Ethical Artificial Intelligence, Fintech and Data Protection: A Path Forward for Training in Europe

Maria Moloney[1*], Ioana-Florina Coita[2], Eleftheria Paschalidou[3], Ekaterina Svetlova[4], Codruta Mare[5*], Liana Stanca[6], Galena Pisoni[7], Karolina Bolesta[8], Olivija Filipovska[9], Valerio Poti[1], Cal Muckley[1], Barbara Będowska-Sójka[10], Joerg Osterrieder[11], Veni Arakelian[12]

[1]University College Dublin, Belfield, Dublin 4, Ireland

[2]University of Oradea - Faculty of Economic Sciences, Oradea, Romania

[3] School of Economics, Aristotle University of Thessaloniki, GR 54124, Thessaloniki, Greece

[4]Department of High-Tech Business and Entrepreneurship, University of Twente, Drienerlolaan 5, 7522 NB Enschede, Netherlands

[5]Dep. of Statistics, Forecasts, Mathematics, Faculty of Economics and Business Administration, and the Interdisciplinary Centre for Data Science, Babes-Bolyai University, Cluj-Napoca, Romania

[6]Dep. of Business Information Systems, Faculty of Economics and Business Administration, and the Interdisciplinary Centre for Data Science, Babes-Bolyai University, Cluj-Napoca, Romania

[7]Université Cote d'Azur, Polytech Nice Sophia, Campus ShopiaTech, France SSRN 6266394

[8] Warsaw School of Economics (SGH) - Department of Economics I

[9]Komercijalna Banka AD Skopje, Skopje, Republic of North Macedonia

[10]Poznań University of Economics and Business in Poland, Department of Econometrics, Poznań, Poland

[11]Department of High-Tech Business and Entrepreneurship,University of Twente, Drienerlolaan 5, 7522 NB Enschede, Netherlands, and Applied Data Science and Finance, Berner Fachhochschule, Brückenstrasse 73, 3005, Bern, Switzerland

[12]Economic Analysis and Investment Strategy, Piraeus Bank, Greece, and UCL Center for Blockchain Technologies, UK

*corresponding authors: maria.moloney@ucd.ie, codruta.mare@ubbcluj.ro , codruta.mare@econ.ubbcluj.ro

Abstract

Artificial Intelligence (AI) systems process massive quantities of data. A lot of this data is related to *identifiable* individuals and is what we call personal data under the European Union (EU) General Data Protection Regulation (GDPR). To process such data legally, organisations that develop or deploy AI systems in Europe must understand their regulatory obligations under the GDPR. This paper examines the increasing need for comprehensive data protection training in Europe, given the rapidly evolving landscape of Artificial Intelligence (AI) and the potential harm these systems can cause to individuals and society at large. By way of survey, the paper examines the current level of data protection knowledge among academics and professionals in the field of Finance who either use or develop AI systems on a regular basis. The results of the survey support the need for increasing and emphasising training in data protection for this cohort.

The paper underscores the critical importance of equipping Finance academics and professionals with robust data protection and ethical training so our leaders of tomorrow will be able to foster responsible AI use, by safely and confidently navigating the intricate interplay between AI systems innovation, and the safeguarding of the public good and human rights.

Keywords: Data Protection, Artificial Intelligence, Privacy, Ethics, Training, European Policy, Data Privacy, Responsible AI

Introduction

The forthcoming EU Artificial Intelligence (AI) Act will be one of the first laws on AI to be passed by a major regulator globally. The approach that the EU has taken with this law is to break down AI applications into four main risk categories. The first risk category is made up of applications that are deemed as unacceptable risk. These will be banned in the EU. The second category of risk is classed as high-risk applications and this category, while not banned, will be subject to specific legal requirements before they will be permitted to be used in the EU. Finally, the last two categories of risk consist of AI that is not high risk and are left generally unregulated by the Act (Laneret, Tielemans, & Zenner, 2022).

During its development, the AI Act has been closely modelled on the General Data Protection Regulation (GDPR), which has been in force across the EU since 2018. The European institutions recognise the wealth of experience already gained during the last six years of enforcing such an ambitious piece of legislation and are clearly trying to minimise confusion and bureaucratic burden by using what has been learned with the GDPR and applying it to the forthcoming AI Act (Laneret, Tielemans, & Zenner, 2022).

It could be argued that the GDPR is the toughest data protection law across the globe currently and is considered by many as the gold standard for privacy regulation worldwide (Mantelero, 2021). Even though the GDPR is technology neutral, there was an awareness from the onset, even during the years of drafting the regulation, that 'automated decision-making' regarding the processing of personal data could pose problems to the rights and freedoms of European citizens. Thus, scattered throughout the GDPR's Acts and recitals are instructions on how to deal with automated decision-making for processing personal data (Laneret, Tielemans, & Zenner, 2022).

In fact, the GDPR, if correctly applied, goes a long way to ensuring that the class of technologies named as Artificial Intelligence remains accountable and transparent when processing personal data. However, with the need for European innovation and digitalisation to keep pace with

the rest of the world, there is a growing tension between the processing of large amounts of data (and often personal data) for AI innovation and safeguarding the rights and freedoms of Europeans by protecting their personal data (Sartor & Lagioia, 2020).

This paper looks to explore those tensions and puts forth some suggestions as to how to ensure European innovation in AI keeps pace with the rest of the world while also complying with one of the most fundamental pieces of legislation Europe currently has, the GDPR. To understand the current level of data protection awareness that exists among developers and users of AI in the financial sector, a survey was conducted over a series of months during the winter of 2022/2023. The aim of the survey was to measure the level of GDPR knowledge and training among academics and industry professionals who work with AI on a regular basis. The results of the survey are presented in the paper. This is followed by a discussion of potential solutions to current challenges in the field.

Artificial Intelligence and EU Citizens: the Wider Picture

Computer systems that possess the ability to carry out activities that, up until now, required human intelligence are known as Artificial Intelligence (AI) systems. Examples of these systems are speech recognition systems, decision-making systems, and natural language processing. By employing algorithms and models to evaluate vast amounts of data to arrive at conclusions or predictions, the developers of these AI systems have sought to build intelligent machines that can reason, learn, and adapt to new circumstances (Mitchell, 1997).

In an attempt to further the research agenda and industrial capacity of Europe, while preserving safety and basic human rights, the EU's approach to AI systems use is centred around promoting quality and trust (European Commission, 2021a) and forms part of a wider, more long-term digital strategy from Europe. Building robust and efficient AI systems requires access to high-quality data, and regulations like the EU Cybersecurity Strategy, Digital Services Act, Digital Markets Act, and Data Governance Act provide the required foundation to ensuring data quality in Europe[1].

Additionally, for Europe to maintain its competitiveness in the global digital economy, it must develop its digital skills base. The goal of the Digital Europe Programme is to provide all Europeans with the digital skills necessary to thrive in the digital economy through investments in education and training, up-skilling and reskilling, partnership with industry, and addressing the gender gap (European Commission, 2021b).

The EU is also funding initiatives like the Digital Europe program that emphasize data protection and privacy in training and education. To close this knowledge gap and ensure that professionals have the abilities necessary to adhere to the most recent data protection laws and safeguard the security and privacy of EU citizens.

On 19 February 2020 the EU Commission adopted its White Paper on Artificial Intelligence entitled “A European approach to excellence and trust” (European Commission, 2020), whose purpose was to set out the policy options to achieve the twin objectives of promoting the uptake of AI and of addressing the risks associated with certain uses of this emerging technology.

In this report, the Commission expressly recognized that *“Europe’s current and future sustainable economic growth and societal well-being increasingly draws on value created by data. AI is one of the most important applications of the data economy”* (European Commission, 2020, p. 1).

[1] https://digital-strategy.ec.europa.eu/en

The strong connection between data (either personal or non-personal) and AI systems is reflected also in the draft AI Act, which expressly sets out that "Union law on the protection of personal data, privacy and the confidentiality of communications applies to personal data processed in connection with the rights and obligations laid down in this Regulation. This Regulation shall not affect Regulations (EU) 2016/679 (the "GDPR"), (EU) 2018/1725, Directives2002/58/EC and (EU) 2016/680" (CEDPO's AI Working Group, 2022).

The European Fintech Industry

It could be argued that in 2022 the European fintech industry was having its heyday with 22% of European unicorns being in the financial sector. European fintech companies raised a total of $22.2 billion, making the fintech industry the most-well funded sector in 2022 (Pun, 2023). Towards the end of 2022, however, there was considerable restructuring and mass layoffs across the technology sector globally. Fintech was not immune. Fintech companies as well as traditional bank that have the most robust business models, which usually rely heavily on AI, have a better chance of survival in this environment (Thomas, 2021).

