Annex to the French Banking Federation (FBF)'s consultation response on the White Paper on Artificial Intelligence – A European Approach

General considerations

Definition and scope of AI

The concept of "Artificial Intelligence" (AI) is based on terms that can sometimes seem overused, as it is used generically to cover multiple technologies. Can we speak of "Artificial Intelligence"? Most of the time, the use of algorithms is limited to mimicking scenarios, reproducing and automating the processing of repetitive tasks that a human being could perform.

In order to identify current practices in the banking world, it is therefore important to define what is meant by AI at the present time. **It could be defined as follows: "cognitive technologies which rely on large volumes of structured or unstructured data (Big Data)".** It would perhaps be more appropriate to speak of "cognitive intelligence" defined as "any treatment/any modelling of unstructured data which emulates/replaces the cognitive capacities of man".

Data, big data, machine learning algorithms (including deep learning) constitute the first base of AI, thus providing the capacity to correlate and memorize, therefore, to learn and by extrapolation to predict.

This field is constantly evolving. This definition and the fields making up the perimeter of AI are likely to evolve. It is therefore necessary to challenge and if necessary, to adapt these elements with time and context.

So, it would be a bit restrictive to limit AI to machine learning. Many practical solutions that integrate Artificial Intelligence will also use probabilistic models such as Bayesian networks and Markov models which are not always considered to belong to machine learning. Likewise, some solutions will combine business rule systems with a machine learning component and automatic natural language processing.

It would undoubtedly be useful, in a longer term, to also **underline the probable development of more prospective systems** (reasoning machine, exploratory algorithms combined with deep learning ...) located higher on the cognition scale, and which will mark probably a new stage in the evolution of the "customer relationship" (empathetic intelligent assistants in support of customer advisers for example).

A strategic priority leveraging incremental technologies

The Artificial Intelligence is a strategic priority for the banking sector, because it makes it possible to accelerate decision-making processes, to stay in the race and not to leave the monopoly of decision-making to other Big Tech players (GAFA, BATX, etc.), and possibly to get ahead in the fintech world.

However, AI is above all based on an **incremental technological evolution**, sometimes based on old technologies, the use of which is now made possible by the access and processing capacities of existing volumes of data.

The impact of these technologies must therefore be studied with objectivity and their use must be made reliable, all within a highly regulated banking framework, and with respect of governance and ethical rules.

AI should be seen as a means, not an end in itself. Implementing AI solutions is not an answer to a simple technological appeal, to a promise of process optimization and therefore costs reduction even if the banks remain very vigilant about their operating margin and their operating coefficient.

Technology and usage must be reconciled, which implies a learning curve. At all stages of the implementation of these technologies, human interaction remains essential: both in the learning process and in the use that results from it.

Banks place customer and human relationships, quality of service, loyalty and trust at the heart of their approach. The vision for AI innovation and technological development is motivated by this approach and must therefore systematically serve it. The banks must assert their strengths, already recognised by their customers when trust and security are essential in an increasingly competitive market.

Section 1 - An ecosystem of excellence

Ethical vision of AI

In order to define what could be an ecosystem of excellence, it is essential to build **a global vision of the impacts of AI that goes beyond technical, legal and regulatory issues.** The impacts in terms of businesses, jobs and human resources in the banking sector must be thought of, in parallel with ethical, social and societal questions.

There is a need for human intervention in the decision-making process, in connection with respect for privacy, security and transparency in the use of data. This represents a real transformation of the industry which must be further supported.

Furthermore, we believe it is necessary to encourage **a pedagogy of AI**: a positive communication, based on pedagogy and training, with a contribution from public Authorities and private actors.

A harmonized research & innovation framework in Europe

Coordination and cooperation in Europe

We consider it important to feed an AI ecosystem to **promote and incentive effective sustainable medium/long term fundamental research and development activities** that meet international competitive challenges.

Consequently, we recommend:

- at the national level, **an enhanced collaboration** to develop transversal processes and/or technologies;
- at EU level, **a homogeneous framework and a level playing field** for retaining talent and counterbalancing non-European players.

