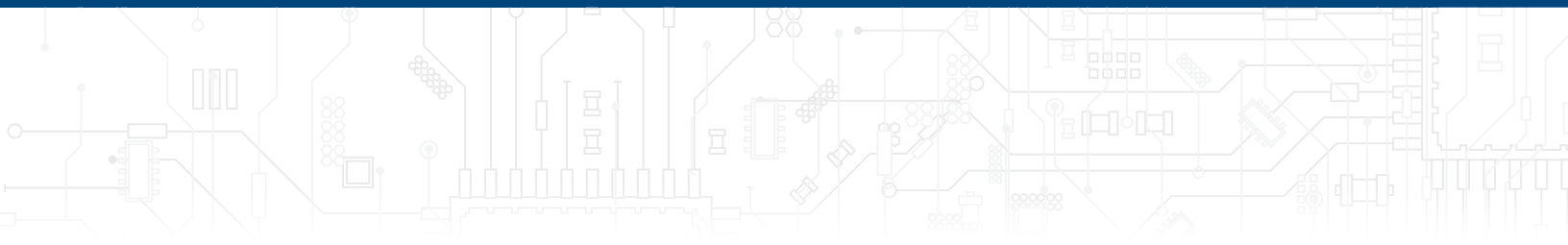




AI-generated image
Source: Adobe Stock



Issues and Discussion Paper

Best practices for the
responsible use of AI
in the financial sector



**AUTORITÉ
DES MARCHÉS
FINANCIERS**

Legal Deposit – Bibliothèque et Archives nationales du Québec, 2024

ISBN 978-2-550-96846-7 (PDF)



Table of contents

1. Preamble	4
2. Use of AI in the financial sector	5
3. Best practices for the responsible use of AI	9
3.1 Practices related to consumer protection	9
3.2 Practices related to transparency for consumers and the public	12
3.3 Practices related to the appropriateness of AIs	13
3.4 Practices related to responsibility	14
3.5 Practices related to AI design and use.....	14
3.6 Practices related to managing AI-associated risks	16
4. Discussion	19
Additional discussion questions	20
AMF contact persons	20
Bibliography.....	21

1. Preamble

The Autorité des marchés financiers (**AMF**) is a key player within Québec's financial ecosystem. In its role as regulator, the AMF acts to maintain a financial sector that is dynamic, operates with integrity and warrants public confidence. The AMF sets the rules and standards governing market activities and supports the adoption of best practices. In this mode, it is informed by the realities and lived experiences of its clientele, key trends, innovations, and insights into domestic and international markets.

Since 2016, the AMF has undertaken various mission-aligned initiatives relating to the digital transformation of the financial sector to, in particular, anticipate regulatory and consumer protection issues. In November 2021, it made a clear statement of its interest in the responsible use of artificial intelligence (AI) by signing the [Montréal Declaration for responsible AI development](#) and by publishing the paper [Artificial intelligence in finance – Recommendations for its responsible use](#) (the **2021 Report**), a report prepared at the AMF's request by Algora Lab, an interdisciplinary lab of the University of Montréal and the Institut québécois d'intelligence artificielle (Mila). The 2021 Report sets out 10 recommendations to promote the responsible development of AI in finance: three directed toward the AMF and seven toward the industry.

In 2023, the AMF contributed to the [réflexion collective sur l'encadrement de l'intelligence artificielle au Québec](#) (collective reflection on the regulation of artificial intelligence in Québec), an initiative led by the Conseil de l'innovation du Québec (**CIQ**) to identify issues and opportunities presented by AI with a view to ensuring its ethical and responsible development and use while remaining true to Québec values. This activity culminated in a report entitled [Prêt pour l'IA – Répondre au défi du développement et du déploiement responsables de l'IA au Québec](#) (the **CIQ Report**) (in French only).

In line with the recommendations put forward in the 2021 Report and in the CIQ Report, the AMF is continuing its work by publishing this issues and discussion paper inventorying the best practices that collectively define what is meant today by "responsible use of AI in the financial sector." The publication of this paper and the subsequent period of discussion with stakeholders is in response to the recommendations directed toward the AMF in the 2021 Report.

The purpose of this paper is not to implement a new framework or modify an existing one. None of the practices presented here constitute a new obligation for financial institutions and other players in the financial sector (financial players¹). Nevertheless, the AMF wishes to engage in dialogue with the industry about the use of these best practices, which can guide the financial sector toward the responsible use of AI. The financial players are also reminded that they must continue to comply with all currently applicable laws and requirements.

The AMF will continue to monitor AI developments and the integration of AI in the financial sector. It may consequently review the herein-described practices in the future and adjust them as new trends or risks emerge.

¹ In this paper, "financial players" include financial institutions, investment fund managers, dealers and advisers, firms, independent partnerships and independent representatives, credit assessment agents, and other companies and professionals subject to the laws and regulations administered by the AMF, except for reporting issuers under the *Securities Act*, market infrastructures and self-regulatory organizations.

2. Use of AI in the financial sector

Innovations that are helping to digitally transform the financial sector include ever-growing, “on-demand” computing power, which is facilitating the processing of large volumes of data generated through, among other things, digital technologies and connected objects. Unsurprisingly, there is an increasing interest in advances in AI, which are now being leveraged in all sectors of the economy to extract more value from data.

In the financial sector, the use of AI offers a multitude of opportunities with potential benefits for both consumers and businesses. For example, the integration of AI could lead to the development of new financial products and services or a reduction in costs for consumers. AI algorithms can also be used by businesses to improve client segmentation and more accurately tailor services to the specific needs and circumstances of clients, thereby enhancing the client experience. However, the integration of artificial intelligence systems (**AISs**) into financial players’ activities should be guided by best practices so as to properly manage the associated risks.

WHAT IS ARTIFICIAL INTELLIGENCE?

Artificial intelligence refers to a field of science that studies and attempts to reproduce the various mechanisms that make up human intelligence. Such efforts are generally derived from a concerted combination of computer science and statistical methods that make use of big data and exponentially growing computational power.

Artificial intelligence is generally associated with **machine learning** and **deep learning**, which focus on the design of algorithms and methods that efficiently compresses knowledge in a computer system so that it can perform complex tasks through a process akin to “learning.” It is also associated with **natural language processing**, which enables computers to process, generate and manipulate human language. **Large language models**, for example, are AI models that are typically trained on large amounts of text and have a very large number of parameters. Often used for the implementation of chatbots, they can capture many aspects of human language syntax and semantics.

Generative AI refers to the use of AI for the purpose of creating new content such as text, images, music, sounds and videos.

AI model training is the process by which the model “discovers” relationships within the data (training data). The model can then use those relationships, and sometimes continually refine them, to make predictions on new data the model has not encountered before.

Finally, an **artificial intelligence system (AIS)** is “a technological system that, autonomously or partly autonomously, processes data related to human activity through the use of a genetic algorithm, a neural network, machine learning or another technique in order to generate content or make decisions, recommendations or predictions” (Source: Bill 188 [Artificial Intelligence and Data Act](#)).

