The Impact of Artificial Intelligence on the Digitalization of Banking Services. Perspectives about Legal Challenges and Liability Issues

Mădălina-Anca CARP[1]
Anne-Marie BRICIU DIACONU[2]

Abstract

As technology advances rapidly, society is nearing a juncture where a genuine reconfiguration of the entire system will become not merely an option, but a necessity. This technological surge has permeated a vast array of fields, notably health, education, justice, and, perhaps most significantly, the banking sector. The impact on each domain underscores a pressing need for legislative adaptation, raising questions about the adequacy of current regulatory frameworks and the role of law in fostering secure, ethical integration of technology in these critical areas.

Over the next decade we will see more changes in the banking Industry than we have witnessed in the past 100 years[3]*. We believe that these changes are significantly influenced by artificial intelligence, which is emerging as a new agent within society and the rule of law. Therefore, an analysis of the impact of this technological phenomenon is a veritable necessity. As a result, based on its impact, particularly on the legal field, in the following paper, we will analyse the impact of artificial intelligence on the banking sector and the legal challenges associated with it.*

Keywords: *Banking Law, Artificial Intelligence, Liability, Decision making, Ethical Challenges.*

1. Introduction

Digitalization is a crucial factor in the evolution of the banking sector, having a significant impact on the way financial services are offered and utilized by consumers. In recent decades, the banking sector has undergone rapid transformation, shifting from traditional methods of operation, characterized by the physical presence of branches, to modern digital solutions that enhance accessibility and operational efficiency. In Europe, this trend has been supported by the development and adaptation of innovative financial technologies (FinTech)[4], which

[1] Student, Faculty of Law, Bucharest University of Economic Studies, carpmadalina22 @stud.ase.ro

[2] Student, Faculty of Law, Bucharest University of Economic Studies, briciudiaconuanne22 @stud.ase.ro

[3] KPMG, *The future of digital banking*, Ed. Can, (Australia, 2024), p. 5.

[4] The term FinTech covers the entire scope of services and products traditionally provided by the financial services industry and has become a common way to describe any business that uses technology to conduct financial transactions. See Felix I. Lessambo, *Fintech Regulation and Supervision Challenges within the Banking Industry: A Comparative Study*

facilitates the creation of a more competitive and customer-oriented banking landscape.

Alongside these developments, digitalization is subject to a rigorous legislative framework imposed by the European Union. A key example in this context is the Payment Services Directive (PSD2)[5], adopted in 2015 and implemented in national legislation through Law no. 209/2019[6]. The central objective of this directive is to modernize the payments market by creating opportunities for FinTech service providers and by establishing strict standards for security, transparency, and consumer protection. These regulations are essential to ensure a safe and fair operating framework in the context of accelerated digitalization.

In this context, a crucial element of digital transformation is the use of artificial intelligence. According to an European survey[7] the awareness of AI is almost universal with 78% of enterprises stating that they know what the term Artificial Intelligence is, and also, of specific AI technologies is consistently high ranging between 87% for anomaly detection and 96% of enterprises aware of autonomous machines.

Artificial intelligence hasn't started making its presence felt in our contemporary society, but it started over a century ago, when personalities like Alan Turing imagined computer systems capable of logical reasoning, concepts rather speculative at the time. Essential developments in recent decades have led to an explosion of AI applications, making it an essential part of the global technological infrastructure. Two notorious Stanford professors stated, back in the 80s, that Artificial Intelligence (AI) is a branch of computer science focused on creating intelligent computer systems - systems that demonstrate traits we typically associate with human intelligence, such as understanding language, learning, reasoning, solving problems, and so on.[8] Essentially, Artificial intelligence involves simulating human intelligence in machines programmed to think and act like humans. The term can also be applied to any machine demonstrating characteristics typically associated with the human mind, such as learning and problem solving. [9] In the banking sector,

within the G-20, Ed. Palgrave Macmillan, (Fordham University, New Britain, CT, USA, 2023), p. 1.

[5] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, OJUE, L 337, 23.12.2025, pp. 35-127.

[6] Regarding payment services and for the modification of some normative acts, Of. M. nr. 913 / 2019.

[7] European Commission, *European enterprises survey on the use of technologies based on artificial intelligence, (*Belgium, 2019).

[8] For more details see Barr, A., & Feigenbaum, E. A. (Eds.). T*he Handbook of Artificial Intelligence,* Vol. 1, Ed. Stanford University, (1981), p. 3.

