December 2018

Artificial intelligence: challenges for the financial sector

Discussion paper

AUTHORS
Olivier FLICHE, Su YANG - Fintech-Innovation Hub, ACPR

ACPR
BANQUE DE FRANCE

SUMMARY

The ACPR's work on the digital revolution in the banking and insurance sectors (March 2018) highlighted the rapid growth of projects implementing artificial intelligence techniques. A task force was therefore established by the ACPR in early 2018. It brought together professionals from the financial industry (business associations, banks, insurers, Fintechs) and public authorities to discuss current and potential uses of artificial intelligence in the industry, the associated opportunities and risks, as well as the challenges faced by supervisors. The purpose of this discussion paper, based on these discussions as well as on exchanges abroad or with other French players, is to present a first diagnosis of the situation and to submit to consultation the reflections that deserve further study to enable the development of these new technologies within a secure environment.

Artificial intelligence is a polysemous notion that tends to cover different realities as algorithmic techniques evolve: the report followed a relatively broad definition of artificial intelligence, including all machine learning techniques, but generally excluding robotic processes that automate repetitive cognitive tasks.

The first finding by the *Task Force* is that projects based on artificial intelligence are at uneven levels of progress and their development is often less advanced in the processes that a supervisor would tend to consider to be most sensitive. However, all conditions are met for a rapid and widespread development of artificial intelligence techniques in the financial sector: a growing awareness of the possibilities of exploiting data, which are increasingly numerous and varied; development of available technology offers (open source libraries, new specialised players, major technology providers, notably through the cloud…); multiplication of tests and projects.

There are many uses – in production, tested or just planned - covering most of the banking and insurance activities: from customer relationship (with the already very advanced rollout of chatbots and also opportunities in advice or explanation to customers), back office management (e.g. insurance claim management) to personalised pricing, risk management and compliance (fraud detection, anti-money laundering, cyber security, internal risk modelling for regulatory capital requirements).

The development of these technologies is naturally not without risk: those inherent in the techniques used and those associated with their “disruptive” power. The first category relates to the risk of algorithm bias, increased by their complexity and the effects induced by the combination of the different underlying statistical and heuristic methods, as well as cyber risks. In the second category are risks related to the possible emergence of a small number of key players in the use of these techniques and the power relations - possibly systemic effects – that such a phenomenon would induce.

Against this background, supervisors have to deal with issues with strong differences in statement and time horizon.

In the short term, it seems important that the development of artificial intelligence in the banking and insurance sectors be accompanied by practical reflection on the minimum criteria for governance and control of these new technologies. This should allow for progress, among other things, on techniques to prove the reliability of the algorithms used (for both internal and external auditability), their “explainability” and the interactions between humans (clients, advisers, supervisors, etc.) and smart algorithms. It also needs to clarify, more generally, what good “governance of algorithms” might look like in the financial sector.

At the same time, supervisors need to remain alert to the medium and long-term impact of artificial intelligence developments on the market structure in order to anticipate the necessary changes in the performance of their mission.

Finally, the discussion paper discusses the need for increased expertise and cooperation of supervisory authorities to address these two types of issues.

Keywords: artificial intelligence, Fintech, innovation, technology, digitisation

JEL codes: G28, O38

CONTENTS

Introduction

The use of artificial intelligence (AI) in the financial sector is subject to mixed judgements. On the one hand, this set of new techniques holds great promise for the future of financial services. On the other hand, its practical applications still face many unresolved challenges. However, real and rapid progress in this area could soon solve the question, as the industry appears to be on the brink of a set of innovations that will profoundly transform it.

The importance of AI is becoming more evident as the digital transformation[1] landscape becomes clearer. Companies have realised the value of the data they have. They now need tools to make better use of them. The rise of artificial intelligence is thus fostered by a twofold movement: on the one hand, the digitisation of the economy and the automation of existing processes; on the other hand, a breakthrough on the supply of services based on Big Data.

This paper was prepared by the Fintech-Innovation Hub of the ACPR. It follows up on the discussions of a task force composed of market participants and public authorities, and is based in particular on the answers of the *task force* members to three thematic questionnaires drawn up by the team. It also benefits from the discussions led at the national level by the Autorité des Marché Financiers (AMF), the Banque de France, the Commission Nationale de l'Informatique et des Libertés (CNIL), Tracfin and the Treasury Department, as well as at the European and international level by the Financial Stability Board (FSB), the European Banking Authority (EBA), and the European Insurance and Occupational Pensions Authority (EIOPA).

The document first features the state of development of artificial intelligence in the financial sector and the factors that accelerate this development. In a second step, it lists the use cases of AI in production or in development in the banking and insurance sectors to identify risks and opportunities that artificial intelligence represents to the market. This dual diagnosis allows, in a third part, to identify the challenges for supervisors associated with changes in the short, medium or long term.

[1] The digital revolution in French banking and insurance sectors, ACPR, March 2018. Sectoral studies (bank and insurance) are available on the ACPR's website.

1. The development of artificial intelligence in the financial sector

1.1. Artificial intelligence, a polysemous notion

1.1.1. Defining artificial intelligence

The definition of artificial intelligence (AI) gave birth to very different formulations ranging from imitation of human cognitive functions to the ability to interact with the environment, through the ability of a machine to achieve objectives autonomously. The aim of AI is to imitate different cognitive functions such as perception, memory, reasoning and learning or to reproduce skills such as organisation, description and processing of information. However, although artificial intelligence can be defined as the set of technologies to imitate human operation autonomously[2], it seems useful for the purpose of this document to restrict the concept of AI to programmes that have at least an autonomous learning capability, in other words, to machine learning algorithms[3].

Today, the technical progress of AI is mainly within the area of **machine learning**, i.e. all the algorithms that make it possible to learn by identifying relationships within data and to produce predictive models in an autonomous manner. **Deep learning** is a particular area of machine learning whose algorithms are particularly effective in processing complex and unstructured data such as images or voice.

To mention but one example, **the natural language processing** (NLP), which consists in developing algorithms to process language data such as phrases or texts, is one of the most dynamic research areas today. It is used for example for an automatic first reading through of emails by banking institutions.

Other robotics processes, assimilated to AI, are understood as opportunities to improve the customer experience (proximity, fluidity, customisation, increased transparency…), productivity growth and well-being of employees. Automation of the most repetitive tasks allows for more creative or higher value-added tasks. They will not be discussed in detail in this document.

1.1.2. Factors of its growth

The major advances in artificial intelligence, both in the financial sector and elsewhere, are based on three main factors:

- **Data availability and diversity**. One of the drivers of *Big Data* is the growing availability of data, both structured and unstructured: there is now an annual growth of 80% of the quantity of unstructured data (photos, videos, texts, cardiac signals…). For example, 90% of the data available in 2016 was produced over the previous two years[4].

[2] Tools that automate repetitive manual or cognitive tasks such as *Robotic Process Automation* (RPA) or text entry or data collection via *Web Scrapping* are sometimes considered to be rudimentary applications of AI. However, the term AI now refers to much more complex algorithmic processes.