AISs differ from the static systems or models traditionally used in the financial sector in the following respects:

- **Complexity:** AISs use advanced algorithms that can contain millions of parameters. AISs are also capable of processing very large volumes of data, including unstructured data.
- **Probabilistic models:** AISs process the information fed to them using probability-based models to, for example, anticipate a future outcome using standard sequences or historical data, assign an element to a pre-defined category among all possible categories, or update an assumption based on new facts. As using these models involves a margin of error, it is not possible to anticipate future outcomes with certainty.
- **Opacity:** AISs are sometimes called “black boxes” because it is generally difficult to understand how they reach a particular outcome or decision. The model structure (e.g., deep learning algorithms) makes it impossible to clearly establish the logical relationship between inputs and outputs. This lack of transparency can, among other things, impede the processes for identifying and correcting errors or discriminatory biases.
- **Dynamism:** Some AISs (continuous learning models) are designed to continually adjust as new data inputs are received. Their performance may therefore change over time: this is referred to as model drift.

Unstructured data is data that is not arranged according to a pre-defined model. It can take the form of images, videos, audio recordings and other types of media. Unstructured data is distinguished from structured data, which is organized into pre-defined items, each of which relates to a specific concept or data item.

(Source: [Statistics Canada](#))

AI model drift (or concept drift) is where the statistical properties of the data the model is trying to predict change unexpectedly over time. This causes problems because the model’s predictions become less and less accurate as time goes by.

(Source: [Wikipedia](#))

Complex models and algorithms are already widely used in the financial sector. However, the following AIS characteristics have the potential to cause material harm:

- *For investors and financial consumers* (collectively, **consumers**): Consumers may be denied access to a financial product or service as a result of discriminatory biases introduced into an AIS or a flaw in the AIS. Moreover, conflicts of interest may influence an AIS's recommendations to an investor.

AIS-powered digital engagement practices (e.g., gamification and nudging) can be used to consumers' detriment by exploiting their behavioural biases (e.g., by "nudging" them to take actions that are not in their best interests). AI can also facilitate consumer surveillance or other privacy incursions owing, for example, to the use of information collected from a smart phone or other connected object.

Another risk for consumers is the absence of clear, accessible information explaining how AI is integrated into a financial product or service, the reasons for decisions affecting consumers or what remedies are available to them.

Lastly, the availability of generative AI tools on the web significantly increases the risk of fraud for consumers. Deep fakes lend added credibility to misleading posts on social media, and large language models (LLMs) may be used to draft phishing e-mails in multiple languages.

- *For financial players*: Deploying a biased or flawed AIS could pose a significant reputational risk. What is more, errors or drift in an AIS used for resource allocation or investing could affect financial players' solvency. This risk may also materialize as a result of an employee's uninformed or ill-intentioned use of an AIS (e.g., use of a generative AI tool for which the training data include one or more copyrighted works without the copyright holder's permission).


Lastly, AISs pose a cybersecurity risk for financial players because, for example, they may be targets of attacks designed to deceive or exploit them. Moreover, AIS training requires large quantities of data that, if it contains personal information and is not properly protected, could be vulnerable to privacy breaches.

Gamification involves applying mechanisms used in gaming to marketing practices. **Nudging** involves using various techniques (such as notifications) to draw consumers' attention to something or encourage them to take a particular action. Gamification and nudging are two digital engagement practices, which are various engagement techniques used with clients in a digital environment.

(Source: [Insights into the risks and benefits of digital financial services for consumers](#))

A **deepfake** uses AI to create highly realistic images or sound clips of fake events.

(Source: [Autorité des marchés financiers](#))

- 
- *For market integrity:* The opacity and dynamism of AISs used to automate trading processes and investment decisions creates risks for the financial markets. For example, some AISs used to interact with investors or consumers may present conflicts of interest that, once uncovered, could adversely affect public confidence in the financial markets. The use of AISs could also facilitate media dissemination of false or misleading information (e.g., deep fakes).
 - *For financial stability:* Errors or drift in such AISs may also result in flash crashes. These sudden market movements, made more frequent by the increasing speed with which orders are placed and executed, could also result in market liquidity issues. Large-scale movements could also be generated by the widespread adoption of similar AISs or AISs trained and fed with similar data, resulting in unexpected concentrations or interconnections that would be difficult to detect owing to model opacity.

In general, the use of AI increases the scope and speed of impact of existing risks. AIS harm resulting from poor data quality or from outcomes generated by a biased, flawed or poorly implemented AIS may be more widespread and be perpetuated more quickly than when traditional systems are used. For example, the use of AISs may, in some cases, lead to increased systemic discrimination or the exclusion of certain groups of consumers from the financial system and produce inequality.

Lastly, governments and the private sector are investing heavily in AI research and marketing, causing scientific and technological advances to accelerate at breakneck speed. The fast pace of development is widening the mismatch between the opportunities afforded by AI and our understanding of the issues it may present in the medium to long term. In view of the rapid, uncertain pace of AI development, but also the potential benefits of AI for the financial sector, the AMF wishes to deepen its understanding of the risks associated with this technology and the practices to be implemented so that those risks can be managed without inhibiting innovation. At stake is continued confidence in our financial system.

3. Best practices for the responsible use of AI

The AMF is proposing 30 best practices for the responsible use of AI that draw from ethical principles and legislative and regulatory projects put forward in a number of jurisdictions. These practices apply to all AISs implemented by a financial player, including those that continue to be internally focused. These practices should be adapted to the characteristics of the AIS used, the financial player’s business environment and the risk assessment for the use of an AIS, especially as regards its impact on consumers.

3.1 PRACTICES RELATED TO CONSUMER PROTECTION

The practices presented in this section could help protect consumers from the unfair, abusive or misleading use of AI by financial players. These practices promote the use of AI in a manner consistent with consumers’ reasonable expectations with respect to both privacy and autonomy.

1. Using AI in consumers’ best interests

The use of AI should not cause any harm to consumers, individually or collectively, by, for example, creating barriers to financial inclusion, systemizing unjustified discriminatory biases or increasing economic and social inequalities.

AISs can model and influence human behaviour through mechanisms that can be difficult to detect because they can exploit unconscious processes. AI should not be used to mislead or manipulate the public through, for example, an AIS that unduly influences and inform consumers’ product or service decisions, the posting of misleading content on social media (e.g., deep fakes), or the communication of exaggerated information on the value added by a financial player’s use of AI in its activities.

Lastly, where an AIS presents itself as human, consumers should be clearly told that it is an automated agent.

2. Respecting consumers' privacy

Any intrusion by an AIS into consumers' private lives should be consistent with personal information protection and privacy laws and regulations² and warranted by the potential benefits accruing to consumers.

Requests for consumers' consent to the collection and use of their data should be in plain language and based on a clear description of the AIS's purposes and the need for the AIS to collect data to ensure its proper functioning. The consent should cover any collection of consumers' personal information, including data relating to them (e.g., data contained in social media posts). Outcomes or decisions provided by an AIS regarding a consumer may constitute personal information and should therefore be treated as such.

An AIS intended to monitor a consumer's behaviour should only be deployed with the consumer's consent. Such monitoring should be relevant and necessary for the use of the product or service offered. However, no AIS should make a consumer feel under constant surveillance.