There is, however, limited scope for human oversight in these AI-first business models. The whole aim of these models is to build algorithms that can learn, and make predictions, from data, i.e. replacing the human aspect in the approach. This means that the algorithm operates dynamically, adapting itself to changes in the data, relying not only on statistics, but also on mathematical optimisation (Agarwal, Singhal, & Thomas, 2021). The whole aim of financial companies using ML and AI is to reduce costs and time by eliminating the intervention of humans in the equation.

The obligations of financial companies under the GDPR are, however, problematic to this situation. Article 22 of the GDPR (European Commission, 2018), requires human oversight when decisions are automated by technology:

'*The data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision*.'

It is not clear whether financial companies are providing for these data protection obligations in their AI-first business models.

In keeping with the ethos of the GDPR, the AI Act, under Art. 10, outlines that the datasets used by the Provider [of the AI technology] in training, validation and testing AI are subject to appropriate data governance standards and must meet high requirements for relevance, representativeness, correctness, and completeness in order to limit the possibility of harmful and discriminatory bias. The principles of data minimisation and of data protection by design and by default, as referred to respectively, in Art. 5(1), point (c) and in Art. 25 of the GDPR shall be applied when developing and using High-Risk Artificial Intelligence (HRAI) systems and during the entire lifecycle of those systems.

In reality, however, the development and training of adaptive AI/ML-enabled devices, having a design based on a self-learning mechanism, can continually change and is developed for the purposes of operating with limited human intervention. For supervised Machine Learning, oversight concerns are somewhat diminished by data-labelling and by the accompanying human input, though inaccurate or inconsistent data-labelling can itself lower product efficacy whilst introducing human biases into the system (Tsang, et al., 2022).

If we consider another industry where AI has been heavily used for some time, the medical industry, we see that the risk to humans from unrestrained AI has been recognised for some time. From the perspective of technology, traditional models of medical device regulatory oversight focus largely on evaluating safety and functional characteristics against pre-defined criteria at a given point of the product lifecycle. Such evaluation should ensure that the marketed devices can be used safely and effectively to protect public health and patient safety. Manufacturers initiate design and manufacturing process changes throughout the product span. Regulators expect that such changes are supported by data generated by incremental R&D efforts for independent regulatory assessment, to ensure that the benefits continue to outweigh the anticipated risks.

In the financial industry, the risk to physical life by unrestrained AI use is arguably not as high as in the medical domain, however, recent examples of unrestrained (with a lack of human oversight) AI use in other essential sectors such as the public sector have shown untold damage to the rights and freedoms of individuals. A recent example is the Dutch Child Benefit scandal. On 25 May 2022, the Dutch government publicly admitted for the first time that institutional racism on the part of the Dutch Tax and Customs Administration was the root cause of the Dutch childcare benefit scandal. This scandal led to the resignation of the Dutch government in 2021[2].

For these reasons, many regulatory authorities have recognised that even the rigorous paradigm of medical device regulation may no longer be adequate to control AI/ML technologies, which have the potential to adapt and optimise device performance in real time. The highly iterative, autonomous, and adaptive nature of these tools requires a new, total product lifecycle regulatory approach ("TPLA") that facilitates a rapid cycle of product improvement and allows these devices to continually improve, while providing effective safeguards against deterioration of the performance characteristics. Some advocate for the TPLA to include a continuous assurance protocol whereby the product undergoes continual (or frequent periodic) monitoring and review. Even with a continuous assurance protocol in place, the fundamental regulatory question is how and when self-developing devices would require a new premarket review or conformity assessment (Tsang, et al., 2022).

To add to this already complex landscape, there is vigorous debate on the one hand between the need to maintain this accountability and transparency in AI systems through human-oversight, while, on the other hand, to ensure they are sufficiently robust to futureproof the financial industry against global financial crises. The Financial Stability Board (FSB) was particularly interested in enhancing data transparency and harmonizing reporting across Systemically Important Financial Institutions (SIFIs)[3], since this would give states and the financial services sector a better understanding of how these SIFIs are interrelated.

It is recognized by some financial authorities that Global Systemically Important Banks (G-SIBs) should establish worldwide government relations teams with personnel knowledgeable in the politics and culture of national and regional data protection regulations (if they haven't already). These people would broaden the knowledge of those who are knowledgeable about business regulatory concerns and provide governmental viewpoints on these problems that those in the corporate world would not

[2] In order to create risk profiles of individuals applying for childcare benefits, the Dutch Tax and Customs Administration used algorithms in which 'foreign sounding names' and 'dual nationality' were used as indicators of potential fraud. As a result, thousands of (racialised) low- and middle-income families were subjected to scrutiny, falsely accused of fraud and asked to pay back benefits which they had obtained completely legally. Thus, the algorithms led to racial profiling (European Parliament, 2022).

[3] SIFIs are broadly defined as companies that are so essential to the domestic and global financial systems that the collapse of such companies would be extremely significant for national and worldwide economies.

frequently meet. It is only by establishing effective international relations at all levels concerning AI and data protection, that financial innovation processes can bring benefits to the global society.

It is worth re-emphasising the increasing importance of GDPR as AI development is progressing fast. Whenever new technologies appear in everyday life, it takes time to create rules and regulations that embrace and control them, not to mention the need to foster education and training for their correct use and enhancement. One of the broadest and most recognizable third-level educational programmes is Horizon Europe (HE) which provides funds for research and innovation and consists of a budget of €95.5 billion (European Commission, 2020a). The key pillars of Horizon Europe are: to tackle climate change, help to achieve the United Nations sustainable development goals and in general to create more competitive advantage for the EU. AI research and development sits at the centre of all these initiatives. As Mariya Gabriel, Commissioner for Innovation, Research, Culture, Education and Youth said in 2020, "Research and Innovation in artificial intelligence underpins the digital and green transition." (The European Commission, 2020a).

This combination of training in both GDPR and AI is something that remains open for the AI Act. It is not clear yet to what depth this issue of prioritising AI and data protection training and education across Europe is addressed by the AI Act. The Act speaks about the need for training when developing and using AI but exactly what type and how much training is not clear. Neither is how much the GDPR is expected to enforce its fundamental principles of transparency and accountability to ensure the protection of individuals rights when using AI technology. Although, the AI Act does not go against the GDPR but in fact complements it in many of its articles and recitals (CEDPO's AI Working Group, 2022).

GDPR and Explainable AI for Fintech companies

GDPR requires that any decision made by an AI system that affects individuals must not only have human oversight but must also be transparent and accountable. Such a requirement could be met by making the AI *explainable*. Explainable AI (xAI) is an emerging field that aims to create transparent AI models that provide understandable and interpretable explanations for AI decisions.

The GDPR requires that individuals have the right to access information about the data processing activities that involve their personal data. This requirement could be met by providing interpretable and understandable explanations of AI-based decisions. Overall, the literature suggests that GDPR-compliant xAI is critical for ensuring transparency and accountability in AI-based decision-making. The development of GDPR-compliant xAI requires the integration of GDPR principles into the xAI development process, collaboration among data scientists and legal experts, and the use of interpretable and transparent xAI methods (Singh & Bajaj, 2019).

According to a study by Gartner in (2019), 75% of Fintech companies will use some form of AI, which highlights the importance of ensuring that these technologies are GDPR-compliant. In a study by the European Parliament (2021), it was noted that the GDPR's right to explanation presents challenges for AI systems, as it requires that individuals be provided with a clear and understandable explanation of how decisions that affect them were made. The study highlights the need for xAI, which allows for the transparency of AI decision-making processes, and can help Fintech companies demonstrate compliance with the GDPR.

Another study by the International Association of Privacy Professionals (IAPP, 2018) suggests that xAI is crucial for ensuring GDPR compliance, as it allows individuals to understand how their data is being used and why certain decisions are being made. The study also notes that xAI can help Fintech

companies avoid the risk of algorithmic bias, which can lead to discrimination and other negative outcomes.

Singh and Bajaj (2019) examine the impact of xAI on consumer behaviour in the context of GDPR compliance by arguing that the right to explanation under the GDPR is crucial for building consumer trust in AI systems and for ensuring ethical and responsible use of consumer data. The study by Jia, Huang, & Dai (2020) highlights the importance of xAI in enhancing the transparency and interpretability of financial models, improving decision-making accuracy, and identifying hidden risks. The authors also note the challenges associated with xAI, such as the complexity of financial data and the need for specialized knowledge and expertise. The study suggests that xAI can be useful in various financial decision-making scenarios, such as credit risk assessment, portfolio management, and fraud detection.