[3] For a more general context, see Annex I.

[4] *Straight talk about big data*, October 2016 McKinsey, Nicolaus Henke, Ari Libarikian and Bill Wiseman

- **Increasingly efficient IT equipment**, both in terms of storage, computing speed (according to Moore's Law) and infrastructure (*cloud computing*).

- **Progress in machine learning** *(*or *statistical learning*), especially in the area of *deep learning*, or more generally the development of tools to exploit increasingly diverse and large amount of data (*Big Data*).

Financial players thus benefit from the progress made in AI by other sectors, first of all major technological firms that finance most of the research and development in this area. More general factors further strengthen this progress:

- **Expectations of consumers**, accustomed to faster and more ergonomic digital services;

- **Enhanced trust of the consumers** in technology;

- **The maturity of the technological solutions and related methodologies**, especially in the field of computer security and agile working methods.

As a corollary, lowering the costs of these technologies fosters the development of Fintechs, increases client expectations, urging banks and insurers to invest in these technologies.

1.2. The development of artificial intelligence in the financial sector takes place against a background of profound mutation of IT infrastructures.

1.2.1. The stake in the data changed the strategic priorities of banks and insurers

After the crisis of 2007-2011, banks and insurers focused on strengthening the compliance and risk management departments, supported by regulatory developments and enhanced financial supervision. This trend has stabilised for several years to give rise to another stake: the data.

Indeed, with the emergence of large internet players, the role of data has become central in many sectors of the economy. The financial industry is no exception, with the arrival of innovative players building new business models utilising their knowledge of the customer, their understanding of his/her behaviour and the upgrading in his/her expectations.

The rapid development in artificial intelligence in the financial sector is broadly due to its value added in terms of data exploitation and also to the growing availability and quality of data collected. For financial players, exploiting them is an opportunity to improve the customer experience and the performance of the distribution function, increase productivity and operational performance, and improve risk management. So there is a symbiotic relationship between artificial intelligence and data: as data become a critical competitiveness stake for financial players, mastering AI becomes necessary.

1.2.2. Projects to unequal degrees of progress

The progress of AI projects is marked by a significant disparity. The implementation of such technologies seems more advanced in the banking sector than in the insurance sector, while algorithmic has been developed in investment banking and asset management activities since the 2000s, preceding the development of AI tools.

The effective use of complex algorithms, such as those operating *deep learning*, is only in certain limited areas: translation, *chatbots*… Most of the applications of AI are based on simpler learning algorithms, leading some of the players to argue that AI is already used in most financial activities. Indeed, it is already widely deployed to optimise operational processes, either to process written contents with greater efficiency through the use of NLP technologies, or to address fraud issues. By contrast, it seems to be very little used in activities with a strong impact on the customer, such as *credit scoring*, advice, client underwriting processes, automatic responses… activities that will probably not incorporate AI before 2020.

Finally, the heterogeneity of AI adoption can be explained by the differences in strategy at work in financial institutions. Most banks and insurers use both *Open Source* libraries[5] operating internally and solutions provided by technology partners. However, smaller financial structures tend to develop their own tools (some do not use any technology providers, even though it is rarely true that everything is done from scratch: the use of *Open Source* libraries seems to be a common denominator).

More generally, the development of AI tools is conducted in three ways, often complementary:

- **Through internal development**, typically via *Open Source* libraries such as *ScikitLearn, Keras*, *Faiss* or *Tensorflow*. These algorithms often help to gradually improve the interpretability and "explainability" of machine learning.
- **Through large technology provider** offering solutions incorporating AI, like Microsoft and its *Pack Office* or Salesforce.com. Almost all financial players use this type of services, especially for the *Cloud* (see below).
- **Through service offers of new players** including AI. Again, many banks and insurers are involved. Note that this includes Fintech providing services integrating AI (such *as Shift Technology*) as well as generalist technology providers (such as *Datarobot*).

1.2.3. Widespread use of *the Cloud*

The need to exploit exponential quantities of data raises new technical challenges. Internal storage, a solution preferred by many up to now, presents several major limits: the cost of maintaining servers, the variability of storage needs, growing vulnerability to attacks… Using *Cloud* and *Big Data* technology providers is therefore not only beneficial but sometimes also necessary, depending on the financial actors, to optimise the data potential and, ultimately, artificial intelligence tools.

The vast majority of financial institutions use *cloud computing* services, and its extensions including AI, on part of their activities. The main benefits they identify are:

- *Flexibility*: The company may modulate the storage capacity it leases according to its needs.

[5] The term "open source" applies to software (and sometimes more broadly to intellectual works) whose licence complies with criteria precisely established by the Open Source Initiative, i.e. possibilities of free redistribution, access to source code and creation of derivative works. Available to the public, the source code is generally the result of collaboration between programmers. Wikipedia

- *Interoperability*: Since the services are offered on a remote server, access to these resources can take place from any device that allows the exchange of data (smartphones, computers etc.).

- *Mutualisation:* The *Cloud* allows to respond to variations in computing power and bandwidth needed by customers. In pooling them, it ensures user cost optimisation.

- *Security and availability*: *Cloud* providers often make several copies of the data and store them at different locations[6]. Therefore, access to data is almost permanent and data loss very unlikely.

- *Access to state-of-the-art technologies: Cloud* providers have technologies that financial players cannot buy, including some of the AI algorithms embedded directly on *cloud computing* solutions…

Financial players benefit from the expertise of *Cloud* providers in both operational and security terms. However, the *Cloud* also increases some cyber risks to the extent that most financial institutions are adopting its use and that data pass through the company as well as the network and the *cloud* service provider: many potential vulnerabilities having to be monitored[7].

Cloud market leader is undoubtedly *Amazon Web Services* with 40% of market shares worldwide. Microsoft (with *Microsoft Azure*), IBM (with *Blue Cloud* or *Bluemix*) or Google *(Google Cloud Platform*) are the main challengers and hold 23% of the market[8]. The American hegemony is hardly challenged by Asian players: globally, only *Alibaba Cloud* really competes with US players. Most of these technological providers offer, in addition to storage services, services to monitor transactions, data analysis, domain management and applications/media services… Such services could incorporate artificial intelligence and thus increase the stake of strategic and technological dependence to *cloud* providers.

[6]It should be noted that the practice of back-up centres is also common in the "internal" IT systems of bankers and insurers as part of their business continuity plan.

[7]On the IT risk side, the ACPR also published a paper in March 2018, which includes elements relating to the use of the *Cloud*.

[8]*Microsoft, Google and IBM Public Cloud Surge is at Expense of Smaller Providers*, February 2017, Synergy Group

2. Artificial intelligence in the financial sector, opportunities and risks

2.1. Uses and opportunities

2.1.1. The stake of competitiveness and quality of the offer

In terms of competitiveness, mastering artificial intelligence appears to be a strategic priority[9]: it helps to build a faster decision-making process, to be closer to the technological frontier and to prevent that a technological oligopoly be built up by a few players (GAFAM, BATX). According to Villani[10]'s report, French financial players are not late for AI; however, it seems essential to remain among the most advanced countries on the topic given the forthcoming transformations.