Lastly, some AISs enable inferences about a person's characteristics, habits or life events. For example, a person's chances of having children or belonging to a particular ethnic group can be evaluated. In some contexts, the inference may be perceived by the consumer as an intrusion into their private life. AISs should produce inferences only about characteristics, events or habits that may reasonably be expected by the consumer and that are related to the nature of the financial product or service offered.

3. Increasing consumer autonomy

The deployment of an AIS should not have the effect of limiting freedom of choice or influencing a consumer's behaviour or lifestyle. On the contrary, AISs should be designed and made available to consumers to support them in making decisions better aligned with their circumstances and financial goals.

Financial players making automated decisions through an AIS should inform consumers of this fact and obtain their prior consent. Clear, reasonably priced options should be offered to consumers who do not wish to interact with or be monitored by an AIS or have an automated decision made about them.

² Particularly the rules governing the financial player's privacy policy, the consent of the person concerned, the security and destruction of personal data, the rights of access and correction, and the disclosure of confidentiality incidents to the bodies responsible for administering such legislation. In Québec, the [Act respecting the protection of personal information in the private sector](#) and the [Act respecting Access to documents held by public bodies and the Protection of personal information](#) are administered by the [Commission d'accès à l'information](#).

4. Treating consumers fairly

Consumer segmentation based on relevant and socially accepted criteria enables financial players to offer financial products and services appropriate to the circumstances of each group of consumers, at an appropriate price and with an appropriate risk profile. Segmentation is used, for example, in evaluating credit for mortgage loans or assessing the risk covered by an insurance policy. However, the only way to achieve these benefits is to use data and models that are free of quality issues and discriminatory biases.

AIS performance depends intrinsically on the quality of the data used. An AIS should be trained with up-to-date data that is representative of the system's target population and does not reflect, for example, biases from discriminatory practices.

To obtain such data, vulnerable groups of consumers or groups of consumers that may be unduly disadvantaged (e.g., new immigrants, people who are illiterate, or people who are unfamiliar with digital technologies) should be identified, and an AIS's impact on these groups should be assessed at the design phase. Measures should also be implemented to validate the equity of outcomes provided by the AIS, and where two consumers or groups of consumers are treated differently, the difference in treatment should be justifiable on the basis of appropriate criteria. Financial players might consider involving an ethicist or sociologist in such analyses in order to clearly identify sources of discrimination and appropriate mitigation measures.

5. Managing conflicts of interest in consumers' best interests

Conflicts of interest (e.g., the possibility that an AIS will favour a financial player's interests over the interests of consumers) that may appear in AIS outcomes or decisions should be eliminated or mitigated throughout the life cycle of the AIS. Particular attention should be paid to identifying conflicts of interest in complex or opaque AISs or in AISs with hard-to-explain outcomes.

6. Consulting consumers required to use AIS

Consumers should be regarded as stakeholders in an AIS's design. Before deploying an AIS that could have a high impact on consumers, consumers' input should be sought and considered by the financial players in identifying ethical risks, particularly where an AIS could potentially lead to feelings of privacy incursion or loss of autonomy. Consultations would include, but not be limited to, the participation of consumers whose data is used by the AIS or who could be impacted by AIS outcomes or decision making. Minority or vulnerable groups of consumers should be involved in the consultations.

Participation mechanisms enabling consumers' comments to be gathered regularly throughout the life cycle of an AIS should also be implemented for AISs that could have a high impact on consumers generally or on a particular group of consumers.

3.2 PRACTICES RELATED TO TRANSPARENCY FOR CONSUMERS AND THE PUBLIC

This section presents practices intended to establish an adequate level of transparency regarding financial players' use of AI. Such a level of transparency may be achieved without the financial player having to reveal trade secrets.

7. Disclosing information about the AI design and use framework

Consumers must be able to form an opinion about respect for ethical principles and the social acceptability of the use made of AI in the financial sector. A lack of transparency on the part of financial players regarding their approach to and ethical and governance frameworks for the use of AI could limit debate.

8. Disclosing information on the use of AI in products and services

Consumers should have access to the information they need to assess the benefits and risks associated with the use of AI in the context of procuring a financial product or service, especially when making a product or service decision. Such information should cover, in particular, the objectives, limitations and functioning of the AIS and the measures in place to mitigate the associated risks. Consumers should also have access to all relevant information on the rights and remedies available to them should they incur harm from interacting with the AIS.

A **digital watermark** is a permanent mark embedded in a document or other medium to, in particular, protect intellectual property rights and fight piracy.

(Source: [Grand dictionnaire terminologique](#))

Plain, non-technical and concise language should be used when communicating with consumers. The disclosure interface should be designed to encourage consumers to read the information closely rather than respond quickly. Consumers who find the disclosed information insufficient should be able to request and receive assistance from a technical expert.

Consumers should also be informed, by appropriate means (e.g., digital watermarking), that content published by a financial player has been wholly or partly created by a generative AI tool.

9. Explaining outcomes relating to a consumer

Whenever an AIS could have a high impact on a consumer, the consumer should have the opportunity to request a clear, reliable explanation of the process and main factors that led to the outcomes or decision provided by the AIS. The AIS should be designed so that such outcomes are traceable and explainable.

When explanations are clear, there is no need to share intellectual property or source code. Non-technical language should be used, at a level of detail proportional to the seriousness of the consequences for the consumer of an erroneous decision or outcome.

Also, the consumer should be able to obtain a list of any personal information about them that is used by the AIS and to correct or update such information if it is inaccurate.

10. Providing consumers with communication channels and assistance and compensating mechanisms

When consumers interact with an AIS, they should be able to get help, at any stage of the process, through an interaction with a competent person. They should also have the option of requesting to have the outcomes or decision of the AIS reviewed by a person. For this, consumers should have access to someone able to explain the functioning of the AIS to them and give them the opportunity to present their arguments challenging the outcome or decision.

Information on these and other assistance and compensating mechanisms should be easily accessible and comprehensible to consumers. When implementing such mechanisms, particular attention should be paid to vulnerable consumers.

Consumers are generally considered to be in a **vulnerable** situation when they cannot properly assess the consequences of some decisions or situations. The vulnerability may be temporary or permanent.

(Source: [A practical guide for the financial services industry – Protecting vulnerable clients](#), Autorité des marchés financiers)

3.3 PRACTICES RELATED TO THE APPROPRIATENESS OF AISS

The characteristics specific to AISs entail significant risks for all financial sector stakeholders. The practices proposed in this section address the appropriateness of using AI in a given situation, particularly where there are options that perform equally well or yield equivalent outcomes but carry fewer risks or are more easily explainable.

11. Justifying each case of AI use

The objectives sought in connection with the design or use of an AIS should be appropriate to the financial player's mission. Also, consumers should be able to derive a benefit from the AIS, which should be simple and easy to summarize (e.g., consumers will be able to benefit from faster or better-tailored service or save money).

It should also be possible to demonstrate that a proper balance has been achieved between the financial player's interests and the interests of other parties impacted by the AIS (e.g., certain vulnerable groups of consumers).

12. Prioritizing the simplest, most easily explainable treatment

The outcomes obtained using an AIS should generally be better than those obtained without using it or by using simpler, more easily explainable technologies. This practice should be more strictly applied for AISs with a potential high impact on consumers.