Yu, Guo, & Fan (2019) examine the role of xAI in Fintech and highlight its potential benefits, including increased transparency, improved accuracy, and enhanced customer trust. The authors suggest that xAI can be useful in various Fintech applications, such as credit scoring, investment recommendations, and fraud detection. However, the study also identifies several challenges, such as data quality issues, the need for specialized knowledge and expertise, and the risk of model hacking. The authors recommend that Fintech companies prioritize xAI development to ensure transparency in decision-making processes and maintain customer trust.

He, Shi, & Deng (2019) explore the potential of xAI in Fintech applications and highlights its benefits, including increased transparency, improved accuracy, and enhanced interpretability. The authors suggest that xAI can be useful in various Fintech scenarios, such as credit risk assessment, investment recommendations, and fraud detection. The study also identifies several challenges associated with xAI, such as the need for specialized knowledge and expertise, data quality issues, and the risk of model hacking. The authors suggest that Fintech companies should prioritize xAI development to ensure transparency in decision-making processes and maintain customer trust.

Liu & Zhu (2021) discuss the state-of-the-art in GDPR-compliant xAI, emphasizing the need for transparency, interpretability, and accountability in AI systems to ensure compliance with the GDPR's data protection principles. The authors suggest that GDPR-compliant xAI can benefit various stakeholders, including users, data subjects, data controllers, and data protection authorities.

Martin, Langenberg, and Kemp (2020) present a framework for designing and developing GDPR-compliant xAI systems. The framework includes several stages, such as data collection, pre-processing, feature engineering, model development, evaluation, and explanation. The authors suggest that this framework can help ensure GDPR compliance and promote trust and acceptance of AI systems among users and stakeholders.

Turrini, Sartor and Nalin (2020) provide a legal perspective on xAI, emphasizing the importance of GDPR compliance in the development and use of AI systems. The authors argue that GDPR-compliant xAI can enhance the protection of personal data and promote user rights, including the right to explanation. They suggest that GDPR-compliant xAI can also help avoid legal liability for non-compliance with the GDPR's data protection principles. By ensuring GDPR compliance, xAI can promote transparency, accountability, and data protection, while avoiding the risks of algorithmic bias, discrimination, and other harmful outcomes.

GDPR and Ethical AI for Fintech

In 2019, the European Commission selected a group of experts in Artificial Intelligence (AI) that came from civil society, academia and industry to create the High-Level Expert Group on Artificial Intelligence (AI HLEG). It consisted of a total of 52 people from different countries of the European Union (EU). The main objective of this independent group was to provide support in the creation of the European Strategy for Artificial Intelligence with a vision on “ethical, secure and cutting- edge AI” (HL-EGAI, 2019).

Then, on 19 February 2020 the EU Commission adopted its White Paper on Artificial Intelligence - A European approach to excellence and trust (European Commission, 2020) whose purpose was to set out the policy options to achieve the twin objectives of promoting the uptake of AI and of addressing the risks associated with certain uses of this emerging technology.

In this report, the Commission expressly recognized that “Europe’s current and future sustainable economic growth and societal well-being increasingly draws on value created by data. AI is one of the most important applications of the data economy. Simply put, AI is a collection of technologies that combine data, algorithms and computing power. Advances in computing and the increasing availability of data are therefore key drivers of the current upsurge of AI” (European Commission, 2020).

On a more global scale, there are several ethical AI guidelines that have been developed by various organizations and initiatives, aimed at providing frameworks for the responsible development and deployment of AI. Such examples include, the IEEE founded a Global Initiative on Ethics of Autonomous and Intelligent Systems (IEEE.org, 2016), the Montreal Declaration for Responsible AI (Université de Montréal, 2017), the Asilomar AI Principles (Crowe, 2017), the Global AI Ethics Consortium (IEAI, 2021), and the World Economic Forum's Global AI Action Alliance (GAIA) (World Economic Forum, 2020).

Overall, these ethical AI guidelines share many common themes and principles, such as the importance of transparency, fairness, and accountability in the development and deployment of AI systems. However, there are also some differences in emphasis and approach. Some frameworks are broader in scope and focus on a wide range of ethical issues related to AI, while others have a narrower focus. For example, the IEEE's "Ethically Aligned Design" framework covers a broad range of ethical issues, including transparency, accountability, and social impact, while the Asilomar AI Principles are more focused on the safety and reliability of AI design.

Overall, these differences reflect the diverse perspectives and priorities of different organizations and stakeholders in the development and deployment of AI globally. We can conclude, however, that while Europe recognises the need to remain competitive on the global market regarding AI, it also accepts the continued obligations of the GDPR combined with the ethical use of AI to protect the welfare of its citizens’ personal data. It could be argued that nowhere is this tension between innovation and data protection more apparent than the European Fintech landscape.

xAI in FinTech education

There has been a growing interest in the use of xAI in FinTech education. Several studies have been conducted to explore the use of xAI in FinTech education, and to investigate its effectiveness in improving students' learning outcomes.

One study by Xue, Wang, and Zheng (2020) examined the use of xAI in a financial data analysis course and found that it helped students to better understand the relationship between data and

decisions. Another study by Cai, Zhang, and Chen (2021) used xAI to enhance students' understanding of the credit scoring process and found that it improved students' decision-making abilities.

In addition, Qian, Liu, & Fan (2021) explored the use of xAI in a financial risk management course and found that it enhanced students' ability to identify and mitigate risks. Similarly, a study by Liang and Yang (2021) investigated the use of xAI in a financial forecasting course and found that it improved students' accuracy in predicting future financial trends.

Overall, these studies suggest that xAI can be an effective tool for improving students' learning outcomes in FinTech education (Molnár et al, 2020). By promoting transparency and enhancing students' understanding of complex financial processes, xAI can help to prepare the next generation of FinTech professionals to navigate the challenges of an increasingly data-driven industry. Additionally, the use of GDPR-compliant xAI can ensure that students are trained to use ethical and accountable AI systems in their future careers.

There is a growing interest in the use of xAI in the financial technology industry. Some recent studies have investigated the state of the art in this area. For example, Li and Han (2020) conducted a survey of xAI techniques and applications in finance, and identified several promising areas, including fraud detection, credit scoring, and risk management.

In another study, Yang, Zhu, & Pan (2021) examined the use of xAI in the lending industry and found that it can help to increase transparency and trust in the lending process, as well as improve risk assessment and decision-making.

Moreover, a study by Hu, Yu, & Zhao (2020) explored the use of xAI in investment decision-making and found that it can help to improve the interpretability and transparency of investment models, as well as provide insights into the underlying factors driving investment outcomes.

Methods

Currently, a significant number of the world’s nations are drafting and passing data privacy legislation (IAPP.com, 2022). The landscape pretty soon is going to be a mishmash of legislation and terminology that could potentially confuse even the clearest of minds. In order to get an understanding of the current landscape for data protection in the Financial industry with the advent of AI, members of the Fin-AI Cost Action (CA19130) conducted a survey from November 2022 until June 2023. In order to ensure GDPR compliance, we used a European survey platform which stated GDPR compliance on their website. In addition to this precaution, participation in the survey was voluntary and no personal data of respondents was gathered, therefore eliminating any issues with the processing of personal data. This eliminated the need for ethics approval for this study. The name of the survey platform was Easyfeedback.com.

Survey Methods

We received in total eighty-nine anonymous responses out of which fifty came from people working in academia (56%) and thirty-nine came from people working in industry (44%). As Figure 1 indicates, the sub-sample corresponding to industrial participants is well-balanced with 51% of respondents working in banks where the likelihood of them processing personal data is high. This suggests these individuals handle sensitive information about customers, clients, or other individuals, including financial records, personal identity data, transaction details, and more, making the need to understand explainability, transparency and ethics in AI essential for this co-hort.

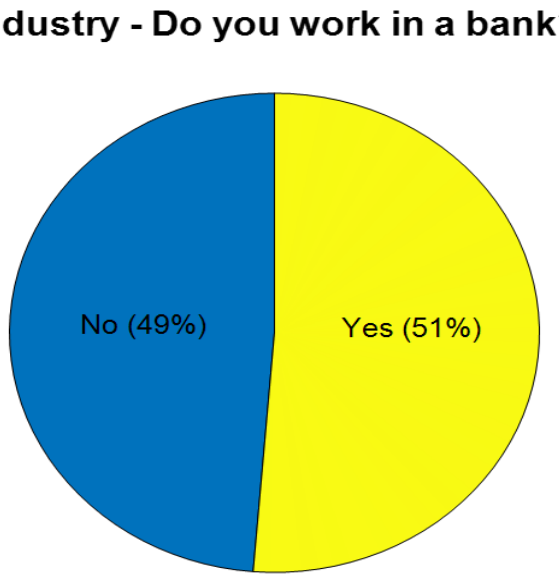

Figure 1: Distribution of the industry respondents based on banking vs non-banking sector.