Amongst transversal processes and/or technologies, we may mention the promotion of natural language processing, the creation of shared resources and datasets in languages other than English.

These national and European ecosystems favourable to AI development may rely on coordinated governance and steering structures, material infrastructures, as well as a legislative and regulatory framework without distortion of competition and a tax framework favourable to innovation.

A world-class research centre developed at the European level should have as one of its tasks to network with existing AI research excellence centres across Europe and beyond.

EU technological sovereignty

EU policy makers must keep in mind that for the time being nothing can compare to what some Big tech companies are able to offer in AI. All EU companies use as is the AI models that have been developed by Google, Facebook or Amazon. EU should be inspired by what they have successfully implemented.

As an example, it is necessary to **build up our own EU libraries of free open source codes for AI algorithms customised to EU standards**. EU lacks autonomy and sovereignty in terms of AI algorithms (open source AI codes). Currently, Europeans use American or Chinese open source AI codes via free access to libraries provided mainly by GAFAM (Google, Amazon, Facebook, Microsoft ...) or Chinese giants (Alibaba…). It is strategic to regain our independence on AI algorithms in the long term.

Partnerships with private sector

Partnership with the private sector is key to embark research and industry together in this journey as the others are doing and as is shown by the Big Techs. There is also untapped reserve of potential AI use cases within the private sector that should be opened.

The partnership with the private sector is important in order to avoid deployed solutions conflicting with the business stakes. The adoption of AI in the European industry is necessary to enable Europe to preserve its technological sovereignty while releasing the full potential of this strategic technology.

To this end, and in order to promote European competitiveness, **the European Commission should give incentives for companies adopting and promoting the uptake of A**I (in the recruitment of future talent and young graduates or in support of opensource work).

The public sector should also be encouraged to adopt AI to improve the efficiency of the administration but with respect for individual rights.

The set-up of public-private partnerships are essential to improve European industrial research. This type of partnerships will ensure consistency with real societal needs. Through this initiative, the setting up of platforms facilitating collaboration and interaction between the various players would be highly desirable (open-source work, sharing of good practices, etc.). For example, a French banking Group is strongly committed to open-source work, particularly with the sharing of its algorithm Skope-Rules on the open source platform Scikit Learn.

That king of coordination can help create reference datasets and benchmark industrial problems, develop better communication between industries and AI researchers, gather significant investments in terms of research and development, but also methodologies to industrialize and implement. **It is a first step to start reducing dependencies on large IT companies and excessive concentration of the market in the hands of a few players**. It is crucial to regain EU independence on AI algorithms in the long term.

A **tax system** that will facilitate investments made by banks in research, particularly through partnerships with schools / universities would be appreciated.

Supporting AI skills development and talent retention

Regarding the research and innovation community, it is indeed necessary to adopt a logic of efficiency in order to retain talents in Europe through remuneration and attractive projects. Concerning skills, it is important to capitalize on the very good training courses that already exist in Europe.

The development of skills represents a very important issue in the context of a shortage of engineers trained in Artificial Intelligence. Already in 2011, a McKinsey Global Institute report stated that there would be a shortage of 190,000 Data Scientists in 2018, as well as 1.5 million managers and analysts who could simply understand the issues and make decisions in the context of AI. The study by Burning Glass Technologies, BHEF and IBM, published in early 2017, predicted that the number of jobs worldwide for Data Scientists and Data Analysts will increase by 28% over the next five years to 2,720,000, and that 39% of these jobs require a master's or doctorate level qualification. Finally, a study compiled by the Tencent Research Institute in December 2017 showed that there are only 300,000 "AI researchers and practitioners" in the world today, while market demand is estimated to be in the millions.

In this context, we consider important to support the development of skills benefiting the European industry. The report on Artificial Intelligence written by mathematician and MP Cédric Villani stated that private research centres are large consumers of both high-level researchers and brilliant freshly

graduated students. Thus the brain drain of French researchers to foreign academic institutions, endemic for many years because of differences in salaries and working conditions, is added another brain drain of researchers to large companies (GAFAM and other unicorns). To that extent, on a European scale, the involvement of the private sector in training programs aimed at developing AI-related skills is a crucial issue allowing all at once students to acquire professional skills and experience and European companies to recruit young graduates.