The benefits of using AI should also outweigh the foreseeable risks and harm, generally and for each group of individuals or consumers that could be affected.

3.4 PRACTICES RELATED TO RESPONSIBILITY

The task-performance and decision-making autonomy that an AIS is capable of exhibiting has profound implications for an organization's AI governance. The practices presented in this section help ensure that responsibility for the outcomes and decisions of an AIS is clearly assigned to an individual.

13. Being accountable for the actions and decisions of an AIS

The use of AI must not contribute to a lack of accountability among financial players. On the contrary, responsibility for all outcomes of and harms caused by an AIS deployed by a financial player (including AISs acquired from third parties) should remain with the financial player, regardless of the intended objectives.

14. Making employees and officers accountable with respect to the use of AI

AISs can enhance the work performance of a financial player's employees. Given the potential for automation bias, financial players' employees and officers should be made aware that they are at all times accountable for their actions and decisions and that their actions and decisions cannot be attributed to an AIS.

Automation bias is the propensity for humans to favour suggestions from automated decision-making systems and to ignore contradictory information made without automation, even if it is correct.

(Source: [Wikipedia](#))

15. Implementing human control proportional to AIS risks

An AIS's level of task-performance and decision-making autonomy should be established and justified at the design stage. The design should also enable an employee with the necessary skills to exercise adequate control over each deployed AIS based on its impact on consumers and the risks associated with its use.

An employee should, among other things, individually review and validate all AIS decisions that adversely affect a consumer's ability to obtain a financial product or service or any other decision that has a high impact on the consumer's financial well-being.

3.5 PRACTICES RELATED TO AI DESIGN AND USE

A flawed governance framework, confusion over roles and responsibilities, or the absence of a clear ethical framework creates situations conducive to the materialization of risks associated with a financial player's use of AI. The practices presented in this section are intended to mitigate such risks.

16. Overseeing AI design and use

A governance structure should be put in place to ensure oversight of a financial player's use of AI. This structure should include standards governing AIS design and use, such as model calibration and data processing standards. It should be possible to adjust these standards based on the AIS's impact on consumers and the risks associated with its use, and to cover all stages of its life cycle.

The roles and responsibilities of each AIS stakeholder, including the officers of the financial player, should be clearly defined. These parties should have the skills and resources required to discharge their responsibilities.

17. Establishing a code of ethics for the design and use of AI

A code of ethics should be established or amended to include the values and ethical principles that should be observed when using AI and to set out the sanctions applicable in the event of non-compliance with the obligations specified in the code. Individuals subject to this code of ethics should also be provided with an interpretation of those principles in plain and concise language.

In the context of the design of an AIS, one might consider involving a committee in the assessment of the ethical risks associated with an AIS and the implementation of mitigation measures.

18. Creating an environment favourable to transparency and disclosure

An organizational environment should be promoted that encourages transparency and disclosure so that doubts or concerns related to AISs (e.g., errors, negative outcomes, data misuse and data leaks) may be raised anonymously and without fear of reprisal.

19. Establishing a consistent approach to AIS design, deployment and monitoring

The approach to AIS design, deployment and monitoring should be consistent across the organization, as opposed to fragmented or decentralized, in order to, for example, be able to identify interconnection risks when a dataset is used as inputs for more than one AIS. An ethics-by-design approach should be favoured.

In addition, financial players should implement regular, comprehensive reporting to senior management and the board directors on the performance of all deployed AISs and the risks associated with them.

20. Facilitating the creation of diversified work teams

Diversity and inclusion are values critical to the development of AISs for use in the financial sector. Consequently, the teams formed to develop, deploy and monitor a financial player's AISs should reflect the diversity of consumers and society as a whole in order to, for example, prevent the risk of unjustifiably discriminating among consumers. These teams would not only be diverse in terms of gender, culture and age but also professionally and in terms of skills.

21. Conducting due diligence on third-party AISs

Due diligence should be conducted when procuring an AIS designed or provided by a third party. Third-party AISs and the associated training data should be subject to the same standards as in-house designed AISs. Consequently, staff involved in procuring a third-party AIS should have the skills required to apply those standards properly.

Also, the financial player and the third party should enter into an agreement setting out clear service levels and the rights and remedies available to the financial player in case of poor AIS performance.

22. Using AI in a manner enabling the achievement of sustainable development objectives

The carbon footprint from the design and use of AISs, including data hosting, should be measured and limited by avoiding such things as the proliferation of unnecessary or redundant data infrastructures, employing simpler or pretrained models or limiting the use of energy-intensive AISs.

Generally, AI should be used by a financial player in a manner consistent with the financial player's environmental commitments.

3.6 PRACTICES RELATED TO MANAGING AI-ASSOCIATED RISKS

The practices presented in this section are intended to reduce the occurrence of potential adverse consequences resulting from unexpected behaviours exhibited by an AIS, including, without limitation, unacceptable harms for consumers.

23. Assessing the risks associated with the use of an AIS

Risks that may result from the use of an AIS must be identified considering the AIS's impact on consumers and the risks associated with its use to the financial player's activities, market integrity, and financial stability. Important factors to consider in assessing these risks include the AIS's degree of complexity, opacity, dynamism and autonomy.

More resources should be dedicated to the design and monitoring of an AIS with a potential high impact on consumers or with a high risk assessment.

24. Ensuring AIS security

A financial player's AISs should be protected, particularly against hacking (including data poisoning or adversarial attacks) and cyber attacks. When implementing security measures, AIS interconnectivity should be assessed to limit the extent of attacks or disruptions. These measures should be monitored and reviewed to ensure, among other things, that they remain aligned with technological developments.

In addition, measures should be implemented to ensure the integrity of the data used as inputs or to train AISs, even if the data is not personal information. Only authorized personnel should have access to such data.

Data poisoning attacks and adversarial attacks (sometimes also referred to as adversarial example attacks) seek to alter an AIS's behaviour by adding malicious or corrupted data during the training or production phase.

(Source: [Commission Nationale de l'Informatique et des Libertés](#))
(in French only)

25. Governing the data used by AISs

Governance of the data used to train an AI model or as inputs for an AIS should be implemented through, in particular, processes for assessing data representativeness and quality and for determining whether discriminatory biases are present in the data. An AIS with a high impact on consumers should not be deployed if the risks associated with the data used are not adequately mitigated.

The financial player's governance rules should be applied to both data it has collected or generated itself and data procured from third parties. Particular attention should be paid to potential issues arising from the use of non-traditional, unstructured synthetic, anonymized and de-identified data, as well as issues that may emerge during the process of aggregating data from various sources (e.g., the risk of consumer re-identification). All AISs should be tested on real (non-synthetic) data before being released to production.

Data should also be used in accordance with the applicable terms of use (e.g., where data is copyrighted).

26. Managing the risks associated with AI models

The robustness of an AIS (i.e., its ability to function effectively under a variety of conditions) is critical to its reliability. The robustness of AISs designed by a financial player should be enhanced by the competence of the staff entrusted with this task and through the use of rigorous design guides based on recognized technical standards.

The risks associated with the models underlying AISs should be identified, assessed and mitigated at each stage of their life cycle. This practice extends to the use of open-source code models.