Despite most respondents working in the banking industry, only 30% of these financial experts possess knowledge of the principles of explainable AI. This finding indicates a gap in the understanding of xAI concepts among professionals who handle sensitive data and work with AI systems. This lack of knowledge could have implications for ensuring compliance with regulations and ethical standards regarding AI decision-making processes. Knowledge of xAI could be considered an essential requirement under the GDPR when considering AI and automated decision-making as individuals have the right to an explanation if they are refused a service through automated decision-making. This is particularly important in industries like banking that process large amounts of personal data, where transparency and accountability are essential. This finding suggests room for improvement in terms of promoting awareness and understanding of xAI in the banking industry.

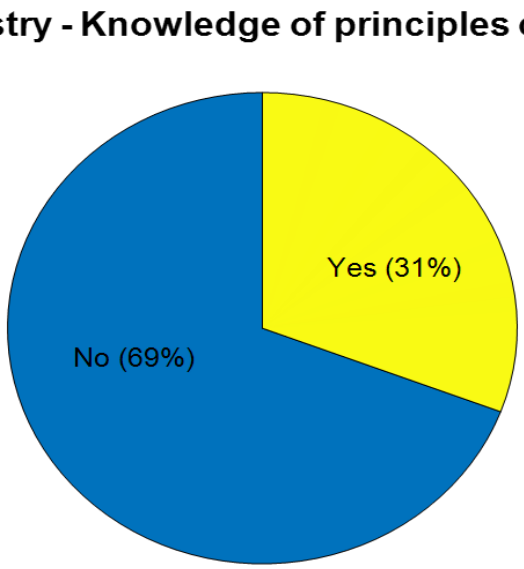

Figure 2: Knowledge of xAI by industry respondents.

Similarly, 31% of the industrial respondents work with AI in their current position (Figure 3). Even though there is some overlap between people who understand xAI's concepts and those who work with it, it is not necessarily the case that all those who work with AI also possess knowledge about making AI systems explainable. So one third of the respondents are directly involved in using AI systems to make decisions or support various processes within their roles.

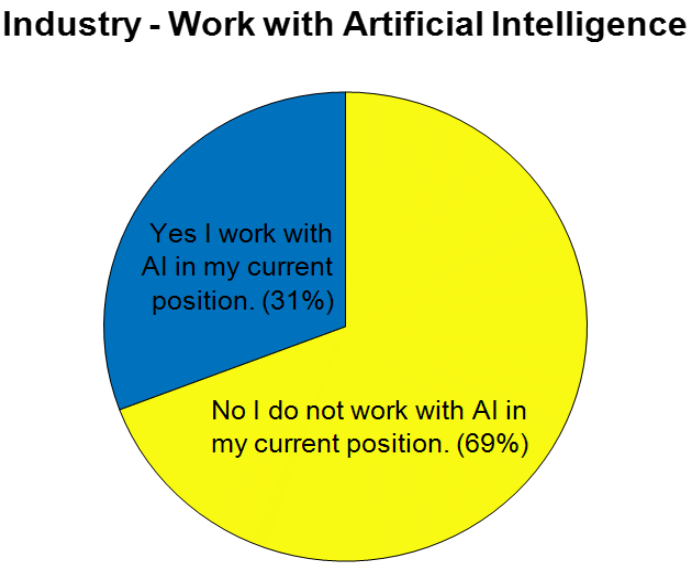

Figure 3: Distribution of the industry respondents working/not working with AI.

To proceed with the analysis of the AI aspects, we evaluate the importance of using AI and developing AI models for our respondents. But since our sample is made up of people from industry and academia, with different interests in applying AI, we have conducted the analysis separately, for each of the two groups. We present in Figure 4, the level of importance of AI and development of AI

models for industry respondents, while Figure 5 gives the same analysis, but from an academic perspective. One third of the industry respondents use AI systems in their work (33%) or, at the very least, believe that AI is essential to their business and their jobs (42%). Given that the majority of respondents come from the financial sector (51% of whom work for banks), this shows that AI is highly applicable in the financial sector. It is quite likely that the industrial respondents (including those in the banking industry) are working with AI applications that involve processing personal data since AI plays a significant role in their organization and area of expertise. This supports the claim that there is a good chance that bank employees will handle sensitive personal data because AI technologies are frequently used for handling and analyzing large amounts of data, particularly related to individuals. However, there is also a significant portion of respondents stating that artificial intelligence is not important for them or their company.

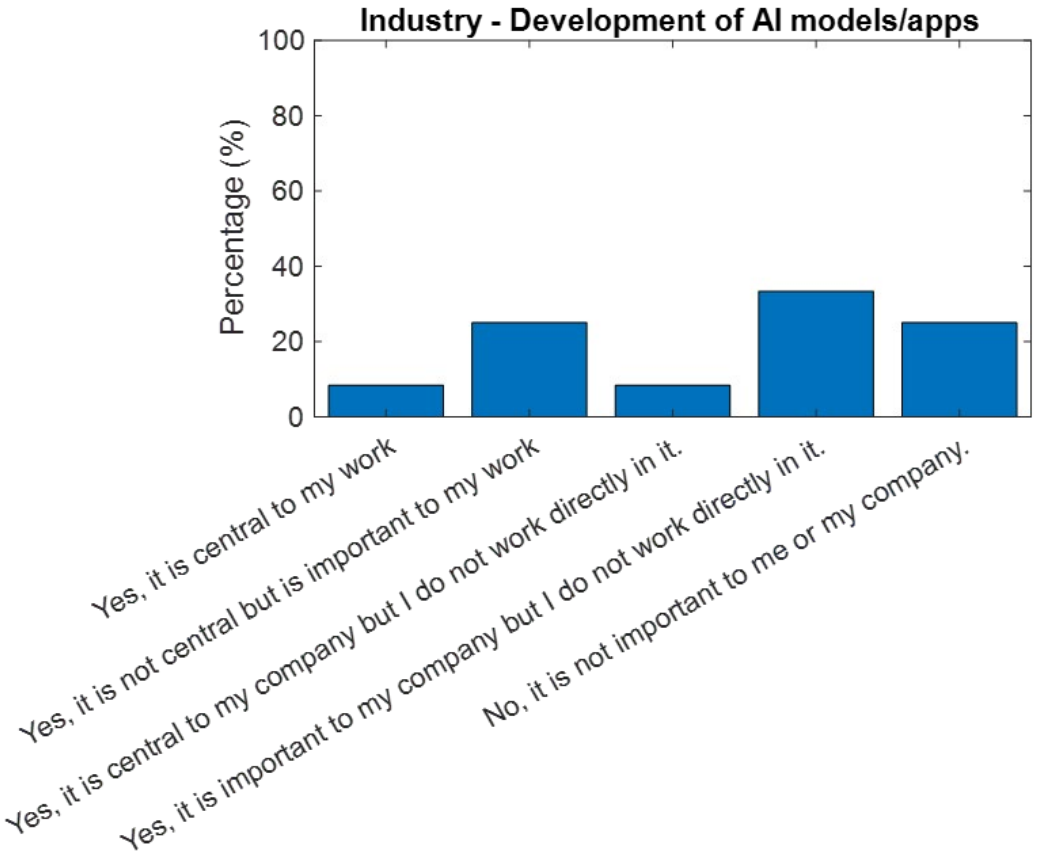

Figure 4: Distribution of the industry respondents developing AI models.

Academic respondents mostly conduct research on machine learning (ML) and artificial intelligence (AI) in the Fintech and financial sectors, either through using or developing AI and ML techniques. Figure 5 offers insightful information on the distribution of these respondents. Most of them (36%) engage in intermittent AI research, indicating that while AI may not be their sole focus, they actively incorporate AI elements into their broader research endeavours. For 22% of the academic respondents, AI is their primary research focus, underscoring the growing importance of AI in various academic disciplines and highlighting the field's expanding significance. Conversely, a small minority (4%) declared that they have never undertaken any research related to AI, suggesting the presence of a subset of academics who have yet to explore the potential of AI applications in their fields. These findings highlight the varying degrees of AI engagement within the academic community

and underscore the need for fostering AI literacy and research opportunities across disciplines to harness the full potential of AI driven advancement.