For players in the financial sector, the operational benefits of artificial intelligence are manifold:

- *From a marketing perspective*. Data analysis helps to **better understand the needs** of customers and understand what aspects of a particular financial product need to be improved. This leads to more adapted financial products.

- *From a commercial perspective*. AI technologies can provide excellent tools (banking assistant, complex simulation, robot-advisor) to facilitate the customer or advisor's **understanding of financial products and services** that sometimes appear too rich or too complex.

- *From a regulatory perspective*. AI is likely to improve the quality of **money laundering detection** processes, which is a crucial challenge for the safety and stability of the financial system.

- *From a risk management perspective*. AI allows **better risk management** by providing a rich toolkit to better control risks by helping to support decision-making.

- *From a financial perspective*. Finally, AI makes possible significant **economies of scale** through automation of certain repetitive tasks and the possibility to improve the organisation of processes…

2.1.2. Client relationship and service improvement

Artificial intelligence can also transform the modalities of client relationship, especially in an environment of increasing customer autonomy. Chatbot, Voicebot and Message Analysers applications are the most commonly seen artificial intelligence applications. These tools are designed for customers but also for collaborators. They can be used to describe customer sentiment, to measure the urgency of demand and in some cases to analyse its content. More generally, AI is used to address repetitive questions or to perform a first sorting in order to facilitate the work of the analyst or advisor. Such applications could evolve to lead to customer understanding tools throughout its relationship with the institution.

Payment services

[9] According to the ACPR's study on the financial sector digitisation in France, up to 30% of the projects in financial institutions are designed mainly around the use of AI. More than half of developing projects use AI.
[10] VILLANI Cedric, *Donner un sens à l'intelligence artificielle*.

In the payment area, the main application seems to be **real-time data analysis** to detect fraudulent transactions. Current projects are between stage of development and stage of industrialisation. Other industry participants have discussed more advanced applications for **the evaluation of attrition rate** of the number of customers through their buying journey.

In insurance

In **risk prevention**: the installation of connected objects, for example in cars or homes, allows to contact customers in case of risk and to prevent damage. Using AI allows for ahead of time or at least early enough detection of these risks using parameters related to the environment of connected objects.

Optimising the search for beneficiaries to meet obligations in the case of unclaimed contracts. In some insurance companies, these applications would already be in the industrialisation phase.

Automation of part of claim management: This includes applications for automated photo analysis or complete documentary search. In China, it is now possible to send pictures of accidents simply through Alibaba's application and receive a refund very quickly thanks to *deep learning* technologies in image recognition tasks. It is generally accepted in the world of insurance that such processes, as well as all things related to damage evaluation and traditionally carried out by the expert, will be partly achieved through artificial intelligence tools within 3 to 5 years.

2.1.3. Pricing, product customisation and underwriting risk control

Granting credit

The use of artificial intelligence in credit activities seems to relate mainly to the optimisation of **scoring systems**, starting with consumer credit where customers are more sensitive to fluidity and speed of execution. By leveraging customer information, *scoring* complements the traditional approach, which uses limited financial data, by using a *Big Data* approach using non-financial data. The canonical example is the credit score that determines the amount and conditions for a borrower; a regression problem particularly adapted to machine learning. The focus of this approach is on the use of external data (e.g. data of utilities, large stores or data related to their customers' behaviour) to banking data, traditionally used for the calculation of credit scoring. This approach makes the scoring more precise and complete in the sense that it would be possible to compute it even when the individual's banking history is weak or non-existent, using non-banking data. Some institutions already claim to use AI tools to perform the scoring, while others indicate that they have completed the development phase but are working on greater clarity and “explainability” of the method to ensure regulatory compliance.

Insurance underwriting

While data have always been critical for insurance activities, artificial intelligence further strengthens their value to actuaries. Several AI solutions are likely to improve insurance offerings, especially with regard to **customer segmentation**. AI would be used to better assess the risks of customer profiles and to optimise pricing systems. Some state that they have purchased external modules, others rely on internal development.

There are also some applications that are still in development:

- Automatic qualification of the compliance of beneficiary clauses in life insurance, which is used thanks to Named Entities Recognition algorithms.

- **Life-events scores**: application by some groups that seek to develop a dynamic personalised score of the policyholder throughout the duration of the contract.

- Services such as **parametric insurance products,** for instance pricing based on car driving profile and weather conditions**,** the latter are the parameters of these contracts**.**

Fraud prevention, anti-money laundering and counter-terrorist financing (AML-CFT)

For the banking and insurance sectors, **the identification of documentary fraud and the fight against money laundering and terrorist financing** are areas of recurring use of artificial intelligence. AI techniques are used in particular for the recognition, analysis and validation of the provided documents. The algorithms developed in this field are generally both mature and already integrated into many control processes.

In the area of payments, **detecting fraudulent transactions** is also a significant scope of real-time data analysis allowed by AI. Improving these techniques could eventually lead to other uses, with more commercial objectives, based on a better understanding of customer consumption habits. However, the valorisation of payment data, if not beyond the reflections of the established players, is still in an early stage[11].

In insurance

- **The fight against underwriting fraud**: the objective is to terminate fraudulent contracts during the interim warranty period using Gradient Boosting algorithms and data from unrelated sources (both contractual and web-based).

- **Detection of fraud in the management of claims**: most insurers seem to use technological providers to develop solutions to prevent documentary fraud and fraud networks. These applications seem rather mature.

2.1.4. Cyber risk management

Financial players, especially banks, increasingly use artificial intelligence to guard against cyber-attacks. Security data are very difficult for a human to understand: these are mainly logs of connections and activities generated automatically by the IT infrastructure. Therefore, the data are primarily semi-structured (text format) but can be processed efficiently with smart algorithms. These tools have the advantage of adapting themselves in real time without requiring any update by the software company. The usage of AI against cyber threats can be classified into three categories:

AI can be used pre-emptively before the attack:

- Through the detection of vulnerabilities using autonomous scan tools.

- Through the correction of these vulnerabilities either through a temporary patch or through the application of a durable solution.

- By accompanying developers in writing the code by helping them, through the analysis of known patterns of past attacks, to write a secure code.

[11]However, some interviews outside the *Task Force* show that many Fintechs projects revolve around the valuation of transaction data.

AI can be used to detect cyber-attacks:

- The error detection algorithms are often used to detect internet attacks (especially on the websites of financial players), security failures or bugs, or viruses before they spill over into internal IT networks.
- In particular used to identify attacks on payment transactions, AI makes it possible to complement traditional detection techniques through tools more adapted to computer attacks, especially in behaviour analysis.

AI may also contribute to incident management and analysis:

- Some AI tools are experimented in order to better identify the origin of cyber-attacks, in particular the profiles of cyber criminals.
- Finally, AI allows to refine the databases that identify known incidents and thus contribute to the rating of corporate security[12].