[9] For more details see Felix I. Lessambo, *Ibidem*, p. 307.

AI is implemented to manage and analyse large volumes of data, automate processes, and enhance operational decision-making.

However, the implementation of innovative technologies like artificial intelligence (AI) introduces new challenges related to regulatory compliance, particularly regarding the management of risks associated with cybersecurity and personal data protection. For example, banks utilize AI technology to develop advanced fraud detection systems that analyse transactions in real time to identify suspicious behaviours. Yet, the challenges of managing false alerts and ensuring a positive customer experience are becoming increasingly significant.

Thus, the integration of AI technologies in the banking sector not only has the potential to transform bank operations but also raises fundamental questions about legal responsibility and compliance with existing regulations.

2. The Role of Artificial Intelligence in the Digitization of Banking Services

In this section, we rerun the definition of artificial intelligence (AI), considering that it can be approached from two perspectives: (i) as a field of research and (ii) as an intelligent agent.

(i) The first perspective defines AI as a scientific and technological field dedicated to the development of systems and algorithms capable of imitating and replicating human abilities in thinking, understanding, and decision-making. Here, AI is understood as a theoretical process—a scientific rationale within a doctrinal framework.

(ii) The second perspective presents AI as a system capable of interacting with its environment, learning autonomously based on received data, and making decisions through algorithms that simulate human reasoning. In this view, AI is seen as an intelligent agent that develops with accumulated experience in a manner comparable to human adaptation.

These two perspectives suggest that AI is a broad concept, challenging to define concretely, and one that raises numerous questions. AI has become a cornerstone of contemporary technological innovation, significantly influencing society's trajectory. Consequently, understanding how AI functions is crucial from a legal perspective, particularly considering that, in the future, the notion of an agent might be confused with that of a person. In its milestone 2017, the Parliament called on the Commission, with the resolution on Civil Law Rules on Robotics, to explore the possibility of granting them a specific status, close to the notion of *legal personality*, so that they can be held responsible for any damage they may cause.[10] However, this is a more controversial subject, because of what it could supposedly give them this status to the traditional policies. Experts argued that it would need to

[10] European Parliament, EPRS, *Briefing. EU legislation in Progress. Artificial intelligence liability directive,* 2023, p. 10.

adapt traditional policies on strict liability and fault-based liability to the context of AI services and products and this approach is likely to fall short.[11]

But where do we find this technology in banking law? Artificial intelligence has increasingly penetrated the banking sector, becoming integral in areas such as compliance, fraud detection, risk management, and customer service. Banking law intersects with AI technology particularly through regulations on data protection, cybersecurity, and operational transparency. Moreover, the future financial customer experience will be affected by AI. This will be most noticeable through the delivery of mass personalization and assisting customers as they overcome challenges. Robots and automated technologies are increasingly used in the banking sector for various functions, such as: (i) customer assistance – chatbot robots that provide quick answers to customer inquiries, (ii) data analysis – robots that analyse customer behaviour and provide personalized recommendations, (iii) credit decisions – algorithms that assess credit applications based on customers' financial data.

The cornerstone of an AI is its reasoning module, which analyzes sensor data and translates it into actionable decisions aligned with a specific goal. This means that the data collected by the sensors need to be transformed into information that the reasoning module can understand.[12]

Whether it involves understanding and solving problems or reasoning and decision-making, the foundation of these functions lies in a specific learning process, which varies depending on the type of activity involved. In the banking field, learning is based on neural networks—mathematical models inspired by the functioning of the human brain, playing a key role in machine learning and deep learning. Essentially, these networks operate similarly to the human brain. Human brains and *artificial neural networks (ANNs)* share similarities in their learning methods, though their differences are substantial. In the brain, biological neurons are connected through synapses that adapt based on experiences, in a process known as plasticity. In ANNs, neurons are mathematical nodes connected by weights that adjust according to errors encountered during training.

The human brain's learning process is based on associative learning and the strengthening of synapses according to personal experiences, a highly complex mechanism. Conversely, ANNs use specific algorithms, such as supervised learning, in which network weight adjustments are based on prediction errors. Thus, while ANNs mimic brain function through their architecture, the adaptability and complexity of learning remain superior in the human brain. These artificial networks can perform specific tasks with a high degree of accuracy, but human learning remains more flexible and deeply influenced by sensory context.