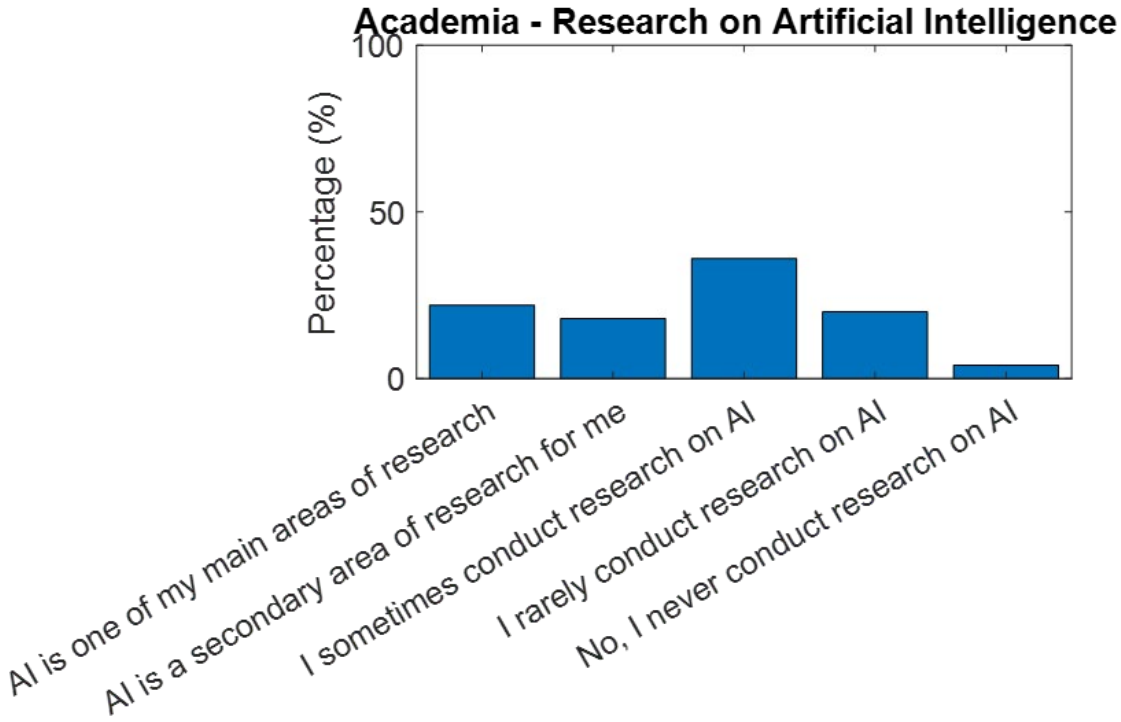

Figure 5: Research conducted on AI by academia respondents.

The distribution of research interests among participants, as indicated by the analysis of Figure 6, justifies the need to address the skills gap in AI training within the Fintech sector. The findings show that a considerable share of participants (30%) is involved in intermittent AI research in Fintech. This suggests that while AI is being incorporated into their broader research, it may not be their primary focus. On the other hand, 18% of respondents concentrate primarily on AI in Fintech, indicating a specific and dedicated research focus in this area. However, the notable percentage of 12% of respondents who have never conducted any AI in Fintech related study highlights the existence of a significant group of professionals or researchers who may not have the necessary AI knowledge and skills relevant to the Fintech domain. This finding underscores the importance of developing targeted AI training initiatives to bridge the skills gap and equip professionals in the Fintech industry with the expertise needed to leverage AI's potential effectively. By addressing this skills gap, Europe can empower its Fintech workforce to embrace AI innovations, drive industry growth, and maintain competitiveness in the global AI landscape.

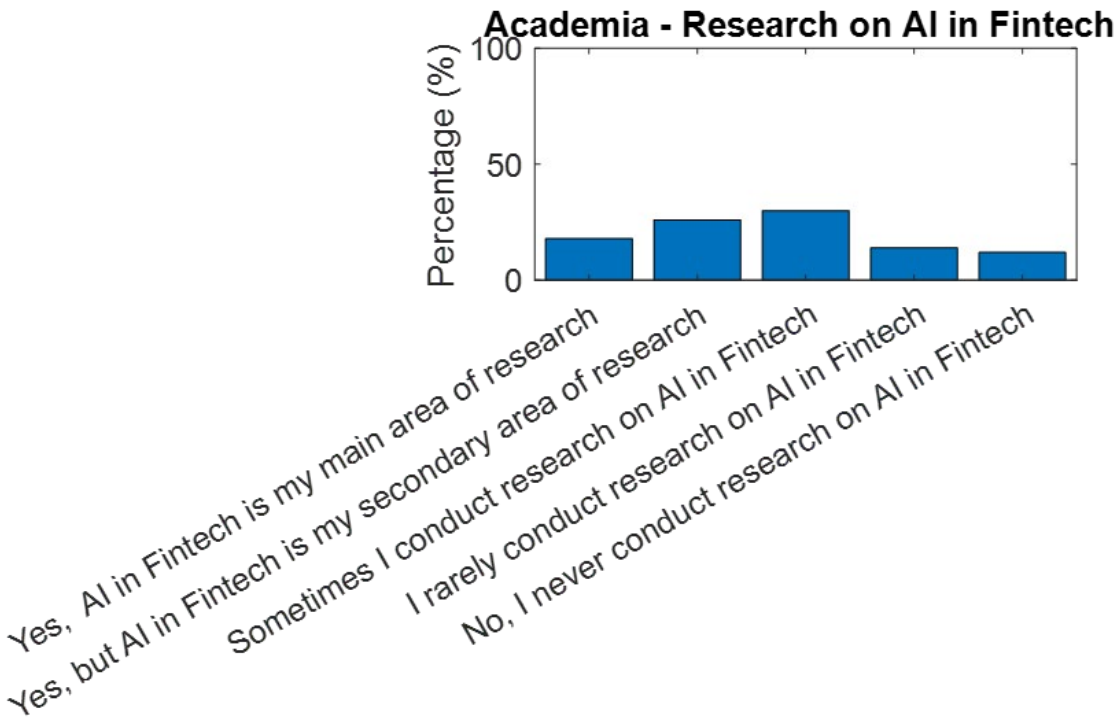

Figure 6: Research conducted on AI in Fintech by academia respondents.

The findings presented in Figure 7 demonstrate the level of academic research conducted in AI. A significant majority of participants (60%) reported having less than three years of experience in AI research. This observation suggests that a considerable number of academics are relatively new to the field, indicating a growing interest in AI across various sub-disciplines of Finance. Additionally, 20% of respondents indicated experience ranging between 3 to 5 years, showcasing a cohort of researchers with more mature expertise in AI. It is worth noting, however, that the remaining options were each represented by 10%, suggesting a somewhat even distribution of researchers with experience exceeding 5 years, as well as those who might not have extensive AI research backgrounds. In light of these findings, it could be argued that efforts to support and nurture the emerging AI research community are crucial. Institutions and policymakers could focus on certain recommendations to enhance AI research capabilities, such as establishing and supporting AI research centres, mentoring students with an interest in AI and encouraging multi-, inter- and trans-disciplinary collaboration, providing training in the form of workshops, work-experience, research conferences and symposia, and lectures in AI, and making research funding available for AI in specific disciplines identified as important.

By implementing these recommendations, the European academic community can cultivate a thriving AI research ecosystem within and beyond Europe, enabling researchers at all experience levels to contribute meaningfully to the field. This proactive approach will not only strengthen the European AI research landscape, but it will also foster a culture of continuous learning and innovation in AI research, ultimately accelerating progress and addressing real-world challenges through AI-driven advancements.