2.1.5. Artificial intelligence and compliance

Artificial intelligence could improve the performance of risk management and compliance[13] by automating processes. To do so, most financial institutions prefer to innovate internally rather than using outsourced solutions, especially for governance, data, intellectual property and legal responsibility.

Among the applications mentioned are the *Know Your Customer* processes (KYC). However, the final analysis is always performed by an expert. Still in the fight against money laundering and terrorist financing, tests are under way to assist compliance departments in reporting suspicious transactions, including detecting low signals in registered transactions.

When performing its supervisory tasks, ACPR has observed that automatic learning methods are used in some **internal models** to address the inability of traditional actuarial methods to handle large amounts of data in numerous dimensions. Attention shall be paid to the **validation framework** to ensure the quality of the results obtained, while providing for **add-on** mechanisms to take into account the possible error introduced if it were material.

In addition, decision trees are used to model **future management decisions** taken into account in the calculation of the ***life best estimate,*** taking into account many exogenous factors (economic environment) or endogenous (accountant: e.g. available wealth). The focus is on ***backtesting*** *in sample* (compared with past decisions) of the AI so used and the likely and prudent behaviour in extreme scenarios (*backtesting out of sample*). In view of the risk of over-parameterization, the authority recommends that simple and robust algorithms be

[12]It can be added that, in a way, AI helps to fill cyber security inequalities. Many SMEs point to many difficulties in achieving the desired level of security; the gap with major industry players, who often benefit from the expertise of the large technological players, is substantial. AI tools help to limit the workforce and funds used for cyber security as solutions provided by *the cloud* very often incorporate performing security systems based on this technology.

[13]The application of new technologies (including AI) in this area of risk management and compliance is commonly referred to as “Regtech”.

preferred to enable them to be understood by the AMSB[14] that is responsible for validating them.

2.1.6. Investment services, asset management and financial market activities

A report by the Financial Stability Board showed the prospects opened by AI for financial markets, by improving risk analysis and management and reducing price differentials more quickly[15]. To stick to the work of the *Task Force*, the main identified applications of the AI are:

- **Detection of anomalies in market operations**, both against external fraud, insider trading and "*fat fingers"*.
- **Market risk monitoring:** machine learning algorithms are tested to anticipate the realisation of market risks (intrinsic or linked to the actions of the institution), some of these methods are about to be put into production.
- **The recommendation of investment strategies for customers:** this application seems to have already been put into production in some institutions. The algorithms offer the cheapest solutions for the buyer/seller and have the least impact on the market. This leads to strategies around random sequencing of buy/sell orders, a modern approach to *Time Weighted Average Price*.
- **The assessment of risk profiles** for portfolio management to better capture customers' appetite for different investment and savings products. Similarly, some insurers have put in place tools to detect the possible appetite of their policyholders for certain insurance products or investment media: some of these tools have recently entered into production.
- **Portfolio management for third party** (**asset management, management mandate) in** which AI does not appear to be in production according to the answers; however, AI algorithms are tested by some institutions to assist in this task.

[14] *Administrative Management or Supervisory Body*, introduced in Article 40 of Solvency II, this concept refers to the ultimate management or control body responsible for the implementation of Solvency II within the entity or group.

[15] *Artificial intelligence and machine learning in financial services*, FSB, November 2017

2.2. Risks

2.2.1. Data processing: risks associated with artificial intelligence

The performance of artificial intelligence is largely dependent on data quality and lack of bias in processing. The existence of bias in the results of artificial intelligence algorithms may jeopardize both those firms that use them and their customers, as consumers or citizens, due to the risks of discrimination or inadequate advice.

Data quality is naturally a prerequisite for the effectiveness of smart algorithms. It shall involve checking the quality of the sources used, the relevance of the data with regard to the objectives pursued and their completeness: in particular, it should be ensured that the data are representative of the target population so that they do not lead to exclusion phenomena.

Biases may exist both in the data collected and in the manner in which they are processed.

- They may be present directly in the variables used, for example, with variables considered discriminatory such as gender;

- They can be implicit: these biases are harder to identify because discrimination results from the interaction of several variables that are not in themselves discriminatory. They require an analysis of the results by a business expert and, as regards the risk of discrimination, a comparison with a result which would be obtained from discriminatory variables.

Biases can be reinforced by algorithm and lead to unfair treatments. For example, information such as the department can discriminate against people in a poor department to obtain a loan, which may reinforce existing inequality. Similarly, models based on behaviour history are less performing for younger customers with a limited history, in which case other explanatory variables need to be found. Some effects could be a significant issue for financial inclusion.

In the very functioning of the algorithms, other undesirable effects may arise. This is the case for the “filter bubble” effect, i.e. to consistently offer the same products to similar profiles, preventing a company from offering unusual offers to an individual. This is often the case in content suggestion algorithms, when standard profiles dominate the supply by leaving no space for new products. We refer to *filter bubbles* when suggestions sent to a user are the result of a customisation process whose mechanisms cannot be understood.

The identification and removal of biases is ultimately based on the rigor of data scientists who are not always trained to take these risks into account. For this reason, some financial institutions have specific training courses in place to raise awareness among their data scientists.

2.2.2. Artificial intelligence increases cyber security issues

As regards cyber security, the development of artificial intelligence does not open up new breaches, but could exacerbate pre-existing ones. The diagnosis can be summarised as follows:

AI increases possible attack points:

- Using artificial intelligence automates repetitive tasks and increases the volume of IT interconnections. This automation thus increases the number of potential breaches that can be exploited by cyber criminals.

- The increasingly systematic use of the *Cloud* for AI is multiplying possible points of entry for a cybercriminal, although technology providers ensure a very high level of security. For example, the deployment of SaaS (*Software as a Service*) solutions involves regular interactions between the financial player and the service provider, which can lead to new vulnerabilities exploitable by cybercriminals.

New attacks are designed to alter the functioning of artificial intelligence algorithms:

- One of the most frequent attacks uses *"flooding"* techniques, which seek to skew the results of the AI algorithm through the introduction of falsified data into models.

- Other targeted attacks can arise, such as *adversarial* attacks, which, by a small alteration of an image, lead to error shape recognition algorithm[16].

In particular, AI could increase the dangerousness of cybercriminals:

- Using AI could make cybercrime more accessible and cheaper: using AI to automate the tasks needed for a cyber-attack will alter the existing compromise between the size and effectiveness of attacks.

- Using machine learning could help to «crack» passwords from previous passwords archives.

- Finally, cyber-attacks could be customised, making them more effective (personalised phishing, using chatbots or voice mimic technologies to extract confidential information).