To illustrate these latter aspects and examine how human decision-making process functions compared to that of robots, let us consider a historical example –

---

[11] See, for instance, U. Pagallo, *The way ahead on AI liability issues - Will the developing UE liability framework for regulating AI prove sufficient?,* https://www.adalovelace institute.org/blog/the-way-ahead-on-ai-liability/, 2022, accesed at 08 November 2024.

[12] The report of December 18, 2019, by the High-Level Expert Group on Artificial Intelligence, *A definition of AI: Main Capabilities and Disciplines,* p. 3.

general MacArthur[13], who amid a state of transcendence and imbalance at the political, economic, and social levels, alongside the onset of the Korean War, found himself at a crossroads regarding the adoption of security and preventive measures. The proposed measures risked worsening the situation, prompting the team to seek an objective perspective and ultimately decide to transfer responsibility to a device called the "Electric Brain." This oracle-like machine was fed with the necessary data to make decisions, considering factors such as the characteristics of a potential war, consequences, profitability, etc.—critical aspects in such situations. Thus, with the data provided, the Electric Brain managed to reach an appropriate decision, which, of course, remained subject to human approval. [14] As a result, we can affirm that, if data is correctly and comprehensively provided, ANNs might be capable of addressing issues in an objective and accurate manner.

However, could we then claim that an artificial agent possesses reason? This is a frequently debated issue among researchers and others, largely remaining a theoretical matter rooted in dogmatic and philosophical frameworks. In the vast legal field, judgment is of paramount importance. Judgment is the faculty of applying rules—specifically, the ability to discern whether something falls under a given rule *(casus datae legis).*[15] Consequently, does the artificial agent, through an accumulation of knowledge in a predominantly empirical manner, possess—or stand in the hypothesis of possessing—this faculty? Finding an answer to these questions holds significant relevance in determining the legal status of this artificial agent.

3. Ethical Challenges in Artificial Intelligence

Thanks to remarkable technological advancements, modern agents can now perform tasks once considered uniquely human - such as granting loans, creating a stock portfolio, etc., Moreover, the integration of autonomous and cognitive capabilities has transformed these agents into entities that actively interact with and significantly influence their environments. Therefore, in such a context, the legal responsibility arising from those “robots” 'harmful action becomes a crucial issue.[16]

---

[13] Douglas MacArthur (born January 26, 1880, Little Rock, Arkansas, U.S.—died April 5, 1964, Washington, D.C.) was a U.S. general who commanded the Southwest Pacific Theatre in World War II, administered postwar Japanduring the Allied occupation that followed, and led United Nations forces during the first nine months of the Korean War. See James, D. Clayton, *Douglas MacArthur,* Encyclopedia Britannica, 22 Oct. 2024, https://www.britannica.com/biography/Douglas-MacArthur, accessed 09 November 2024.

[14] G. Anders, *Obsolescența omului: despre suflet în epoca celei de-a doua revoluții industriale,* Ed. Tact, Cluj-Napoca, 2013, pp. 98-99.

[15] I. Kant, *Critica rațiunii pure,* Ed. Univers Enciclopedic Gold, Gogito, 3rd edition, Bucharest, 2009, p. 164.

[16] European Parliament Committee on Legal Affairs, *Civil Law Rules on Robotics (2015/2103 (NIL)), (*Brussels, 2016), p. 5.

Artificial intelligence presents a series of potential risks, including opaque decision-making processes, biases such as gender discrimination, intrusions into privacy, and misuse for criminal purposes.[17] Thus, given the rapid growth of AI and the significant impact it can have on society, it is essential to ensure a solid legal foundation for the legal relationships arising from its activities. Therefore, the use of this technology may create tensions or risks in fundamental areas, such as human protection, privacy, integrity, dignity, autonomy, or data protection.

Referring to the points made in the previous section, we emphasize that a large portion of algorithms (based on deep learning) are not well understood by specialists, particularly regarding the mechanisms by which they make decisions. AI techniques such as *decision-tree*[18] induction offer *built-in explanations*[19] but are generally less accurate. Therefore, researchers need to develop systems that are both transparent and inherently capable of explaining the reasoning behind their results to users.[20] In this regard, we do not believe that the responsible party should be considered entirely as the one who programmed or coded the software that caused the damage.