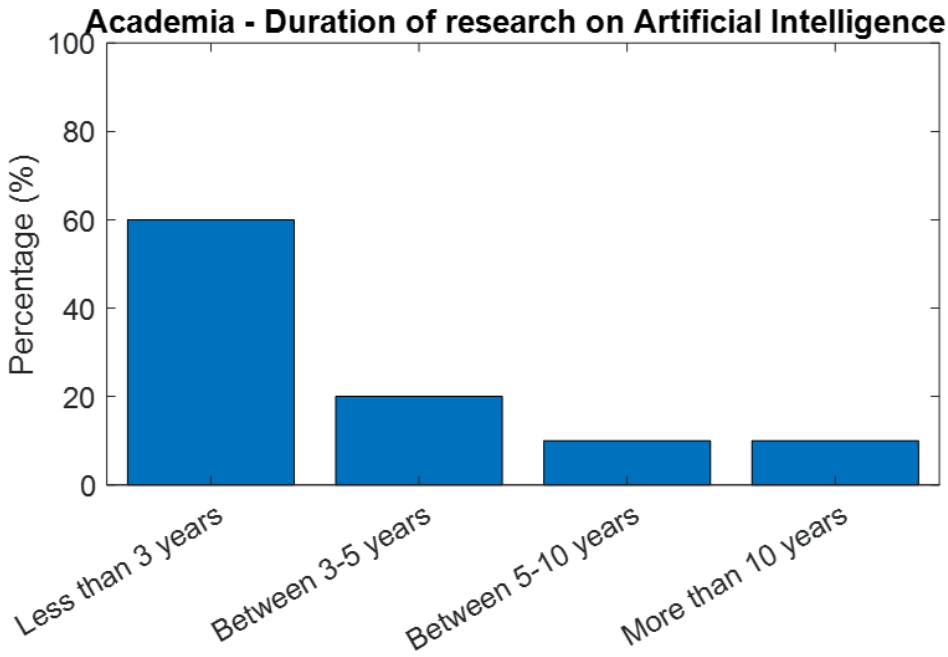

Figure 7: Duration of research conducted in AI by academia respondents.

The data obtained from the study reveals a striking contradiction between how respondents perceive their own expertise in the field of AI and their actual knowledge of one of its crucial aspects - explainable AI. In Figure 8, a staggering 78% of the respondents considered themselves to have a high level of expertise in AI. However, when it comes to understanding explainable AI, only 31% of the participants demonstrated a sound grasp of the concept, as shown in Figure 2. However, Figure 8 indicates that industry professionals consider themselves more expert in AI than the academics.

This disparity is noteworthy and holds significant implications for the AI industry, especially in sectors like finance that deal extensively with sensitive and private data. While a considerable portion of industry professionals may believe they possess a comprehensive understanding of AI, the fact that a substantial percentage lacks in-depth knowledge about making AI systems explainable is noteworthy.

Explainable AI is crucial for building transparent and accountable AI systems. In industries like finance, where decisions made by AI algorithms can have far-reaching consequences, it is imperative to comprehend the inner workings of AI models and be able to explain their decision-making processes. This not only helps build trust among users but also ensures that AI-driven decisions can be scrutinized and justified when necessary (Yang, Zhu, & Pan, 2021).

The contrast between perceived AI expertise and the understanding of explainable AI underscores the pressing need for continuous education and awareness-raising initiatives in the AI community. Professionals should be encouraged to stay updated with the latest developments in AI, especially those related to interpretability and transparency. Workshops, seminars, and training programs could be organized to bridge the gap between perceived and actual knowledge, equipping individuals with the necessary tools to create more accountable AI systems.

Moreover, collaboration between AI researchers, practitioners, and policymakers is essential to establish guidelines and standards for explainable AI implementation. By fostering a collaborative

environment, the industry can work towards making explainable AI an integral part of AI development processes, thereby mitigating the risks associated with opaque and black-box AI models.

In conclusion, the discrepancy in respondents' self-perceived AI expertise and their limited understanding of explainable AI calls for action. Initiatives like continuous education, awareness-raising, and funding for industry specific AI training will support professionals in creating transparent and accountable AI systems. Addressing this discrepancy is crucial if we are to have responsible and ethical AI development in the future, particularly in industries like finance, where the stakes are high in terms of privacy, security, and fairness.

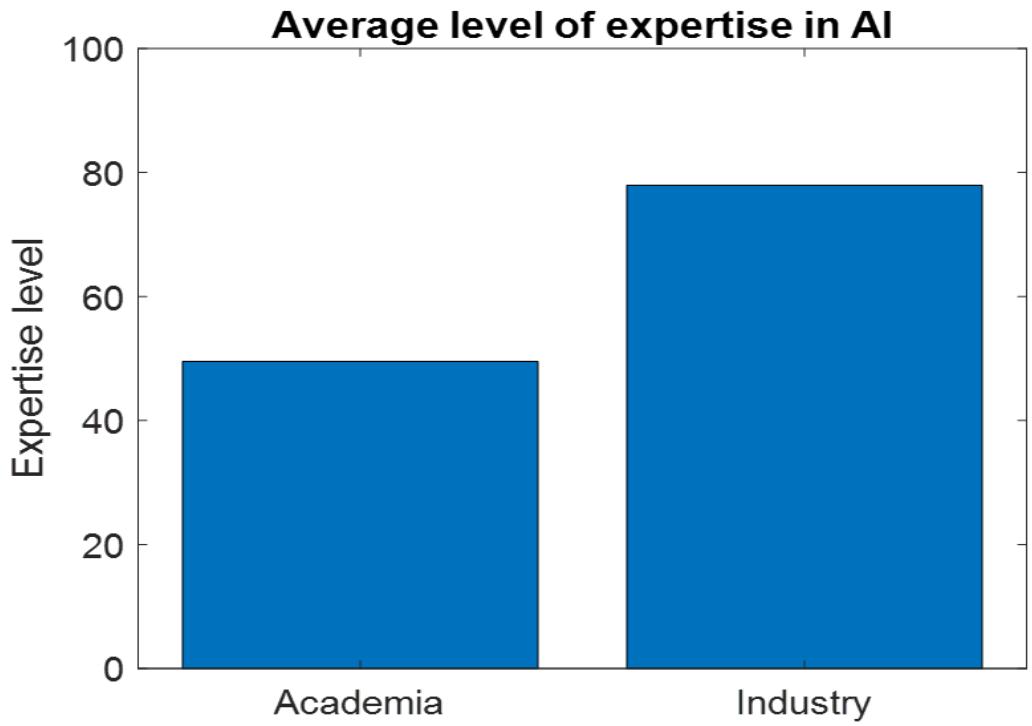

Figure 8: Perceived level of expertise in AI.

The findings from Figure 9 are indeed intriguing, as they reveal a high level of awareness of the existence of the GDPR among the respondents. A significant percentage, amounting to 88% of the participants, demonstrated familiarity with the GDPR, indicating that the importance of this data protection legislation is well-recognized within the surveyed population. This robust awareness is noteworthy as it reflects the growing acknowledgement of the GDPR's significance in safeguarding individuals' privacy rights and regulating the processing of personal data. The fact that such a substantial majority of respondents were aware of the GDPR suggests that efforts to promote data privacy awareness and compliance have been effective. However, it also underscores the need for continued education and vigilance to ensure that individuals, organizations, and institutions maintain a strong commitment to GDPR compliance, fostering a culture of data protection and privacy in the digital age.

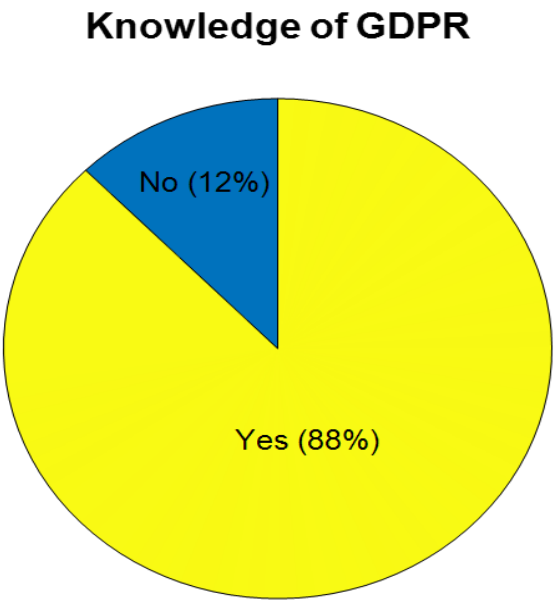

Figure 9: Awareness of GDPR.

Scrutinizing the respondents that were aware of the GDPR legislation (Figure 10), there is a discrepancy between respondents' estimated low level of data breach awareness (about 30%) and reality. Research shows that the majority of, if not all, businesses have experienced a data breach at some point. A study in 2022 by KPMG reported that found 62% of companies experienced a data breach or cyber incident in 2021 alone (Rigby, Melo, Espinar, Carlucci, & Preciado, 2022). One study published in CPO magazine in 2021 claimed that almost 100% of companies using the cloud had experienced a least one breach in the previous 18 months (Hope, 2021).

The frequency of banking cyber-attacks is another factor that emphasizes how serious the situation is (Maurer & Nelson, 2021). This emphasizes the need for more education and understanding of cybersecurity, with a focus on preventative measures and strong security solutions to safeguard sensitive data from online threats. Businesses must prioritize cybersecurity, particularly in the financial industry, to protect themselves from potential breaches and their far-reaching consequences, such as identity theft and reputational damage.