2.2.3. The risk of players' dependency and the change of power relationships in the market

Controlling artificial intelligence techniques by large IT companies mainly non-European (providers of IT solutions or services, such as *cloud services*, consultancy companies…) could lead to excessive market concentration in the hands of a few players, with the following potential drawbacks:

- Artificially high prices;

- Limited access to certain services that would use AI;

- Unbalanced trade relationships;

- Sovereignty issues related to monitoring platforms, technologies and data (example: cloud service providers, AI solution providers…);

- Poor control by end users and increased opacity of the algorithms (black box);

- Difficulties in accessing and auditing the financial activities.

The most important risk is arguably that the increasing sophistication of AI algorithms does not allow their reproduction, or even merely their explanation, by other players. Thus, a

[16] *Shotgun shell: Google's AI thinks this turtle is a rifle,* The Guardian

delay in this area could induce French financial institutions to adopt foreign solutions and to fuel a vicious cycle leaving the development monopoly of the AI to non-European firms.

2.2.4. Challenges to financial stability and sovereignty

Financial stability

The issue of financial stability was raised at the beginning of the 21st century with the arrival of high frequency *trading* algorithms. It knows a renewal with the arrival of machine learning algorithms since it is difficult to predict the future behaviour of these algorithms. In particular, three risk factors could be exacerbated by the use of AI:

- **Technology directional trading**, the source of "sheep-like behaviour". By coding the algorithms with similar variables, high frequency trading programmes tend to converge towards the same strategy. The resulting risk is to increase the pro-cyclicality and market volatility through simultaneous purchases and sales of large quantities.

- **Market vulnerability to attacks**, partly due to sheep-like behaviour. It is easier for a cyber-criminal to influence agents acting in the same way rather than autonomous agents with distinct behaviour.

- **Training on historical data**: many algorithms were trained in normal situations, not in times of crisis. There is therefore a risk that machine learning will exacerbate financial market crises in the absence of training during crises.

These risks are not the only ones. Misuse of AI can also lead to systemic risks in other financial activities. For example, it can lead to increased credit risks if the algorithm evaluates them badly, thereby weakening the bond market or banking players.

On sovereignty

Inequalities in technological expertise have already been mentioned: they could lead to significant asymmetries across countries. The risk of data leakage to US providers is one example. The US government promulgated the *Cloud Act* on 23 March 2018, providing it with the opportunity to access the data hosted on servers of Cloud US suppliers. This legislation seems to be in direct conflict with the principles of the GDPR, in particular Article 48 on "Transfers or disclosures not authorised by Union law" which provides that "*Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement…*"[17].

[17] Text of the GDPR, also available on the CNIL website.

3. The development of artificial intelligence: what are the challenges for supervisors?

3.1. Governance and "explainability" of the algorithms

Artificial intelligence aims to automate a number of actions or decisions taken so far by humans or to customise previously standardised decisions. By changing the conditions for making decisions, developments in artificial intelligence may also challenge traditional methods of framing *a priori*, tracing and controlling (internally and externally) such decisions.

Depending on the use cases of artificial intelligence, regulatory issues differ significantly.

For example, using a *"chatbot*" to support customer complaints must, in a fairly simple way and for customer protection, comply with general complaints management rules that are broadly similar in different financial sectors[18].

In a quite different area, the use of artificial intelligence for the allocation of assets or internal modelling of capital requirements may question the governance and risk management rules of the company concerned: in the second case, in particular, a dynamic change in some parameters of the model by a self-learning algorithm, such as the probability parameters of default for credit risk models, could undermine the model change policies and the validation rules of these models by the supervisors.

Finally, the examples, already mentioned in the report, of the possibilities of artificial intelligence in the selection and pricing of risks - both in banking and in insurance - are of particular interest since they have to take into account the principles of several regulations:

- The need to control the risks accepted by the company;
- A duty of loyalty to customers - or, according to regulations, to take account of their interests;
- General obligations related to automated processing of personal data and transparency on decisions taken by such treatments;
- Where relevant, the integration of objectives for combating money laundering and terrorist financing.

In this context, three main issues can be identified.

3.1.1. Defining appropriate governance of algorithms

The principles of governance and internal control of different sectoral regulations are of course applicable and, generally, their objectives (i.e. risk management, client protection, AML-CFT) have no reason to be challenged.

However, their effective recognition in the design of smart algorithms should require particular attention from supervised entities and supervisors.

[18] In 2016 the ACPR published recommendations in this field as an annex on digital interfaces to the Recommendation on the duty to advise in life insurance that dates back to 2013.

As regards the protection of personal data, the GDPR clarified the principle of *"privacy by design*" - which highlights the need to integrate the purposes of the regulation from the first steps in the design of the data processing tool[19].

In the financial sector, it is clear that the *"privacy by design*" principle is not sufficient to deal with all regulatory issues. However, the same idea may usefully be transposed to apply to the purposes of other applicable regulations, with the focus being to accurately identify and take into account each of the objectives set by internal policy in accordance with these regulations (prudential, customer protection, AML-CFT).

In addition, in some cases the use of artificial intelligence may challenge, in practice, commonly accepted conventions: reference has been made to the case of model changes policy; as regards customer protection, the theoretical distinction between "product governance" and the duty to advise or provide personalised explanations can also be mentioned.

These considerations tend to confirm the need, expressed by some players in the work of the *task force,* on a code of conduct and even ethics adapted to the banking and insurance sector and setting out practical examples. The main objection raised by other participants is that the enactment of such a code would be premature because of low collective maturity for the use of artificial intelligence.

Indeed, there may be a risk of setting standards too early that would hinder the development of certain uses of artificial intelligence in the financial sector. Conversely, however, it is important that the development of uses of artificial intelligence is accompanied by practical reflection on the appropriate forms of their governance, with respect to "technologically neutral" regulatory objectives.

3.1.2. Ensuring the reliability of algorithms and achieving their objectives

Once the compatibility and compliance of the algorithms of artificial intelligence algorithms with principles of governance provided by regulations have been ensured, the second question that arises, both for firms and their supervisor, is their reliability.

This reliability first comes from data quality. This requirement, which is already provided for in many sectoral regulations[20], is of particular significance for artificial intelligence, the use of which relies on the exploitation of a large volume of data from very diverse sources. Some precautions appear to be of current use: minimising on the use of public external data (almost no use currently of social media data among respondents), using external data from sources considered reliable (e.g. INSEE), regular data quality checking, regular update of personal data with customers themselves.

The reliability of the algorithms is then based on the verification that data use is appropriate for the purposes set out and does not result in unintended biases. Several approaches are envisaged by financial actors in this respect:

[19]The prospect of the entry into force of the GDPR in May 2018 led to significant work by financial actors, including some market work. Examples include the NPA 5 practice standard issued in November 2017 by the Institute of Actuaries.

[20]For example, we can note, in banking prudential regulation, the requirements for completeness and quality of risk data and risk notification of BCBS 239 standards.

- Use of experts to validate the relevance of the variables used, eliminate those that are unnecessary[21] or source of potential biases;

- Use of safer and more traditional parallel process on part of the test data;

- Use of a standard dataset on the algorithms to regularly monitor both the relevance and non-discriminatory aspect of the algorithms;

- Develop tools that would assess conceptual drift to control this specific risk of automatic learning.