Talent retention can be encouraged through the creation of incentives. Education is key to raise awareness, ensure transition today in current structures (public and private sector) and train talents to inspire careers for tomorrow. If EU cannot have centre of excellence that attracts talent globally, we will have a hard time competing.

Focus on Small and Medium Enterprises (SMEs)

It's important to target SMEs because they are at the origin of an important part of innovation (e.g. biotech). **In a post-Covid context, helping to raise awareness among SMEs of the potential benefits of AI can be particularly relevant, especially in the field of automation.**

SMEs are a major part of the industry and often lack the critical mass in terms of R&D or training to migrate to a data-enabled model. There is a risk that the current shift towards data introduces a comparative disadvantage for small structures.

Digital Innovation hub

Banks agree that innovation requires experimentation with new technological solutions and new business models. However, this approach should not lower regulatory standards, as both financial stability and consumer protection are paramount.

The banking profession is **not in favour of the regulatory "sandbox" according to the Anglo-Saxon model**. The principle of the "regulatory sandbox" with prior authorization does not necessarily seem appropriate to us. It seems to us more effective, if necessary, to adapt the applicable legislation and to give access to the innovation poles to all the actors concerned by a given activity, whatever their nature, their size or any other criteria. They should be based on a limited set of eligibility criteria, such as the amount, duration, number of clients and countries ...

The banking profession supports the establishment of a fair and harmonized regulatory framework for banks and new entrants. It is necessary to ensure that there is no level-playing field in favour of new entrants / TPPs.
There are many sandboxing regimes, innovation and acceleration hubs with different characteristics, especially in Europe. **In our view, competition between national supervisors based on regulatory arbitrage should be avoided at all costs.** A national approach could create unequal conditions of competition and further fragmentation among EU Member States.

The financial sector must benefit from technological improvements, so that regulation should not hamper innovation or prevent healthy competition. **Europe must therefore promote agile, proportionate and effective regulation of financial innovation.** The level of regulation and supervision must always be proportionate and supported by taking risks into account (consumer protection and AML / CFT mainly). The introduction of greater proportionality must nevertheless be treated with the greatest of care in order to correctly assess the effects both on consumer protection and on the distortion of competition. In addition, we believe that a comprehensive regulatory and supervisory framework should be provided before the introduction of new license categories for fintech-related activities.

More specifically regarding SMEs, innovation hubs should not be "specialised", but open to all types of actors, use to experiment use cases with a pre-defined purpose, a limited customer base and timeframe. It is necessary to encourage SMEs on their own mostly. In the past, there were consortium including SMEs but it was unclear if the SMEs completely benefited from it.

Section 2 - An ecosystem of trust

Potential concerns about AI

As recalled in the White Paper of the European Commission, AI can relate to a wide variety of risks. **In our perception, these risks are more often directly related to the service as such than to AI itself.**
AI is not an "autonomous" subject, but a technical object serving use cases. Even in automatic execution, there is no real autonomy. It is not true to say in general "AI may endanger safety". It may be relevant in a subset of the domains where AI is used. In addition, some risks (e.g. bias.) related to the (involuntary) partiality of human judgment were pre-existing at the adoption of AI.

Public education and behaviour facing AI
There is a need to bridge the AI awareness, information and education gap between industry and the public. Managing accurate and thoughtful communication about the aims and limitations of the technology will be critical to its adoption.
There is a risk that companies hide behind algorithms not to face the responsibility of a claim, and that victims will find it difficult to question a large-scale algorithm.
AI is not always accurate: Computers are thought to be unbiased as they execute mechanical tasks for which human trust them (scanning barcodes, etc.). AI algorithms are a different story as the outcome is heavily dependent of the data used to train with, but the public might not realise this and still trust the computer blindly.
AI makes mistakes and is not always accurate (like humans). One of the most important point is how to manage these mistakes and what is acceptable. At the end, undertakings will be responsibility for these mistakes and not the models

Furthermore, some specific processes can already contribute to the prevention and minimization of risks caused by algorithms.
According to a Deloitte study (May 2019), in terms of algorithmic risk management, several tools and algorithms have been put on the market in order to identify and control biases induced by data or

algorithms, but also to better visualize the functioning of some deep neural network algorithms. These algorithms, mainly open source and developed by a community of researchers, analyse data in the form of different classifications.
Moreover, the models are monitored over time which minimizes the risk of "abnormal behaviour".