We agree with the idea that once the responsible parties are identified, their liability should depend on the amount of instruction given to the robot and its level of autonomy. This means that as a robot becomes more capable of learning or operating independently, the responsibility of other parties should decrease. On the other hand, the longer the robot has been trained, the greater the responsibility of its "trainer" should be.[21] In this sense, we find Regulation (EU) 2021/1232, art. 10,[22] which protects the person of the producer from possible errors of the intelligent agent stating that if harm or damage results from both an AI-driven physical or virtual activity, device, or process and the actions of the affected person or someone for whom the affected person is responsible, the operator's liability under this Regulation will be reduced accordingly. The operator will not be held liable if the harm or damage is entirely caused by the actions of the affected person or the person they are responsible for.

---

[17] European Commission, *White paper: On Artificial Intelligence - A European approach to excellence and trust,* Brussels, 19.2.2020 COM (2020) 65 final, p. 1.

[18] Quinlan, J. R. (1986). *Induction of Decision Trees. Machine Learning, 1(1)*, 81-106, available at https://link.springer.com/article/10.1007/BF00116251, accessed at 10 November 2024.

[19] *Ibidem*.

[20] Networking and Information Technology Research and Development Subcommittee, *The federal big data research and development strategic plan,* University of Nebraska, (Lincoln, 2016), p. 28.

[21] European Parliament Committee on Legal Affairs (2016), *ibidem*, p. 11.

[22] Regulation (EU) 2021/1232 of the European Parliament and Council, *on Liability for the Operation of Artificial Intelligence Systems*, OJEU, series L, nº 274/41.

3.1 Legal Responsibility for AI-Based Decisions in the Banking Sector: Software Producer's Liability vs. Bank's Liability

The use of artificial intelligence (AI) systems in the banking sector has increased significantly in recent years, and with this development come critical questions regarding legal responsibility in cases of automated decisions. It is essential to analyse who holds responsibility when AI systems generate errors, such as denying a loan based on discriminatory or inaccurate criteria. These issues not only affect consumers but also raise concerns about compliance with existing legislation and consumer protection.

A. Liability of the software producer

Software developers who create AI algorithms hold significant responsibility regarding their design and implementation. This responsibility includes the obligation to create software that functions correctly, is safe, and does not discriminate against users. If an algorithm has defects or is built on inadequate databases, leading to errors in automated decisions, the developer may be held liable for the damages caused.[23]

For example, if credit assessment software uses a dataset containing errors or historical biases, the result could be a system that unfairly discriminates against certain demographic groups. In such cases, individuals affected by this discrimination could seek compensation, arguing that the developer failed to meet quality and ethical standards in the product creation process. Consequently, there is significant pressure on software developers to conduct rigorous testing and audits of algorithms before implementation to minimize liability risks.

Moreover, beyond direct responsibility to users, software developers must also collaborate with financial institutions to ensure adequate transparency in how algorithms function. This includes providing detailed documentation explaining how automated decisions are generated. Implementing ethical and quality standards in software development is essential for maintaining public trust in the use of AI technologies in the financial sector.

B. Liability of the Bank

On the other hand, banks that use these technologies have their own responsibilities. Even if algorithms are developed by third parties, banks are required to ensure that these systems are implemented correctly and that the data used is not only accurate but also ethical. This responsibility extends beyond the mere use of technology, involving an ongoing assessment of how automated decisions affect customers. Banks must be aware of the impact that automated decisions have on their clients, especially in cases where these decisions could have significant financial

[23] European Commission, *Proposal for a Regulation Laying Down Harmonized Rules on Artificial Intelligence* (Artificial Intelligence Act), COM (2021) 206 final 2021/0106(COD), (Brussels, 2021).

consequences. Also, due to increasing availability of data and technological progress, it is widely discussed that financial market participants (will) use Artificial Intelligence (AI) and Machine Learning (ML) in the provision of financial services and investment activities. [24] Specifically for the European Union (EU) and similarly to the above, the Commission's Expert Group on Regulatory Obstacles to Financial Innovation (ROFIEG) in 2019 concluded that AI and ML solutions are being increasingly applied in the financial sector, highlighting, inter alia, their use in portfolio management.[25]

From a normative perspective, therefore, two building blocks of EU financial markets law that regulates this area: the Markets in Financial Instruments Directive II (MiFID II)[26] and the Alternative Investment Fund Managers Directive (AIFMD)[27].