Finally, we need to think about the conditions for monitoring these algorithms - by internal control or by the supervisor. Two complementary aspects can be identified.

Explainability of algorithm

This is necessary to connect the underlying techniques and statistics to the objectives set *ex ante* (in the internal policy framework for AI algorithms).

Furthermore, the particular case of certain customer protection rules, where the obligation to explain is also derived from the rules governing the service provided, shall be noted. This is the case with the advice or personalised recommendation in insurance or the assessment of the creditworthiness of the borrower: the professional is required to demonstrate that the due diligence or service is relevant with regard to the information the customer provided on his/her needs and financial situation. As appropriate, all or part of this demonstration must be displayed to the customer to clarify the proposal made to him/her: this is the reformulation of client requirements and needs and the motivation of the advice provided.

The professional should therefore be able to explain:

- Generally, the mechanisms and criteria followed by the algorithm during its analysis process;

- For a given action (a decision taken, an advice provided) the objective criteria and discriminant elements that conducted the algorithm, in the case examined, to effect one action or propose a solution rather than another.

Testing results obtained

In addition to the work on explaining the algorithms, a number of tests (on datasets independent from those used for algorithm learning) could be considered to assess the quality of the results. However, the methodology for such tests remains to be defined: in particular for learning algorithms (and depending on regulatory stakes), the question arises from version historisation - in order to be able to assess the actual performance of an algorithm on a given date.

Algorithms and human intervention

As a precaution, some players consider maintaining a human intervention to check the consistency of the results of the algorithm. This is particularly the case in the sensitive areas of information and advice provided to clients or AML-CFT. This practical precaution,

[21] In the case of personal data, two factors may limit the use of too many data: obligations arising from the GDRP but also the need not to unduly restrain the customer path.

which is very understandable at a time when artificial intelligence techniques are at their beginnings, should not, however, lead to underestimation of the importance of work to improve the "explainability" of algorithms and the methodologies for testing their results. In particular, the following considerations should be recalled:

- A human intervener is more responsible for contradicting the outcome of an algorithm than to validate it[22];
- If a human is likely to identify manifest errors in the assessment of the algorithm (which can help the learning process), he is less prepared to identify other forms of bias, less visible but which can cause problems;
- His/her own perception of the situation can lead it to find evidence of the outcome of the algorithm totally disconnected from the actual underlying of the proposed decision: this raises clear issues of transparency towards customers in advisory or information matters, but also a more general governance problem by delaying the detection of possible structural weaknesses of the algorithms used.

3.1.3. The specific case of using algorithms in internal control and conformity

Artificial intelligence has strong developmental potential in the areas of internal control and compliance. In this area, uses and regulations should evolve in concert.

In fact, the current texts[23], if they do not exclude the use of artificial intelligence in the internal control framework, were written in the view that controls were carried out by humans:

- Permanent internal control by persons engaged in operational activities on the one hand and by persons dedicated to the sole operational control function on the other hand;
- Periodic internal control carried out by dedicated persons, independently of the persons, entities and services they control.

However, it seems difficult, in view of the generalisation of artificial intelligence, to exclude as a matter of principle from the scope of its implementation, the internal control activities, some of which may be performed more effectively and on a larger scale by algorithms. Moreover, the growing replacement of human decisions by automated processes, "smart" or not, calls in any event for a review of risks and controls mapping.

The introduction of artificial intelligence, in the operational processes or in the controls themselves, calls therefore for specific thinking about what controls should be left to humans and how. In this respect, while some forms of operational control have to disappear, new forms of control may also be identified, for example in "supervised learning" models. Finally, the interaction between men and algorithms, as discussed above, needs to be taken into account in the design of the various levels of permanent supervision.

3.2. Challenges related to possible market restructuring

[22] The responsibility of the human who is mistaken "like the algorithm" may seem mitigated while that of the human who is mistaken against the opinion of the algorithm may seem aggravated, especially in the eyes of those who will control it.

[23] Order of 3 November 2014 on internal control

As mentioned in Part one, the development of artificial intelligence takes place amid a context of profound change in IT infrastructure; and it contributes to this mutation.

The supervisor's analysis would therefore be incomplete if it did not take into account the changes that could result in the nature or size of financial institutions, their interactions with technology providers and the possible displacement of risks between different actors.

3.2.1. Possible concentration or fragmentation phenomena

Since quantity and quality of data are a key factor in the development of artificial intelligence, players who already hold useful data in quantity have a clear advantage. As highlighted by the first parts of this report, this advantage is particularly pronounced for the *cloud* players who provide artificial intelligence services, since they are likely to drain more data to further improve the performance of their algorithms. The oligopolistic position of these major players, already clearly affirmed, could be reinforced by the development of artificial intelligence. Indeed, many respondents consider using artificial intelligence "as a service".

As a result, the issues already identified by the authorities[24] about cloud computing could also be found, *mutatis mutandis,* in processes relying on AI services provided by a few major technology providers. In particular, the reversal of the traditional power relationship between the financial institution and subcontractor and, perhaps even more, the gap in technological skills that may grow between these two parties, questions the effectiveness of the rules which today govern the outsourcing of "essential services [25]".

An opposite phenomenon of re-intermediation may also arise concurrently with this phenomenon of technological concentration[26] : the multiplication of niche players - specialised in a customer or a service. This phenomenon, which is already visible in the payments industry due to other technological changes, can be reinforced, at least initially, by the rapidity of Fintech players to identify and implement new or more efficient services made possible by artificial intelligence.

Such a reorganisation of the market, if it were to occur, would pose more fundamental questions to supervisors:

[24] Recommendations on outsourcing to cloud service providers. We can note that the EBA suggests that the collective audit of a major player in cloud computing is a possibility, first signal of an adaptation of supervisors to phenomena of new pooling made necessary by technological mutations.

[25] The list of core services in which AI could apply is long. Based on the responses received, the following may include:

- The calculation of risk tolerance and loss aversion scales;
- Identification of individual savings models;
- Asset allocation;
- pricing optimisation;
- Active management;
- Financial analysis;
- the management of insurance claims;
- Combating fraud;
- Combating money laundering and terrorist financing.
- …

[26] This concentration and simultaneous emergence scenario for niche players was described, in a more holistic approach, in a report by the World Economic Forum: *The new physics of financial services*- August 2018 (page 39)

- In terms of individual supervision of entities: the heterogeneity of the population to be controlled, both in terms of size and activity, would call for the revision of supervisory methods and to take greater account of the risks of dependency among stakeholders. It would also question the current approach of regulation which tends to link proportionality of applicable rules and licensing categories - the multiplication of licensing categories to reflect the diversification of business models entails the risk of a loss of regulatory clarity and regulatory arbitrage.

- In terms of assessing risks to financial stability: the shift of certain risks to a few technology providers, the creation of new, more complex networks of interdependent players could also lead to a review of current methodologies for addressing systemic risks by supervisors[27].