AI usage in the financial sector
The concerns flagged by the European Commission are valid, yet not all are relevant to financial sector. **The sector being heavily regulated, risk management frameworks in place can help to ensure effective mitigation.** This framework relies on risk assessment criteria that should be defined and linked to applications and use cases, not to underlying technology.

Numerous laws already regulate the governance of algorithms. We can mention the GDPR, but also the aspects defined in the Monetary and Financial Code in France.

Some banks have set up systems to ensure the relevance of the algorithms used, which may vary depending on the projects: **cross-validation process, "out-of-sample" and "out-of-time" test in addition to back tests, user feedback…**

Other banks are working to define **a model governance approach** that incorporates Artificial Intelligence algorithms: standards (best practices) for the development of algorithms, mapping of models (business scope, geographic area, type of data used as input, nature of the result, type of learning, etc.), support for self-assessment of risks, identification of roles and responsibilities, identification of cases involving an independent review of the model, production and monitoring process.

The development and implementation of AI solutions must continue to be done within this same regulatory framework with an approach of good practices and quality control internal to each establishment.

No new AI regulatory framework needed

Application and supervision of existing principles
To guarantee efficient and secure AI development and secure in Europe, relevant EU authorities must work with the industry and the civil society **to develop guidance on how to apply existing requirements to new AI use cases and provide clarity on issues such as validation criteria.**

It should be ensured that regulators are capable (resources, training) of providing oversight and supervision of AI, particularly for EU experimentation frameworks: understand better the advantages of AI applications for companies and consumers, mitigate potential risks, and reduce uncertainty to foster innovation.

In all cases, the principle of technological neutrality has to be guaranteed, also if an adaptation – at the margin – of the current regulation is needed.

No additional regulation of AI in the banking sector

In our view a regulation could hinder the development of AI in the banking sector. AI is in a phase of appropriation and exploration by the banking sector.

In addition, the use of human expertise (data scientist, compliance and legal officer, client managers, etc.) remains essential to guarantee the quality and security of AI-related processing.

Last December, Denis Beau, Deputy Governor of the Banque de France, went in this direction, saying "It is not desirable to regulate too quickly and too precisely the use of techniques that are being perfected every day and for which there is insufficient hindsight. It seems more appropriate to accompany the market in the resolution of questions (explainability, control of deadlines...) still unanswered to date. We will open a space for dialogue to identify regulatory obstacles or irritants."

Data minimisation and AI

The applicable EU legislation already allows for risks to be addressed: AI should comply with the rules in force, in particular the GDPR (any processing of personal data through an algorithm falls within the scope of the GDPR). This has been recalled by the European Data Protection Board in an answer to MEP Sophie in 't Veld (01/2020): "Any processing of personal data through an algorithm falls within the scope of the GDPR. This means that the GDPR covers the creation of and use of most algorithms. Thanks to - inter alia - the risk-based approach, the data minimisation principle and the requirement of data protection by design and by default, the current legal framework addresses many of the potential risks and challenges associated with the processing of personal data through algorithms."

Moreover, the banking industry is already subject to legal and regulatory obligations that address the risks mentioned. As a result, banks have already developed and continue to adapt their risk models when implementing AI applications into their processes and services.

Focus on high-risk applications

We do not think that new rules are needed.

Guidance on AI issues produced collaboratively by competent authorities for different sectors could help firms apply their obligations under different regulatory regimes effectively to AI use cases.

If the Commission decides to proceed with a horizontal regulation, **we support the risk-based approach taken in the White Paper to focus on high-risk applications and high-risk usages**. We also recommend the adoption of a **principle of technological neutrality**. Legal requirements should not apply to the underlying technology but to the use which it is put.