To better illustrate this dynamic, let's consider a hypothetical scenario where an investment firm uses algorithmic trading to make financial decisions for its clients. Whereas the AI system denies a transaction based on incorrect criteria and therefor the client loses a profitable opportunity, who is responsible for? Art. 17 (6) MiFID II is of a great relevance in this cases stating that an investment firm functioning as a general clearing member for others must implement effective systems and controls to ensure that clearing services are provided exclusively to individuals who meet specific suitability criteria, while also imposing the necessary requirements on those individuals to mitigate potential risks to both the firm and the overall market. Therefore, looking closer at Art. 17 (2) MiFID II contains arguably three distinctive elements: firstly, an initial notification duty and secondly (potentially) ongoing reporting obligations closely linked to catch-all supervisory powers to "request further information", which can be seen a third element.[28]

---

[24] L. Böffel, J. Schürger, *Digitalisation, Sustainability, and the Banking and Capital Markets Union: Thoughts on Current Issues of EU Financial Regulation,* Ed. Palgrave Macmillan, (Germany, 2022), p. 99

[25] Cf., ROFIEG, *'30 Recommendations on Regulation, Innovation and Finance—Final Report to the European Commission*', December 2019, 38, available at https://ec.europa.eu/info/files/191113, accessed at 08 November 2024. On the benefits and risks of AI-use in robo-advice also already Wolf-Georg Ringe and Christopher Ruof, *Robo Advice: Legal and Regulatory Challenges,* in Iris H.-Y. Chiu and Gudula Deipenbrock (eds), *Routledge Handbook of Financial Technology and Law* (Routledge, 2021), 193, 204 et seq.

[26] Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU, OJUE, series L, nº 173/349.

[27] Directive 2011/61/EU of the European Parliament and of the Council of 8 June 2011 on Alternative Investment Fund Managers and amending Directives 2003/41/EC and 2009/65/EC and Regulations (EC) Nº 1060/2009 and (EU) Nº 1095/2010, OJUE, series L, nº 174/1.

[28] L. Böffel, J. Schürger, *ibidem*, p. 115.

In such a case, **who is responsible?** If the transaction denial is due to coding errors or incomplete datasets, the software developer could be held accountable. However, the bank also has a duty to validate the information and ensure that the financial assessment process is accurate. If a client contests the decision, the bank must provide a clear explanation and a mechanism for reviewing the decision; otherwise, it risks being accused of unfair, inadequate, or discriminatory practices.

This distinction between the responsibility of the software developer and that of the bank highlights the complexity of the issue. As AI technologies continue to develop and become integrated into banking processes, it is essential for both parties to understand their responsibilities and to collaborate in creating a safe and fair operating framework. Regulations in this field, therefore, must evolve to clarify these responsibilities and to protect consumers from potential abuses or errors in the use of AI systems.

3.2 Contractual Liability: How banks can legally protect themselves through contracts with AI software developers and clients

To clarify this subsection, we shall define the term "*artificial intelligence system"*. Cf art. 2 CETS 225[29], it refers to a system driven by machines that, in pursuit of specific or implied goals, processes the input it receives to produce outputs such as predictions, content, recommendations, or decisions, which can affect either physical or digital environments. These AI systems differ in their degree of autonomy and adaptability once they are put into operation.

Thus, AI is considered an agent capable of acting based on data provided by its operator. One might argue that the operator (for example, the software developer) bears responsibility for the data supplied to the intelligent machine – the robot – and, *a fortiori*, is also liable for any damages potentially arising from its fault. The CETS 224[30] remains somewhat vague in this respect; see Article 12, which merely stipulates that signatory states must adopt appropriate measures to promote trust in this emerging technology.

In light of the European Parliament's Resolution on the civil liability regime for artificial intelligence[31],AI should be treated as a *product* under the Product Liability Directive, with software developers being regarded as *producer*.[32]. In this

[29] Council of Europe, *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law,* (Vilnius, 2024).

[30] *Ibidem*.

[31] European Parliament resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence (2020/2014(INL)), P9_TA (2020) 0276, OJEU, series C, nº 404/107.

[32] European Parliament resolution, *Ibidem*, pct. 8.
Directive 85/374/EEC on the approximation of the laws, regulation and administrative provision of the Member States concerning liability for defective products, OJEU, series L, nº 210/19, art. 3.

context, they would be held liable for any harm or damages caused, directly or indirectly, by AI systems.