3.2.2. Searching for mutualisation and responsibility of institutions

Another phenomenon related to the development of new technologies, the costs of developing new skills and the positive correlation between the performance of algorithms and the availability of data that the AI induced is the search by market participants for possible new mutualisations.

An example of possible mutualisation, given by participants in the *Task Force*, is on AML-CFT. In fact, the unequal development of artificial intelligence techniques in this area could result not in reducing the risks of money laundering but shifting them to the least performing players. Some respondents suggest therefore that reflections on algorithms aimed at preventing the risk of laundering or financing of terrorism should be mutualised, with appropriate governance to take into account the mutualised characteristics of algorithms for:

- their update and control (incidents, data, false positives);

- the prevention of disclosure of operating rules in order to preserve efficiency.

Such an example shows the benefits that can be withdrawn from certain mutualisations. In terms of supervisory practices, it probably calls for a more refined articulation between, on the one hand, standardisation and mutualisation of processes for the common good and, on the other hand, rules that make each player individually responsible for their risk management choices.

3.3. Challenges faced by supervisors

As suggested previously, supervisors should consider the steps to be taken in order to:

- In the short term, accompany the market to ensure its appropriation of artificial intelligence techniques under conditions that ensure compliance with regulatory objectives and allow supervision by the supervisor;

- In the medium term, anticipate market changes (concentration, fragmentation, outsourcing, mutualisation) to adapt regulations and supervisory methods to these new realities;

[27] Big Data meets artificial intelligence, July 2018, *BaFin*

- It seems natural to add a third goal to these two objectives: leveraging artificial intelligence techniques for their own missions ("suptech[28]")

To do so, authorities may consider several lines of action:

- First, like the financial institutions, increasing their expertise in data analysis and the use of artificial intelligence[29].

- Creating mechanisms for enhanced cooperation between supervisors at the national and international levels. In this respect, in the area of artificial intelligence, the interlinkage of the protection of personal data issues and regulatory issues in the financial sector may require closer cooperation between the ACPR and the CNIL - both for ensuring consistency of doctrines and looking for synergies in the skills to be acquired and the controls to be implemented.

- Supporting standardisation and normalisation initiatives [30] and more generally methodological work aimed at improving the auditability and "explainability" of "smart" algorithms.

[28]Suptech is a contraction of the term "Supervisory technology" and refers to the use of new technologies serving supervisory tasks.
[29]Examples are the Staff Recruitment and Training Program, which focuses on data analysis, implemented by the Monetary Authority of Singapore.
[30]Examples include ISO/IEC AWI 23053 [30]standards, attempted standardisation of AI.

4. Annexes

Annex I: History

The term AI first appeared at Dartmouth College in 1956, during a summer session attended by the future tenors of discipline[31]. According to the then organizers, their aim was "to proceed as if any aspect of learning or any other characteristic of intelligence could be described in a sufficiently precise manner to be simulated by a machine".

The modern concept of AI emerged in the 1950s, in particular thanks to Alan Turing[32]: artificial intelligence mimics how humans think but with their own capabilities. AI is studied in relation to human intelligence, taken from modern research. Using the words of Alan Turing, the AI study should not be motivated by the question: can the machines think? But rather by the question: "Can digital computers take the place of a human being in the imitation game?" The imitation game is a man or woman facing a human interlocutor following a series of questions. Finally, it is worth noting that we moved from the machine to the digital computer, a choice made by Alan Turing and justified by the enthusiasm given by this new technology at his time.

This logicist approach distinguishes itself from the neural approach of imitating brain biological processes. This neural approach is more popular today because it has proved successful in demonstrating its performance in different use cases[33]. The neural approach was originally pushed by Frank Rosenblatt at Cornell University, which in 1957 was the designer of the perceptron, a single-layer and single-output network. In a nutshell, the perceptron represents one neuron that applies the simplest function (linear). The model itself inspired ideas developed by the physiologist Donald Hebb, who sets out in 1949 "the Hebb rule" of changing the value of the synaptic coefficients, which define how electric signals pass through the synapses between neurons, depending on the activity of the connected neurons. The research mentioned is now considered precursor to neural networks[34], a branch of machine learning, which is itself a subcategory of artificial intelligence.

[31] J. McCarthy (Dartmouth), Minsky (Princeton), C. Shannon (Bell Labs/MIT), N. Rochester (IBM), T. More (Princeton), A. Newell (Carnegie Tech), H. Simon (Carnegie Tech), R. Solomonoff (MIT), O. Selfridge (MIT).
[32] COMPUTING MACHINERY AND INTELLIGENCE, 1950, Alan Turing
[33] Example of IA's prowess: Victory of Alphago on the human champions in Go.
[34] *Une petite histoire du Machine Learning*, Octobre 2015, *Quantmetry*, Héloïse Nonne

Annex II: Thematic glossary

Brief typology of artificial intelligence techniques

- *Artificial intelligence (AI):* techniques and applications to create a machine capable of imitating human intelligence autonomously. As part of the report, we restrict ourselves to those that have a minimum capacity for automatic learning.

- *Machine learning:* set of algorithms to solve problems and whose performance improves with experience and data without ex post human intervention35. Deep learning is a subcategory of machine learning. Machine learning is used in particular for marketing, fraud detection, portfolio management and risk assessment purposes (e.g. scoring of risk).

- *Natural Language Processing (NLP):* allows to analyse unstructured textual data. Combined with sounds processing techniques, these tools also enable to analyse voice data.

- *Biometrics:* Identification techniques based on biological characteristics such as fingerprints, facial traits… or behavioural features such as voice recognition, signature, gait… Scientific research areas related to artificial intelligence techniques.

- *Neuroscience:* scientific study of the nervous system, both in terms of structure and functioning, from the molecular scale to the level of organs, such as the brain or even the whole body. This discipline is closely linked to AI since it helps to better understand how humans act, that is, what AI specifically seeks to replicate in machines.

- *Representation of knowledge and modelling of reasoning:* allows to check whether the proposed algorithms fulfil the objective pursued.

- *Decision and management of uncertainty:* tools to analyse data with uncertain value.

- *Constraints satisfaction and logical formula satisfiability:* more fundamental research on logic.

- *Planning and heuristic search:* research on planner's construction that allows for the production of customised plans typically used by a robot or any other agent to perform a task. The planner defines possible inflows, outflows and actions and heuristically seeks the best sequence of actions.

- *Autonomous agents and multi-agent systems:* can be useful to simulate the markets

- *AI and Web:* semantic web, particularly important in the field of connected objects (internet of things).

AI jobs

Data governance

- *Chief Data Officer:* is responsible for facilitating access to data for different business areas and identifying among all available data that is most relevant to support project development and decision-making.

[35]The literature also includes definitions that include the notions of knowledge and learning. A work inspired many of them: Russel & Norvig (*Artificial Intelligence: A Modern Approach*, 2003, Russell & Norvig

- *Data Privacy Officer:* is responsible for ensuring compliance with the rules for the protection of personal data by the firm.
- *Chief Data Quality Officer:* is responsible for ensuring the quality of the data used by the firm.