The concept of risks should be extended to all risks that could have serious consequences, ranging from the (physical, etc.) risks mentioned in the White Paper to the risks of manipulation of opinion, risks to democracy, psychosocial risks…

We can understand the need to better manage AI (whatever the level of risk), but this can be done by appropriate governance. For all AI models, it is possible indeed to **develop internal policies and governance** within all Companies to supervise and manage risks.

Risk-based approach in the banking sector

The risk-based approach is **already very widespread in the very strict and highly supervised regulatory framework of the banking and financial sector**. Financial and insurance organizations are particularly vigilant about respecting the law and respecting customers. **Not all business sectors have the same rigor or the same ethics.**

However, these different sectors interfere in the banking market, exploit equivalent data and use similar service bricks. These sectors are not followed with the same rigor as that applied to the banking world. This results in the **creation of a harmful asymmetry between the actors and the sectors of activity yet become interdependen**t. The establishment of exchanges between the regulators of the various sectors concerned with a global approach seems to us to be an essential prerequisite for the establishment of fair rules and practices.

In any sector, any actor (GAFA, etc.) using AI and who may present **high-risks or systemic risks** (impacts on opinion, public liberties, health, etc.) must be required to act within an internal and external control framework, inspired by the best international standards. **The banking regulation relating to technology is already very comprehensive and could inspire all actors; all those who, without being banks, carry out "financial" or related activities.**

In any case, it seems not understandable that an entire sector such as finance can be considered at risk: this could wrongly establish a special status for all AI models in the same sector.

Thoughts regarding suggested mandatory requirements

More than **data quality**, it is their relevance for the task at hand. Is the training data well aligned with the intended usage?

Human oversight is essential. The ability to react and disconnect a faulty model is the most important point (more important than distinguishing high-risk AI from other models)

In addition, the **robustness and the precision of the AI systems** would be very complex to define in a possible future regulatory framework (only the quality of the work can prove that the system is robust).

EU-level guidelines/regulation for use of remote biometric identification system

The current legal framework (GDPR, CNIL, ACPR, etc.) seems sufficiently robust to grasp the main risks linked to the use of AI, especially from the consumer's point of view, and to avoid any risk of excess or slippage.

However, it seems to us necessary to launch **a debate at the EU level**. As indicated by the French data protection authority (CNIL) this complex subject calls for political choices and deserves a lucid and in-depth debate. We support the **gradual approach** proposed by Thierry BRETON, who wishes to give himself a few months to study, anticipate and segment the issue properly.

In order to contribute to the debate on **facial recognition**, in November 2019, the CNIL presented technical, legal and ethical elements that, in its view, must be taken into account in the approach to this complex issue. In this contribution, the CNIL recalled that the framework for facial recognition devices and their experimentation have been modernized both at the European (GDPR, "police-justice" directive) and national levels by providing a stricter framework than before for biometric devices with

the aim of adapting the level of data protection to the new uses of digital technology. According to these texts it is required:

- to establish the need for such devices on a case-by-case basis;
- to ensure the proportionality of the means deployed and the special protection that children must benefit from;
- to place respect for persons at the heart of the devices, for example by collecting their consent or guaranteeing them control over their data.

Voluntary labelling system

We would like to highlight that **labelling systems can be difficult to set up and are likely to complicate the development and implementation of AI systems**, which are often scalable or self-learning, or encapsulated into larger systems in the form of internal or external components that are difficult to isolate, etc.

A label, even non-mandatory or volunteer, will add new burdens of certification, additional rules and procedures. The requirement to set up internal policy and governance would have more value than a new label. It can also suggest that other AI systems without label, are dangerous or unreliable.

There is also a potential risk of "AI washing". What is it that is being labelled – a specific application or the entirety of a firm's activity?

If a scheme is created, it would have to be thought in a supportive/positive way, maybe with a few levels so people can ease into it. The framework should be more specific, simple, and follow a risk-based approach. For instance, the presence of a "shutdown button" to disconnect an AI system at any time, whatever its level of risk, may be more interesting and clearer for the user.