However, this approach is also insufficient, as it presents significant challenges in proving the fault of the AI system or, by extension, the liability of the developer, within the current legal framework. Moreover, recent societal changes have shown that basing civil liability exclusively on the fault or negligence of the liable party is no longer comprehensive enough. This is why, following doctrinal discussions, three groups of theories or concepts have emerged: the subjective theory, objective theories, and mixed theories.[33]

In this context, civil liability is defined by civil fault, referring to the unlawful act of a person that causes harm to another, thus generating the obligation to repair the damages caused. According to Article 1349 of the Romanian Civil Code, "any person has the duty to comply with the rules of conduct imposed by law or local custom and not to harm, through their actions or inactions, the rights or legitimate interests of others."[34] Additionally, "anyone who, having discernment, violates this duty is liable for all damages caused and is obliged to repair them in full."[35] This means that, to establish civil liability, it is necessary to demonstrate the existence of fault, according to Article 1353, which states that "anyone who causes harm through the very exercise of their rights is not obliged to repair it, except in cases where the right is exercised abusively."[36]

The limitations of this liability are stipulated in Article 1354, which provides that "the victim cannot obtain compensation for the damage caused by a person who provided assistance in a disinterested manner or by the thing, animal, or building used gratuitously unless they prove the intention or serious fault of the person who, according to the law, would have been called to respond."[37] This aspect emphasizes the difficulty of obtaining compensation in cases where damages are caused by the actions or autonomous decisions of artificial intelligence, as it is necessary to identify a specific fault of the operator or developer.

However, with respect to the legislation in this field at the EU level, various authors warn about the lack of clarity in some key notions that will have to be applied to national law and will depend upon national judges' interpretations risks, like *fault, duty of care* or *user*. In consequence, this may affect legal certainty and cause fragmentation across the European Union depending on national tort law tradition.[38]

---

[33] L. Pop, I.F. Popa, S.I. Vidu, *Drept civil. Obligațiile,* Universul Juridic Publishing House, 2nd edition, (Bucharest, 2020), p. 329.

[34] See art. 1349 din *Legea 287 / 2009 privind Codul Civil*, M.O. Part I, no. 409 of June 10, (2011), with subsequent amendments and additions.

[35] *Ibidem*.

[36] See art. 1.353, *ibidem*.

[37] See art. 1.354, *ibidem*.

[38] European Parliament, EPRS, *ibidem,* p. 9.

Of relevance are the objective theories[39], which arose with the accelerated pace of technological development, starting as early as the late 19th century. These theories assert that as the cause of harm increasingly stems directly from things and energies—typically, technology—the cause itself becomes anonymous, making it difficult, if not impossible, to link it to the action or inaction of any individual. Moreover, even when a responsible party can be identified, presuming their fault is often contrary to reality, profoundly unjust, and overly formal[40], especially given the growing complexity and autonomy of modern technology.

The European Parliament, through the aforementioned resolution, asserts that the operator should be held liable because they control a risk associated with the AI system, and due to the complexity and connectivity of the AI system, the operator will often be the first visible point of contact for the affected individual.[41] We partially agree with this assertion, while also believing that the operator's liability should be established in proportion to the level of autonomy gained by the AI system as a result of the specific learning process.

4. Conclusions

Considering the above, the discussion regarding responsibility in the field of artificial intelligence is vast and strongly influenced by philosophical aspects, given the lack of specificity in the legal acts presented in this regard. Thus, although the legislator has established that liability is a matter closely tied to positive law, we observe that there is a strong moral foundation for extending responsibility to seemingly impersonal acts as well.[42] A strong argument in this regard is the fact that a person is held responsible for damage caused to another person through both actions and omissions, as well as through the things they have in their care or under their protection. This principle extends the notion of responsibility to situations where the harm is caused indirectly, even in the absence of direct personal involvement, thus creating a broader framework for accountability.[43]

As a result, refining fundamental principles such as proportionality, transparency, and others in relation to the degree of autonomy of intelligent agents within European regulations is a first step toward creating a symbiosis between

---

[39] V.G. Viney, *Traité de droit civil. Introduction à la responsabilité.* L.G.D.J., (Paris, 2008), pp. 26-28, 107-127.

[40] L. Pop, I.F. Popa, S.I. Vidu, ibidem, p. 330.

[41] European Parliament, P9_TA (2020) 0276, *Civil liability regime for artificial intelligence,* European Parliament resolution of 20 October 2020 *with recommendations to the Commission on a civil liability regime for artificial intelligence (2020/2014(INL)),* JOUE, series C, nº 404/107, p.7.

[42] For more details see F.A. Baias, E. Chelaru, R. Constantinovici, I. Macovei, *Noul Cod Civil. Comentariu pe articole,* 3rd edition, (2021).