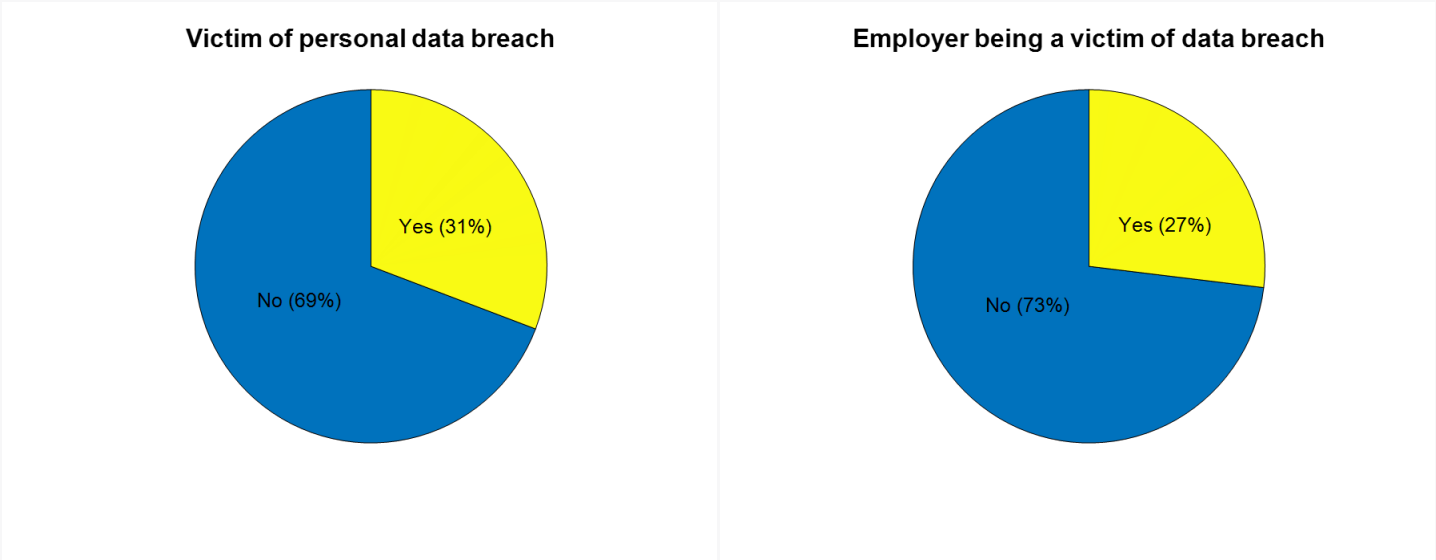

Figure 10: Perceived level of data breach risk.

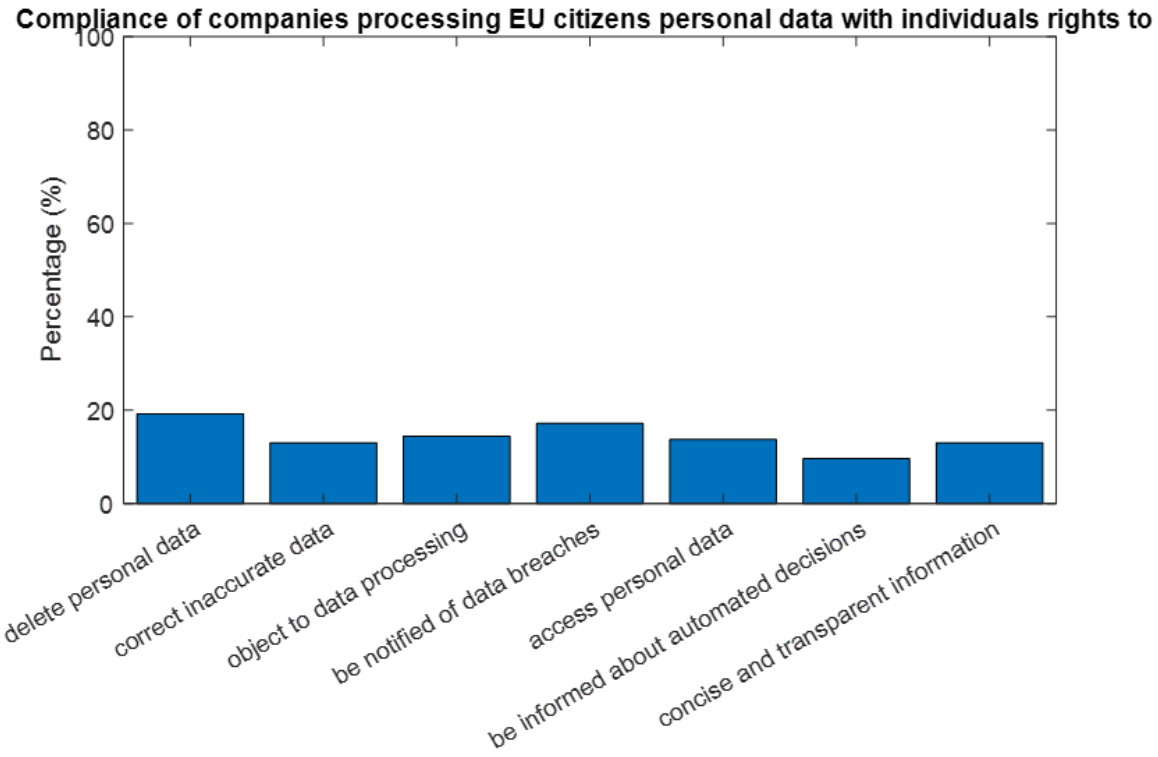

Figure 11: Individuals rights compliance of companies processing EU citizens personal data.

Despite the findings in Figure 9, when the participants were questioned about the specifics of the GDPR legislation, it was evident that their knowledge was limited, as Figure 11 indicates. This question was designed in order to effectively conceive the level of knowledge of the GDPR legislation since all the provided answers were appropriate. However, the results are indicative of the participants' level of knowledge and understanding of their rights under the GDPR. It appears that among the participants, the first right (erasure of all personal data) had the highest recognition (19%),

whilst the last right (clear information provided on how an algorithm made an automated decision) received the lowest recognition (10%).

This finding stems from the lack of any training in GDPR, a requirement under the GDPR if processing personal data. As shown in Figure 12, a substantial portion of respondents (54%) reported never receiving any form of GDPR training. This indicates a concerning gap in educating employees about data protection obligations, given that GDPR mandates regular training when processing personal data. Moreover, the survey reveals that only a meagre 4% of respondents received training in GDPR specifically for AI use or development. That small percentage reporting training in GDPR and AI among the participants points to a serious knowledge gap that should be filled. Understanding how the GDPR principles apply to AI is essential given the complexity of AI and its increasing use across different sectors. Training in GDPR and AI is not only advantageous but also legally mandated as a result of the GDPR, which requires that industries processing the personal data of European citizens comply with strict data protection regulations. AI system developers must be educated about the GDPR to ensure that any personal data is handled ethically and legally by the system. Financial AI systems frequently process personal data. Giving employees training in GDPR and AI shouldn't be done just once; it should be done annually to keep them informed of changing laws, industry best practices, and potential difficulties. In addition to ensuring legal compliance, such training promotes ethical AI development by encouraging responsible behaviour, privacy-conscious AI, and the avoidance of biases and discrimination. Lastly, the numbers are doubled in the figure when it comes to training in GDPR for Fintech, suggesting a higher level of awareness and preparedness in this particular sector. These findings highlight the need for comprehensive and targeted training initiatives to enhance GDPR compliance across the financial industry, especially in the context of AI and Fintech, to ensure the secure and responsible processing of personal data and the safeguarding of individuals' rights.