Another option would be to label, not products or services or specific algorithms, but the ability to set up and comply with an appropriate "algorithm governance framework" allowing, upstream and downstream, to have appropriate risk control.

Labelling only low-risk AI amounts to wanting to highlight AI systems that have the least benefit for the user. Moreover, it is not clear why high-risk AI would be excluded from any labelling.

Enforcement system for trustworthy and secure AI

Most of the banking and financial activities have already a framework that should apply for AI. That's why the FBF supports, through common horizontal rules**, a risk-based, cross-sectoral approach with an extraterritorial scope**, especially since the border between sectors is sometimes difficult to establish.

To ensure proper compliance with the rules, the FBF recommends avoiding setting up a generalist cross-sector supervisor but relying on a coordinated network of specialist supervisors by sector, ensuring that all areas are well covered.

The AI compliance with the regulatory frameworks might be based on two pillars:

- **Ex-ante conformity assessment:** ensure the AI compliance with regulatory frameworks within a governance model; guarantee the quality of training data and the compliance with the requirements of the GDPR and of the various legislative frameworks (security, etc.). Respect and application of MRM (model-risk management) procedures in compliance with ECB and FED requirements.
- **Ex-post enforcement mechanisms:** any prior conformity assessment should be without prejudice to monitoring compliance and ex post enforcement by competent national authorities for all AI applications. Control of AI applications carried out within the frame of the global control of banking activities.

Section 3 - Safety and liability implications of AI, IoT and robotics

Product safety legislation

As AI systems can evolve over time, it seems necessary at EU level to **adapt existing procedures to potential changes in order to comply with the necessary safety measures, in order to strengthen cybersecurity governance in a coordinated way**. Specifically, on cybersecurity, improving information exchange and coordination between the public and private sectors remains a challenge.

Interest in sharing resources is not necessarily specific to AI projects. Shares already exist, within the framework of the development of common infrastructures whose interest has been identified. This is the case for **issues related to money laundering and the financing of terrorism** or for **fraud** but also this is the case for other types of **operational risks**, in particular cyber risks for which data pooling would greatly increase the resilience of banking institutions and beyond.

Risk assessment procedures

From the banking sector's perspective, we are aware of the consideration to be given to the **risk assessment procedure for services, which would undergo significant changes during their lifetime**.

However, our services based on AI should not be submitted to a new horizontal legislative framework for security (as considered by the EC with the new adjustment legal frame on EU product safety and liability legislations) to cover this risk. Therefore, we have no opinion on the question raised regarding the content of the new security product and services legal framework as planned.

The banking industry is **an extremely supervised sector at European and National level**, to which is added consumers laws, banking national laws, national liability laws, civils rights, GDPR, etc. In addition, this sector is originally driven by **a permanent risk control governance** to ensure the safety of services they provide, based on AI or any other kind of technologies. In order to cover the whole potential issues raised by the EC related to AI, we **strongly support the cooperation between Authorities and the Financial/Banking sectors**, through notably the experimentation on specific AI applications under the control of competent Authorities instead of any new non relevant additional regulations.

EU legislative framework for liability (Product Liability Directive)

Referring above mentioned, **the services based on AI provided by the Financial/Banking sector should not be submitted also to a new horizontal legislative framework for liability** (as considered by the EC with the new adjustment legal frame on EU product safety and liability legislations). In this regard, we have also no opinion on this matter regarding the possible changes to the current EU legislative framework.

The banking sector is subject to multiples levels of liability regimes: linked notably to the supervision by National or European Authorities, GDPR, national civil liability laws, all specific banking liability rules as for instance the consumers protection framework, etc. The multiple current legal regimes of responsibility already cover the issues of responsibility in terms of services based on AI provided by the Financial/Banking sector. Therefore, the commission's concern about the risk of liability generated by certain services based on the AI application should **focus on the sectors which are not yet covered by a specific liability regime other than only national civil liability**.

Current national liability rules

We consider that the national liability rules (in France) are suitable and sufficient for the operation of AI to ensure proper compensation for damage and a fair allocation of liability. However, if changes were to be considered, it could only be part of a European framework.