Risks that should be identified and managed include model drift or unexpected AIS behaviours in new conditions. In addition, particular attention should be paid to risks arising from interconnections between a financial player's AIS when, for example, the outcomes of one AIS are used as inputs for another AIS. Finally, succession risk should be mitigated by ensuring the continued availability of competent staff qualified to ensure AIS monitoring.

Synthetic data is data that is artificially generated through simulations rather than produced by real-world events. Synthetic data production aims to create a dataset with statistical properties as close as possible to a real dataset but that does not contain personal information, for example.

(Source: [Wikipedia](#))

Data that is personal information is **de-identified** when it no longer allows the person concerned to be directly identified. In addition, data that is personal information is **anonymized** if it is, at all times, reasonably foreseeable in the circumstances that it irreversibly no longer allows a person to be identified directly or indirectly. **Re-identification risk** is the risk that a person may be identified from data that has been anonymized or de-identified.

(Source: [Commission d'accès à l'information](#)) (in French only)

27. Performing an impact analysis and testing an AIS

An impact analysis (also known as an algorithmic impact assessment) should be initiated at an AIS's design stage. The depth of the impact analysis should be adjusted based on the impact that the AIS could have on consumers (or a particular group of consumers).

As part of the analysis, the appropriateness of using AI and of incursions into consumers' private lives should be justified. The analysis should also address discriminatory biases (often discovered during the parameter estimation and model assessment phases), conflicts of interest, or other factors that could cause inequitable outcomes.

Testing in an environment separate from the production environment should be conducted to validate the absence of errors and malfunctions and verify that the AIS behaves as expected in a variety of conditions.

An impact analysis and pre-deployment testing should also be conducted when material changes are made to an AIS, significant drift occurs, or an AIS is used to achieve new objectives.

Impact analysis and testing should be entrusted to a diversified multidisciplinary team that is competent (particularly in the area in which the AIS will be used) and trained in AI-related ethical issues.

28. Monitoring AIS performance on an ongoing basis

AIS monitoring should be implemented to enable the detection of deviations from normal operation (such as material model drift or a degradation in input data quality), discriminatory or inequitable outcomes, inappropriate use, or use for harmful purposes. Thresholds should be established for critical parameters, and an in-depth AIS review should be triggered if the thresholds are exceeded.

A circuit-breaking feature to interrupt the use of an AIS if its performance deteriorates beyond a given threshold should be implemented and periodically tested. In addition, a financial player should include its AISs in its business continuity plans to ensure the financial player's operational resilience.

29. Regularly auditing AISs

Deployed AISs should be audited periodically. Audit depth and frequency and the determination of whether to use external, independent auditors should be based on an AIS's impact on consumers and the risks associated with its use. Documentation relevant to the AIS, together with the codes and training datasets, should be made available to the auditors and regulators.

30. Training employees and users on AI

Employees and any other third parties involved in designing, deploying and monitoring an AIS, senior management, and other managers with responsibilities in connection with an AIS should maintain an appropriate level of technical skill and sufficient knowledge of the ethical risks to perform their tasks properly. In addition to technical and ethical aspects, training and awareness initiatives deployed by a financial player should cover personal information and privacy protection and intellectual property compliance. Employee training and awareness initiatives should also address the proper use of generative AI tools available online.

In addition, all users of an AIS deployed by a financial player, including consumers or other external parties, should be able to understand the AIS's objectives and limitations. They should have access to the training they need to use it properly.

4. Discussion

The AMF wishes to initiate a discussion with all Québec financial sector stakeholders on best practices that promote the responsible use of AI. It will be a general consultation on the opportunities and risks associated with the use of AI in finance and on the actions that should be focused on to mitigate the risks to consumers, financial players, market integrity and financial stability.

The issues raised and practices proposed in this document affect all financial sector stakeholders, investors and financial consumers.

Interested parties are invited to request a meeting with the AMF contact persons so that they can submit their comments on the proposed practices and their answers to the questions below before June 14, 2024. The AMF will also be organizing round tables and other discussion forums during this period in order to obtain additional input and deepen its understanding of the use of AI in the financial sector. Information about the various ways to participate in this discussion is available on the AMF website at <https://lautorite.qc.ca/en/general-public/publications/for-professionals/ai-in-the-financial-sector>.

Also, anyone interested in submitting comments in writing may do so on or before **June 14, 2024**, by sending them to:

M^e Philippe Lebel
Corporate Secretary and Executive Director, Legal Affairs
Autorité des marchés financiers
Place de la cité, tour Cominar
2640, boulevard Laurier, 3^e étage, Québec (Québec) G1V 5C1
Fax: 418-525-9512
E-mail: consultation-en-cours@lautorite.qc.ca.

ADDITIONAL DISCUSSION QUESTIONS

In addition to comments on the appropriateness of the best practices presented in this paper, the AMF wishes to receive comments responding to the following questions:

1. In addition to the values and ethical principles set out in this paper, what other important principles do you think should be put forward?
2. Which cases of AI use in finance present the most risks? Are the proposed practices sufficient to mitigate the risks associated with the use of AI in the financial sector? Consider the risks to consumers, financial players, market integrity and financial stability.
3. Is there a risk that the implementation of the practices described in this paper could inhibit innovation in the financial sector? If so, why?
4. Do the financial players have the resources, particularly the required qualified human resources, to implement the proposed practices? Does the implementation of the practices described in this paper seem achievable to you? Over what time horizon (short, medium, long term)?
5. What role should technical standards play in practices related to the responsible use of AI in the financial sector?
6. How are the financial players integrating generative AI into their activities? How are they regulating employees' use of on-line generative AI tools?
7. What role do you see the AMF playing in supporting financial players in integrating AI into their activities, and what would be the best way for the AMF to fulfill that role?

AMF CONTACT PERSONS

Clarification or additional information can be obtained by contacting:

Lise Estelle Brault, CFA

Senior Director, Data Value Creation,
Digital Transformation and Innovation
Telephone: 514-395-0337, ext. 4481
Toll-free: 1-877-525-0337, ext. 4481
LiseEstelle.Brault@lautorite.qc.ca

Marie-Ève Lainez

Director, Digital Transformation and Innovation
Telephone: 514-395-0337, ext. 4891
Toll-free: 1-877-525-0337, ext. 4891
Marie-Eve.Lainez@lautorite.qc.ca

February 12, 2024

BIBLIOGRAPHY

AFM (2023). Proprietary traders make large-scale use of machine learning in trading algorithms. March 3, 2023. Online: <https://www.afm.nl/en/sector/actueel/2023/maart/her-machine-learning>

ANDERSEN, ROSS (2023). "Does Sam Altman Know What He's Creating?" *The Atlantic*, July 24, 2023. Online: <https://www.theatlantic.com/magazine/archive/2023/09/sam-altman-openai-chatgpt-gpt-4/674764/>

BANK OF ENGLAND (2022). Artificial Intelligence Public-Private Forum final report. February 2022. Online: <https://www.bankofengland.co.uk/-/media/boe/files/fintech/ai-public-private-forum-final-report.pdf?la=en&hash=F432B83794DDF3F580AC5A454F7DFF433D091AA5>

BANK OF ENGLAND (2022). Artificial Intelligence and Machine Learning. Discussion Paper 5/22, October 11, 2022. Online: <https://www.bankofengland.co.uk/prudential-regulation/publication/2022/october/artificial-intelligence>

BANK OF ENGLAND (2022). Machine learning in UK financial services. October 11, 2022. Online: <https://www.bankofengland.co.uk/Report/2022/machine-learning-in-uk-financial-services>.