[43] See art. 1.327-1.359, *Codul Civil și Legea de punere în aplicare,* Ed. Hamangiu Publishing House, (2022), p. 298.

society and the emerging AI technology. This technological revolution could thus fully benefit humanity while allowing the technology to advance naturally.

However, it is important to note that artificial intelligence brings new risks to the banking sector, such as a lack of transparency and cybersecurity threats, which are not fully addressed by current legislation. To protect consumers, additional legislative measures are needed: transparency of AI algorithms, periodic auditing of models used, and the introduction of strict ethical standards—issues that will be discussed in the next section. Implementing such measures would create a balance between protection and innovation, ensuring a more responsible use of AI in the banking sector.

Lege ferenda

Given the challenges and risks associated with AI, developing a legislative framework that directly addresses these issues and provides clients with clear rights and protections when interacting with AI-driven decisions is essential. This represents a critical first step toward a future where automated decision-making systems operate responsibly and transparently.

In this context, current legislation requires adaptation to ensure transparency, accountability, and, importantly, the protection of individuals' fundamental rights as users. Particular emphasis should be placed on financial institutions that employ AI in their decision-making processes. We believe that additional regulations are necessary for these institutions to establish a framework that is as transparent and robust as possible, guaranteeing users' rights.

In this context, we propose introducing an audibility obligation for financial institutions that use artificial intelligence as a measure to ensure transparency and protect end-user rights. This obligation would require that institutions ensure the explainability of automated decisions and implement a mechanism for reviewing AI-driven decisions at the institutional level. So, in anticipation of a future revision of MiFID II, we propose the addition of the following text for article 4, pct. 1:

lit. e): if the firm uses artificial intelligence to conduct its business activities, its decision-making system must be audited by one or more persons empowered, under national law, to audit accounts.

Such an obligation would contribute to forming a comprehensive perspective on the functioning of these systems and would establish the necessary framework for reviewing automated decisions in the event of errors, by implementing concrete corrective measures. This regulation would ensure transparency in decision-making processes and protect consumer rights by preventing automatic errors and discrimination.

In line with this approach, we believe that a necessary first step towards cohesion and a fair distribution of responsibility would be to establish a legal status for the 'artificial agent' in legal relations, so that it may be considered a limited legal

entity. Such regulation would clarify the role and responsibility of artificial agents, providing a legal basis for managing their use in financial institutions and beyond.

These measures will support the responsible integration of AI technologies, instilling user confidence and ensuring a safer, more transparent financial system. Thus, by establishing clear regulations on the explainability of automated decisions, setting a legal status for artificial agents, and implementing mechanisms for review and auditability, the framework will help prevent automatic errors and discrimination, striking a balance between innovation and consumer protection

In closing, regarding the evolution of EU legislation and banks' preparedness for AI technology, the European Union must implement additional regulations for AI use in the banking sector, focusing on the clarity of automated decisions and data security. At the same time, banks should prepare for these requirements by investing in staff training and developing internal policies for ethics and compliance. Over time, adapting to new standards will facilitate the responsible integration of AI, strengthening consumer trust while adhering to EU regulations.

Bibliography

Legislation

1. Directive 2011/61/EU of the European Parliament and of the Council of 8 June 2011 on *Alternative Investment Fund Managers and amending Directives 2003/41/EC and 2009/65/EC and Regulations (EC) No 1060/2009 and (EU) No 1095/2010*, OJEU, series L, nº 174/1.
2. Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 *on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU*, OJEU, series L, nº 173/349.
3. Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 *on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC,* OJEU, series L, nº 337 / 2015.
4. Directive 85/374/EEC *on the approximation of the laws, regulation and administrative provision of the Member States concerning liability for defective products,* OJEU, series L, nº 210/19.
5. Regulation (EU) 2021/1232 of the European Parliament and Council, *on Liability for the Operation of Artificial Intelligence Systems*, OJEU, series L, nº 274/41.
6. Law nº 287 / 2009 *on the Civil Code*, M.Of. Part I, No. 409 of June 10, 2011.
7. Law nº 209/2019 regarding payment services and for the modification of some normative acts, Of. M. nr. 913 / 2019.

National doctrine

1. *Codul Civil și Legea de punere în aplicare*, Ed. Hamangiu Publishing House, (2022).
2. F.A. Baias, E. Chelaru, R. Constantinovici, I. Macovei, *Noul Cod Civil. Comentariu pe articole*, 3rd edition, (2021).
3. G. Anders, *Obsolescența omului: despre suflet în epoca celei de-a doua revoluții industriale*, Ed. Tact, (Cluj-Napoca, 2013).
4. L. Pop, I.F. Popa, S.I. Vidu, *Drept civil. Obligațiile*, Universul Juridic Publishing House, 2nd edition, (Bucharest, 2020).

