players from the outset of an AI project and to obtain the necessary internal approvals (for example, from management, a project committee, business line committees, etc.). Making these roles permanent is key to ensuring solid governance, and this can be achieved by drafting an internal policy on the subject.

Risks and controls

The use of AI presents specific risks, such as the protection of personal data, intellectual property, security and the management of third parties. It is essential to use existing processes to identify these risks. In this way, each organisation can assess its risk appetite and take appropriate mitigation measures. In particular, there are the risks associated with where personal data is stored or processed, the re-use of data to feed AI or the risks of data leakage.

Training

Employees must be made aware of these risks and trained. Such training needs to be tailored to the target audience, for example, from general awareness to specific training for experts. As far as possible, the level of skills required to manage an AI system should be permanent and acquired, at least in part, internally.

Implementing AI within a banking group raises a number of challenges, of which I will mention just three here. Firstly, the experts, management and competent bodies must agree on a definition of AI. Even though a definition has now been given by the OECD and the European regulation on AI, discussions between experts about what is really ‘intelligent’ and what is not are inevitable. Secondly, the speed at which this technology evolves and is adopted by society, and consequently by employees and customers, needs to be monitored. You have to be reactive to stay competitive. Finally, we need to be transparent about our AI strategy and the optimisation of our processes, so as to break out of *task force* mode. In other words, we need to think about ‘industrialising’ the implementation of AI.