BENGIO, Yoshua (2023). Artificial intelligence: The future of AI – a future I helped create – keeps me up at night. *The Globe and Mail*, October 28, 2023. Online: <https://www.theglobeandmail.com/opinion/article-the-future-of-artificial-intelligence-a-future-i-helped-create-keeps/>

BENGIO, Yoshua (2023). "How Rogue AIs may Arise." Personal blog, May 30, 2023. Online: <https://yoshuabengio.org/2023/05/22/how-rogue-ais-may-arise/>

BENESSAIEH, Karim (2023). "Intelligence artificielle - Un impact environnemental monstre." *La Presse*, June 3, 2023. Online: <https://www.lapresse.ca/affaires/economie/2023-06-03/intelligence-artificielle/un-impact-environnemental-monstre.php>.

BERGAMINI, Massimo (2023). "Pour une vision pancanadienne de l'intelligence artificielle." *La Presse*, August 10, 2023. Online: <https://www.lapresse.ca/debats/opinions/2023-08-10/marche-du-travail/pour-une-vision-pancanadienne-de-l-intelligence-artificielle.php>

BOND, Shannon (2023). "Fake viral images of an explosion at the Pentagon were probably created by AI." *NPR Vermont Public*, May 22, 2023. Online: <https://www.npr.org/2023/05/22/1177590231/fake-viral-images-of-an-explosion-at-the-pentagon-were-probably-created-by-ai>

CASTETS-RENARD, Céline and Anne-Sophie HULIN (2023). "The time for a law on artificial intelligence has come." *Policy Options*, September 27, 2023. Online: <https://policyoptions.irpp.org/magazines/september-2023/law-artificial-intelligence-now/>

CASTETS-RENARD, Céline and Benoît PELLETIER (2023). "Le développement de l'intelligence artificielle doit faire l'objet d'un débat démocratique." *Le Devoir*, March 31, 2023. Online: <https://www.ledevoir.com/opinion/idees/787431/legislation-le-developpement-de-l-ia-doit-faire-l-objet-d-un-debat-democratique>

CFA INSTITUTE (2023). Handbook of Artificial Intelligence and Big Data Applications in Investments. Online: <https://www.cfainstitute.org/-/media/documents/article/ai-and-big-data-in-investments-Intro.pdf>

CHARLAND, Pierre and LAPIERRE, Hugo G. (2023). "L'intelligence artificielle inquiète. Il est temps d'éduquer la population à la programmation." *The Conversation*, April 3, 2023. Online: <https://theconversation.com/lintelligence-artificielle-inquiete-il-est-temps-deduquer-la-population-a-la-programmation-202025>

COLLECTIF (2018). Montréal Declaration for a Responsible Development of Artificial Intelligence. Online: <https://montrealdeclaration-responsibleai.com/>

OFFICE OF THE PRIVACY COMMISSIONER OF CANADA (2023a). Joint statement on data scraping and the protection of privacy. GPA's International Enforcement Cooperation Working Group, August 24, 2023. Online: https://www.priv.gc.ca/en/opc-news/speeches/2023/js-dc_20230824/

OFFICE OF THE PRIVACY COMMISSIONER OF CANADA (2023b). Statement on Generative AI. Roundtable of G7 Data Protection and Privacy Authorities, June 21, 2023. Online: https://www.priv.gc.ca/en/opc-news/speeches/2023/s-d_20230621_g7/

EUROPEAN COMMISSION (2021). Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS. Procedure No. 2021/0106/COD. Online: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206>

STANDARDS COUNCIL OF CANADA (2023). AI and data governance. Online: <https://www.scc.ca/en/flagships/data-governance>

CONSEIL DE L'INNOVATION DU QUÉBEC (2023). Réflexion collective sur l'encadrement de l'intelligence artificielle – Pour le développement et l'utilisation responsables de l'IA au Québec – Thématique 1 : Le cadre de gouvernance de l'IA. Online: <https://conseilinnovation.quebec/intelligence-artificielle/reflexion-collective/thematique-1-le-cadre-de-gouvernance-de-lia/>

EUROPEAN COMMISSION (2023). "Regulatory framework proposal on artificial intelligence." Shaping Europe's digital future, June 20, 2023. Online: <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>

EUROPEAN PARLIAMENT (2021). "Challenges and Limits of an Open Source Approach to Artificial Intelligence." Study requested by the AIDA Committee. Online: [https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662908/IPOL_STU\(2021\)662908_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662908/IPOL_STU(2021)662908_EN.pdf)

EUROPEAN PARLIAMENT (2023). "AI Act: a step closer to the first rules on Artificial Intelligence." May 11, 2023. *European Parliament News*. Online: <https://www.europarl.europa.eu/news/en/press-room/20230505IPR84904/ai-act-a-step-closer-to-the-first-rules-on-artificial-intelligence>

EUROPEAN PARLIAMENTARY RESEARCH SERVICE (2023). "Artificial intelligence act." *Briefing – EU Legislation in Progress*, June 2023. Online: [https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI\(2021\)698792_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf)

GENSLER, Gary and BAILEY, Lily (2020). "Deep Learning and Financial Stability." *MIT Sloan*, November 1, 2020. Online: <https://mitsloan.mit.edu/shared/ods/documents?PublicationDocumentID=7644>

G7 Hiroshima Process on Generative Artificial Intelligence (AI): Towards a G7 Common Understanding on Generative AI. OECD Publishing, Paris, <https://doi.org/10.1787/bf3c0c60-en>

GAGNON, Katia (2023). "Examen du Barreau – ChatGPT recalé." *La Presse*, May 25, 2023. Online: <https://www.lapresse.ca/actualites/justice-et-faits-divers/2023-05-25/examen-du-barreau/chatgpt-recale.php>

GARTNER (2023). "What's New in Artificial Intelligence from the 2023 Gartner Hype Cycle." Gartner, August 17, 2023. Online: <https://www.gartner.com/en/articles/what-s-new-in-artificial-intelligence-from-the-2023-gartner-hype-cycle>

GOVERNMENT OF CANADA. Directive on Automated Decision-Making. Online: <https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32592>

GOVERNMENT OF CANADA. Canadian Guardrails for Generative AI – Code of Practice. Online: <https://ised-isde.canada.ca/site/ised/en/consultation-development-canadian-code-practice-generative-artificial-intelligence-systems/canadian-guardrails-generative-ai-code-practice>

GOVERNMENT OF QUÉBEC. Décision fondée exclusivement sur un traitement automatisé. Online: <https://www.quebec.ca/gouvernement/travailler-gouvernement/travailler-fonction-publique/services-employes-etat/conformite/protection-des-renseignements-personnels/technologie-et-droit-a-la-protection-des-renseignements-personnels/decision-traitement-automatise#:~:text=L%27organisme%20public%20qui%20met,la%20Loi%20sur%20l%27acc%C3%A8s>