Foreign doctrine

1. Barr, A., & Feigenbaum, E. A. (Eds.). *The Handbook of Artificial Intelligence*, Vol. 1, Ed. Stanford University, (1981).
2. I. Kant, *Critica rațiunii pure*, Ed. Univers Enciclopedic Gold, Gogito, 3rd edition, (Bucharest, 2009).
3. Felix I. Lessambo, *Fintech Regulation and Supervision Challenges within the Banking Industry: A Comparative Study within the G-20*, Ed. Palgrave Macmillan, Fordham University, New Britain, CT, (USA, 2023).
5. James, D. Clayton, *Douglas MacArthur*, Encyclopedia Britannica, 22 Oct. 2024, https://www.britannica.com/biography/Douglas-MacArthur, accessed 09 November 2024.
6. L. Böffel, J. Schürger, *Digitalisation, Sustainability, and the Banking and Capital Markets Union: Thoughts on Current Issues of EU Financial Regulation*, Ed. Palgrave Macmillan, (Germany, 2022).
7. Networking and Information Technology Research and Development Subcommittee, *The federal big data research and development strategic plan,* University of Nebraska, (Lincoln, 2016),
8. Quinlan, J. R. (1986). *Induction of Decision Trees. Machine Learning, 1(1)*, 81-106. Available at https://link.springer.com/article/10.1007/BF00116251, accessed at 10 November 2024.
9. U. Pagallo, *The way ahead on AI liability issues - Will the developing UE liability framework for regulating AI prove sufficient?*, https://www.adalovelaceinstitute.org/blog/the-way-ahead-on-ai-liability/, (2022) accessed at 08 November 2024.
10. V.G. Viney, *Traité de droit civil. Introduction à la responsabilité. L.G.D.J.*, (Paris, 2008).
11. Wolf-Georg Ringe and Christopher Ruof, *'Robo Advice: Legal and Regulatory Challenges*' in Iris H.-Y. Chiu and Gudula Deipenbrock (eds), *Routledge Handbook of Financial Technology and Law* (Routledge 2021).

Institutions' official reports

1. Council of Europe, *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law*, (Vilnius, 2024).
2. European Commission, *European enterprises survey on the use of technologies based on artificial intelligence*, (Belgium, 2019).
3. European Commission, *Proposal for a Regulation Laying Down Harmonized Rules on Artificial Intelligence* (Artificial Intelligence Act), COM (2021) 206 final 2021/0106(COD), (Brussels, 2021).
4. European Commission, *White paper: On Artificial Intelligence - A European approach to excellence and trus*t, COM (2020) 65 final, (Brussels, 2020)
5. European Commission, High-Level Expert Group on Artificial Intelligence, *A definition of AI: Main Capabilities and Disciplines*, (Brussels, 2018).
6. *Down Harmonized Rules on Artificial Intelligence* (Artificial Intelligence Act), COM (2021) 206 final, 2021/0106 (COD), (Brussels, 2021).
7. European Parliament Committee on Legal Affairs, *Civil Law Rules on Robotics (2015/2103 (NIL)), (*Brussels, 2016).
8. European Parliament, P9_TA (2020) 0276, *Civil liability regime for artificial intelligence,* European Parliament resolution of 20 October 2020 *with recommendations to the Commission on a civil liability regime for artificial intelligence (2020/2014(INL)),* JOUE, series C, no 404/107.
9. European Parliament, P9_TA (2020) 0276, *Civil liability regime for artificial intelligence*, European Parliament resolution of 20 October 2020 with recommendations to the *Commission on a civil liability regime for artificial intelligence (2020/2014(INL)*).
10. European Parliament, EPRS, *Briefing. EU legislation in Progress. Artificial intelligence liability directive*, (2023).

Other sources

1. European Commission, ROFIEG, *30 Recommendations on Regulation, Innovation and Finance—Final Report to the European Commission'*, (Brussels, 2019), available at https://europa.eu/!yu87Xf, accessed at 08 November 2024.
2. KPMG, *The future of digital banking*, Ed. Can, (Australia, 2024).

Web sources

1. Site EU: https://european-union.europa.eu/index_en
2. Site OJEU: https://eur-lex.europa.eu/oj/direct-access.html?locale=en