Artificial intelligence the jobs

- *Data scientist:* expert who develop machine learning algorithms.
- *Data analyst:* expert who creates the databases or of data lakes needed by the firm and then ensures their proper functioning. Data analysts manage the administration and architecture of the bases and also support data modelling.
- *Data engineer:* engineer who prepares data used by machine learning algorithms by producing new variables from the existing variables and by participating in data storage and processing policy.
- *Ontologist:* expert who identifies, creates and manipulates knowledge graphs.
- *Expert in automated processing of natural language:* expert with both language and data science skills.
- *Expert in computer vision:* data scientist specialised in image and video processing.
- *Expert in human-machine interaction:* expert who designs systems and interfaces that facilitate the use of artificial intelligence tools by humans.

Annex III: Questionnaire

Description of artificial intelligence development in the financial sector (Part 1 and 2 of the discussion paper)

1. Do you have any comments on the paper's definition of artificial intelligence? (Part 1.1.1)
2. Do you identify other contributing factors to AI development in the financial sector than those listed in the paper (Parts 1.1.2 and 1.2)? Conversely, do you identify possible obstacles to this development?
3. Do you have any comments on the considerations of the paper on the use of cloud (Parts 1.2.3, 2.2.3 and 2.2.4)?
4. Do you have any comments or additions to the list of uses identified in Part 2.1 of the report? Where appropriate, you can quickly describe concrete projects, specifying their progress level (note that individual information will remain strictly confidential).
5. Do you share the analysis of the risk of algorithm bias in Part 2.2.1? Which complements would you bring?
6. Same question for cyber security risk analysis (Part 2.2.2)

Issues for supervisors (Part 3 of the discussion paper)

7. Do you think there are business models using AI that cannot grow because of financial sector regulations? If so, can you clarify the relevant regulatory provisions?
8. Beyond the requirements of the GDPR, are you aware of "governance of algorithms" processes that would be developed in line with the general governance requirements for the financial sector? If so, for which activity? (Part 3.1.1)
9. What would be the most useful definition of "explainability" of algorithms for the implementation of governance and control of algorithms in the financial sector? (Part 3.1.2) Do you know practical methods already operational to ensure this "explainability"?
10. According to you, what are the most promising methods for ensuring the reliability of algorithms? (Part 3.1.2)
11. Have you taken into consideration the specificities of the interactions between human and intelligent algorithms in defining operational or control processes? (Part 3.1.2)
12. What specific internal control measures do you consider necessary for AI? (depending on the area in which AI is used, customer sale, pricing, management, AML-CFT, internal models for the calculation of regulatory requirements, etc.)
13. Do you think it possible in the financial sector to entrust "level 1", "level 2" or even "level 3" controls - to smart algorithms?
14. Do you think it useful to clarify or illustrate some regulatory principles due to the emergence of artificial intelligence technologies? If so, which ones?

15. Do you have comments on possible market developments described in Parts 3.2.1 and 3.2.2?

16. Do you believe that the phenomena of mutualisation of technological resources should be better recognised, or even encouraged by supervisors? If so, in which areas? How?

17. What approaches should be preferred by the supervisor to support the development of AI in the financial sector and to address the issues discussed in Part 3?

18. Do you have any comments on the lines of action mentioned in Part 3.3 of the document?

19. What do you consider priority areas where the supervisor should provide guidance to the market on its expectations in order to reduce possible regulatory uncertainty for AI projects?

5. List of Task Force members

Institution/company	First name	Name
ACPR	Pierre	BIENVENU
	Olivier	FLICHE
	Didier	WARZEE
	Su	YANG
AFEPAM	Jérôme	TRAISNEL
AG2R	Tanguy	VINCENT
Allianz	Mathilde	GAROTIN
AMF	Alexandre	BARRAT
	Louis	CHARPENTIER
Aviva	Gilles	PAVIE-HOUDRY
AXA	Martin	DETYNIECKI
	Marie-Neige	COURIAUT
	Cécile	WENDLING
BNPP	Olivier	VANDENBILCKE
BPCE	Loïc	BRIENT
	Bibi	N'DIAYE
CNIL	Sophie	GENVRESSE
CNP Assurance	Romain	MERIDOUX
Crédit Agricole	Alexis	BINAY
	Marie	LHUISSIER
DIGIT/Banque de France	Renaud	LACROIX
	Alexis	LAMING
	Andrés	LOPEZ-VERNAZA
	Farid	OUKACI
	Imène	RAHMOUNI-ROUSSEAU
Direction Générale du Trésor	Geoffroy	CAILLOUX

	Eliott	COMBE-MAZERON
	Sébastien	RASPILLER
FBF	Frédérique	FAGES
	Béatrice	LAYAN
FFA	Jérôme	BALMES
	François	ROSIER
Générali	Sylvain	MOLLET
	David	WASSONG
Groupama	Nicolas	MARESCAUX
Groupe Crédit Mutuel	Marc	RAINTEAU
HSBC	Remi	BOURRETTE
	Julien	MIQUEL
ING	Thierry	DE LA SALLE
	Nicolas	SERRE
La Banque Postale	Fabien	MONSALLIER
Macif	Mehdi	LAHCENE
Nalo	Guillaume	Piard
Orange Bank	Djamel	MOSTEFA
Paylead	Alexis	DEUDON
	Charles	DE GASTINES
	Jérémie	GOMEZ
Société Générale	Marianne	AUVRAY-MAGNIN
	Bernard	GEORGES
Treezor + Hi Pay	Omar	SAADOUN
Younited-Credit	Romain	MAZOUE
Tracfin	-	-

The Task Force drew on the participation of many other contributors from each of the listed institutions as well as the following institutions: Deloitte, DoYouDreamUp, Dreamquark, Microsoft, Quantcube, Shine, Zelros, Strasbourg University… and some 20 other experts in the field.

6. Bibliography

- La révolution numérique dans les banques et les assurances françaises, ACPR, mars 2018. Les études sectorielles (banque et assurance) sont disponibles sur le site de l'ACPR.
- Donner un sens à l'intelligence artificielle, Cédric Villani, mars 2018.
- *Artificial intelligence and machine learning in financial services*, Financial Stability Board, November 2017.
- La norme de pratique NPA 5, Institut des actuaires, novembre 2017.
- Recommendations on outsourcing to *cloud* service providers, European Banking Authority.
- *The new physics of financial services, World Economic Forum*, August 2018.
- Big Data meets artificial intelligence, *BaFin,* July 2018.
- COMPUTING MACHINERY AND INTELLIGENCE, Alan Turing, 1950.
- *Artificial Intelligence: A Modern Approach*, Russell & Norvig, 2003.
- *Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of Artificial Intelligence and Data Analytics in Singapore's Financial Sector*, Monetary Authority of Singapore, November 2018.
- *OECD work on artificial intelligence*, OECD, October 2018.