GUIRODO, Carole (2023). “Face à GPTBot, les médias se rebiffent.” *La Presse* (Agence France-Presse), August 30, 2023. Online: <https://www.lapresse.ca/affaires/medias/2023-08-30/face-a-gptbot-les-medias-se-rebiffent.php>

GURMAN, Mark (2023). “Samsung Bans Staff’s AI Use After Spotting ChatGPT Data Leak.” *Business Insider*, May 2, 2023. Online: <https://www.businessinsider.com/samsung-chatgpt-bard-data-leak-bans-employee-use-report-2023-5#:~:text=Samsung%20bans%20employees%20from%20using,accidental%20data%20leak%2C%20report%20says&text=Samsung%20has%20banned%20employees%20from,code%20to%20ChatGPT%20in%20April>

High-Level Expert Group on Artificial Intelligence (2019). *Ethics Guidelines for Trustworthy AI*. European Commission. April 8, 2019. Online: <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>

HILL, Michael (2023). “Les entreprises confrontées à un recours massif au shadow IA.” *Le monde informatique*. November 2, 2023. Online: https://www.lemondeinformatique.fr/actualites/lire-les-entreprises-confrontees-a-un-recours-massif-au-shadow-ia-92015.html?utm_source=ActiveCampaign&utm_medium=email&utm_campaign=NL+LMI+Quoti+03112023&ep_ee=fb66a5a405c9ff1f1b9ffdc33acdcd3ee95fa972&vgo_ee=DTbK7+6GY0ofyQshnStlKFAjvbTwjYkYVMc4SO6mgLkW2ms=:BV0cRGp48olrsdW4twsOQ9Z/PZV25/by

INTERNATIONAL CONFERENCE OF DATA PROTECTION & PRIVACY COMMISSIONERS (2018). Declaration on Ethics and Data Protection in Artificial Intelligence. Online: http://globalprivacyassembly.org/wp-content/uploads/2018/10/20180922_ICDPPC-40th_AI-Declaration_ADOPTED.pdf

ISACA (2023). The Promise and Peril of AI Revolution: Managing Risk. September 12, 2023. Online: <https://www.isaca.org/resources/white-papers/2023/the-promise-and-peril-of-the-ai-revolution>

INTERNATIONAL ORGANIZATION OF SECURITIES COMMISSIONS (2021). The use of artificial intelligence and machine learning by market intermediaries and asset managers. September 2021. Online: <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD684.pdf>

JONCAS, Hugo (2023). “Nouvelles règles sur les renseignements personnels – Des PME à la traîne.” *La Presse*, September 11, 2023. Online: <https://www.lapresse.ca/affaires/entreprises/2023-09-11/nouvelles-regles-sur-les-renseignements-personnels/des-pme-a-la-traine.php>

KEARNS, Jeff (2023). “AI’s Reverberations Across Finance.” International Monetary Fund, December 2023. Online: <https://www.imf.org/en/Publications/fandd/issues/2023/12/AI-reverberations-across-finance-Kearns>

KIM, Alex, MUHN, Maximilian and NIKOLAEV, Valeri (2023). “Bloated Disclosures: Can ChatGPT Help Investors Process Information?” Chicago Booth Research Paper No. 23-07, April 21, 2023. Online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4425527

LAROUCHE, Pierre (2023). "Réglementer l'IA : mythes, défis et pistes." *La Presse*, May 22, 2023. Online: <https://www.lapresse.ca/debats/opinions/2023-05-22/reglementer-l-ia-mythes-defis-et-pistes.php>

LANGVIN, Richard (2023). "L'IA de plus en plus utilisée dans la gestion de patrimoine et d'actifs." *Les Affaires*, May 24, 2023. Online: <https://www.lesaffaires.com/blogs/richard-langvin/ia-de-plus-en-plus-utilisee-dans-la-gestion-de-patrimoine-et-dactifs/641176>

SQ 2021, C-25. *An Act to modernize legislative provisions as regards the protection of personal information*. Online: <https://www.canlii.org/en/qc/laws/astat/sq-2021-c-25/latest/sq-2021-c-25.html>

MACLURE, Jocelyn and Alexis MORIN MARTEL (2023). "The ethics of artificial intelligence await the law." *Policy Options*, September 27, 2023. Online: <https://policyoptions.irpp.org/magazines/september-2023/ethics-law-ai/>

MONETARY AUTHORITY OF SINGAPORE. Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of Artificial Intelligence and Data Analytics in Singapore's Financial Sector. Online: <https://www.mas.gov.sg/~media/MAS/News%20and%20Publications/Monographs%20and%20Information%20Papers/FEAT%20Principles%20Final.pdf>

OBVIA (2023). "L'éthique au cœur de l'IA." October 27, 2023. Online: <https://observatoire-ia.ulaval.ca/lethique-au-coeur-de-ia/>

OECD (2019). Recommendation of the Council on Artificial Intelligence. OECD/LEGAL/0449, May 21, 2019. Online: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>

ONTARIO SECURITIES COMMISSION and EY (2023). "Artificial Intelligence in Capital Markets." October 10, 2023. Online: <https://oscinnovation.ca/resources/Report-20231010-artificial-intelligence-in-capital-markets.pdf>

BILL C-27 (2022). An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts. 1st session, 44th legislature. Online: <https://www.parl.ca/legisinfo/en/bill/44-1/c-27>

MCKENNA, Alain (2023). "L'IA canadienne limitée dans son développement." *Le Devoir*. April 6, 2023. Online: <https://www.ledevoir.com/economie/788117/techno-l-ia-canadienne-limitee-dans-son-developpement>

MEGAW, NICHOLAS (2023). "Investors use AI to glean signals behind executives' soothing words." *The Financial Times*, November 12, 2023. Online: <https://www.ft.com/content/ee2788dd-aca5-4214-8a08-d88081eac1b9>.

NASDAQ (2023). "Nasdaq Announces First Exchange AI Powered Order Type Approved by the SEC." September 8, 2023. Online: <https://www.nasdaq.com/press-release/nasdaq-announces-first-exchange-ai-powered-order-type-approved-by-the-sec-2023-09-08>

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (2022a). AI Risk Management Framework: Initial Draft. March 17, 2022. Online: <https://www.nist.gov/system/files/documents/2022/03/17/AI-RMF-1stdraft.pdf>

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (2022b). Towards a Standard for Identifying and Managing Bias in Artificial Intelligence. NIST Special Publication 1270. March 2022. Online: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1270.pdf>

OECD AI Principles overview. Online: <https://oecd.ai/en/ai-principles>

OECD Artificial Intelligence Papers (2023). "Stocktaking for the Development of an AI Incident Definition. October 2023." Online: <https://www.oecd.org/publications/stocktaking-for-the-development-of-an-ai-incident-definition-c323ac71-en.htm>

OFFICE OF SCIENCE AND TECHNOLOGY POLICY (2022). "Blueprint for an AI Bill of Rights – Making Automated Systems Work for the American People." Online: <https://www.whitehouse.gov/ostp/ai-bill-of-rights/>

OFFICE OF THE SUPERINTENDENT OF FINANCIAL INSTITUTIONS and GLOBAL RISK INSTITUTE (2023). Financial Industry Forum on Artificial Intelligence: A Canadian Perspective on Responsible AI. April 2023. Online: <https://www.osfi-bsif.gc.ca/Eng/Docs/ai-ia.pdf>

EUROPEAN PARLIAMENT (2023). "EU AI Act: first regulation on artificial intelligence." *European Parliament News*, June 14, 2023. Online: <https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence>

UK GOVERNMENT (2023). "The Bletchley Declaration by Countries Attending the AI Safety Summit, 1-2 November 2023. Online: <https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023>

UK GOVERNMENT DEPARTMENT FOR SCIENCE, INNOVATION & TECHNOLOGY (2023). "A pro-innovation approach to AI regulation." March 2023. Online: <https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper>

RADIO-CANADA (2023). "La lutte contre les hypertrucages s'amorce dans le monde." February 3, 2023. Online: <https://ici.radio-canada.ca/nouvelle/1953308/lutte-hypertrucage-deepfake-gouvernement-loi-monde>

SALMON, Felix (2023). "AI will be at the center of the next financial crisis, SEC chair warns." *Axios*, August 12, 2023. Online: <https://www.axios.com/2023/08/12/artificial-intelligent-stock-market-algorithms>

SCASSA, Teresa (2023). "Regulating AI in Canada : A Critical Look at the Proposed Artificial Intelligence and Data Act." *The Canadian Bar Review*. Vol. 101 No. 1. Online: <https://cbr.cba.org/index.php/cbr/article/view/4817/4539>

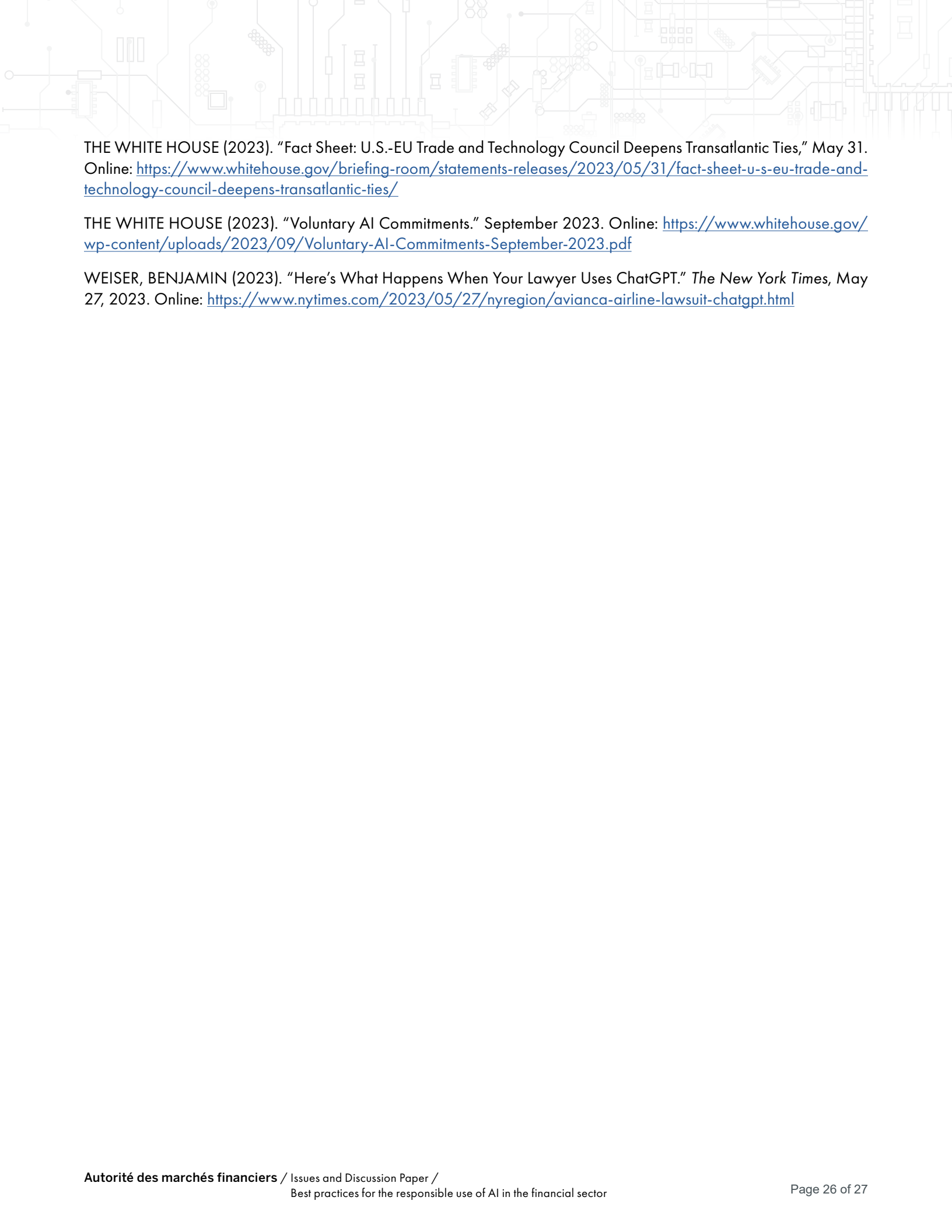
SECURITIES AND EXCHANGE COMMISSION (2023). Conflicts of Interest Associated with the Use of Predictive Data Analytics by Broker-Dealers and Investment Advisers. 17 CFR Parts 240 and 275. Online: <https://www.sec.gov/files/rules/proposed/2023/34-97990.pdf>

SOLAIMAN (Irene), TALAT (Zeeraq) & al. (2023). "Evaluating the Social Impact of Generative AI Systems in Systems and Society." Online: <https://arxiv.org/pdf/2306.05949.pdf>

STATISTICS CANADA. "Responsible use of automated decision systems in the federal government." Online: <https://www.statcan.gc.ca/en/data-science/network/automated-systems>

STRINGER, David (2023). "How AI and Deepfakes are Fueling a New Wave of Cybertheft." *Bloomberg*, August 22, 2023. Online: <https://www.bloomberg.com/news/newsletters/2023-08-22/deepfakes-ai-will-drive-financial-fraud-and-crime-big-take>

THE ALAN TURING INSTITUTE (2023). "The AI Revolution: Opportunities and Challenges for the Finance Sector." September 2023. Online: https://www.turing.ac.uk/sites/default/files/2023-09/full_publication_pdf_0.pdf



THE WHITE HOUSE (2023). "Fact Sheet: U.S.-EU Trade and Technology Council Deepens Transatlantic Ties," May 31. Online: <https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/31/fact-sheet-u-s-eu-trade-and-technology-council-deepens-transatlantic-ties/>

THE WHITE HOUSE (2023). "Voluntary AI Commitments." September 2023. Online: <https://www.whitehouse.gov/wp-content/uploads/2023/09/Voluntary-AI-Commitments-September-2023.pdf>

WEISER, BENJAMIN (2023). "Here's What Happens When Your Lawyer Uses ChatGPT." *The New York Times*, May 27, 2023. Online: <https://www.nytimes.com/2023/05/27/nyregion/avianca-airline-lawsuit-chatgpt.html>