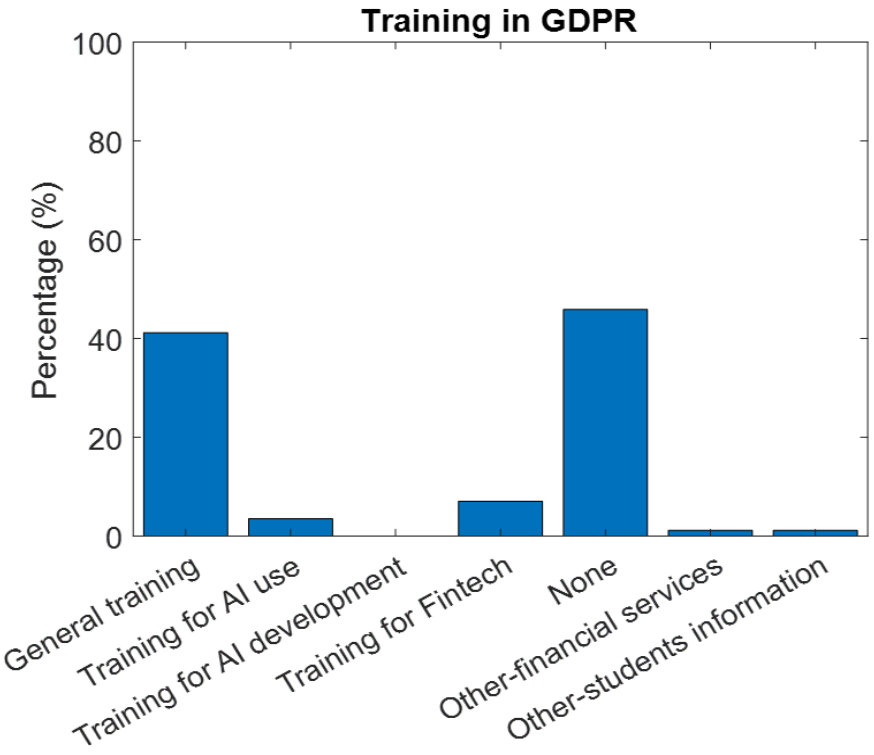

Figure 12: Training in GDPR.

In Figure 13, when respondents who were aware of the GDPR legislation were asked about the type of criteria they considered important for training, several noteworthy trends emerged. A significant percentage (74%) highlighted the importance of general training in data protection, encompassing GDPR as a whole. Additionally, an equal proportion of participants (74%) emphasized the significance of specific GDPR training tailored to AI, reflecting the recognition of AI's unique data privacy challenges. Notably, 73% of respondents underscored the importance of data protection when utilizing AI models, indicating the need to ensure privacy and security in AI applications. Of particular interest was the exceptionally high importance attributed to data protection in the Fintech sector, with 81% of participants expressing its significance. This highlights the growing recognition of the criticality of data privacy in the context of financial technology. Furthermore, an overwhelming 82% of respondents believed that GDPR training in the future would be most beneficial, suggesting the anticipation of evolving data protection requirements and the need for continuous learning and adjustment. Lastly, an impressive 72% of respondents acknowledged the high importance of xAI principles when developing AI models and applications. This reflects the increasing demand for AI systems that provide transparent explanations for their decisions, particularly in sensitive domains such as finance and data privacy.

The results presented in Figure 13 underscore the pressing need for comprehensive training programs that encompass general data protection, AI-specific GDPR training, and a particular emphasis on data protection in Fintech. To stay ahead in an evolving regulatory landscape, institutions must prepare for the future with continuous GDPR training and embrace xAI principles to ensure transparency and ethical use of AI. This proactive approach will not only reinforce data protection practices but also foster trust in AI technologies and promote responsible and secure AI applications across various domains.

In Figure 14 the breakdown of the responses regarding Article 22 of the GDPR is depicted. In particular, this article grants the legal requirement for human oversight when processing personal data in an automated way. The most well-known right, as chosen by 28% of respondents, is the one that allows data subjects to "request a copy of their data and a detailed explanation of how the AI model/app came to the final decision." This implies that individuals have the right to view their personal data and learn the reasoning behind automated decisions that impacts them. Thus, transparency and accountability in automated decision-making are stressed, allowing people to understand and challenge choices that could have a fundamental impact on their lives. With approval from 21% of respondents, the second most popular right is the ability to "request human intervention and receive an assessment of their case by an appropriately qualified human expert." This right aims to promote fairness and reduce potential biases in automated choices. Data subjects can feel secure knowing that when a human evaluation is requested, an expert analgises the automated decision to determine its accuracy and correct any potential flaws. Furthermore, 18% of respondents support that individuals have a right to "be told the lawful basis that the company has for carrying out profiling and/or automated decision-making on the individual/data subject." Data controllers must inform persons about the legal justification for processing their personal data, including the use of automated decision-making and profiling techniques. Such openness is essential for enabling people to comprehend the legal foundation and consequences of decisions made regarding them. Additionally, 15% of participants acknowledge having the right to "access details of the information the company/data controller used to create their profile." In the context of automated decision-making processes, data subjects can inquire about the information on the data points and standards used to create their profiles, strengthening data subject control and fostering openness.

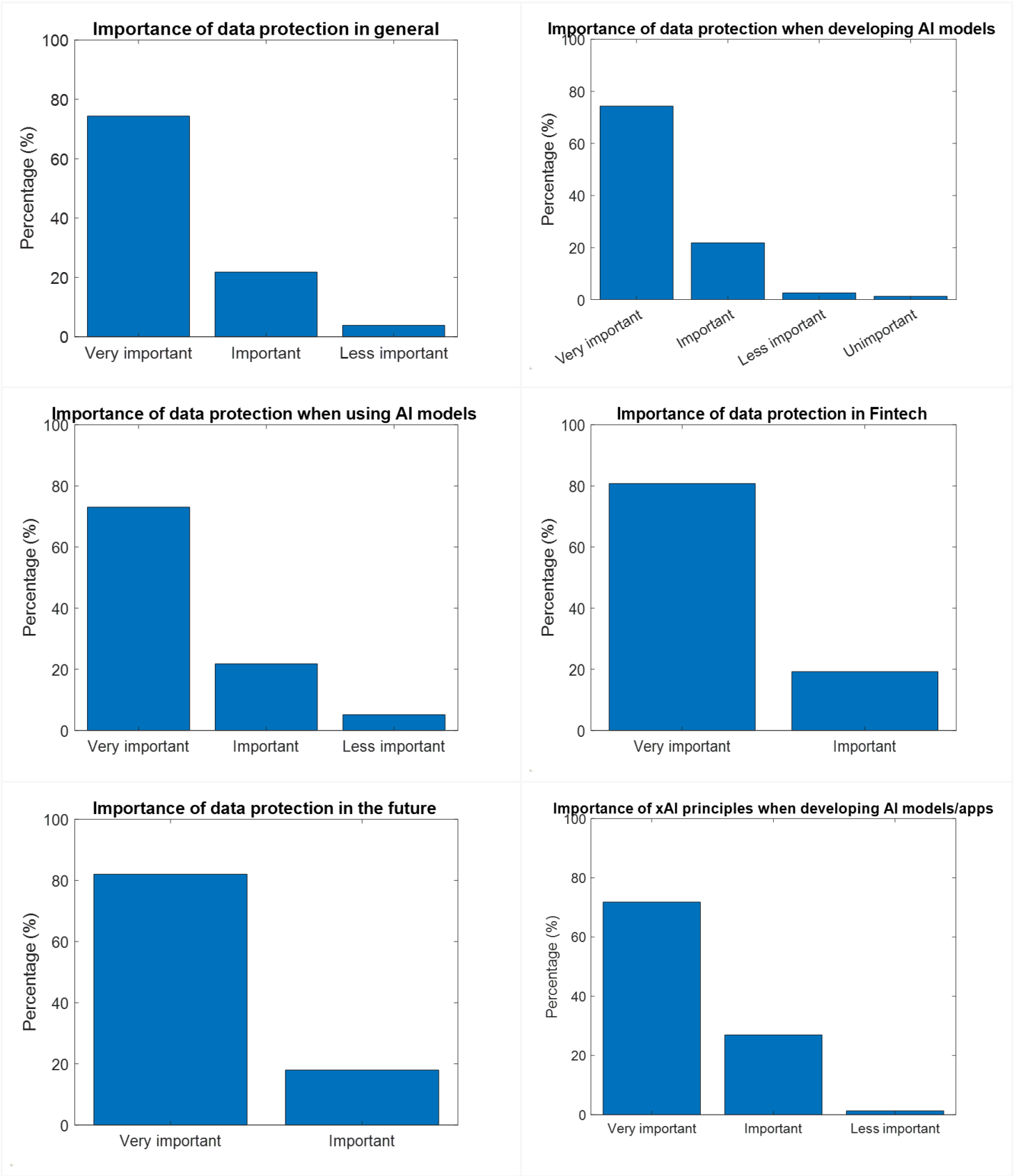

Figure 13: Importance of data protection.

It's interesting to note that only 4% of respondents chose the statement that people have no rights if automated processing is required for the execution of a contract between them and a corporation that controls their data, with this low response rate pinpointing the significance of the GDPR's emphasis on informed consent and human intervention. The right to "appeal the automated decision by taking the company/data controller to court" was acknowledged by 14% of respondents highlighting the importance of accountability and due process in the era of AI-driven decision-making by the opportunity to seek legal redress. This question stresses the need for building trust between data subjects and businesses using AI technologies by emphasizing transparency, human intervention, and individual empowerment.

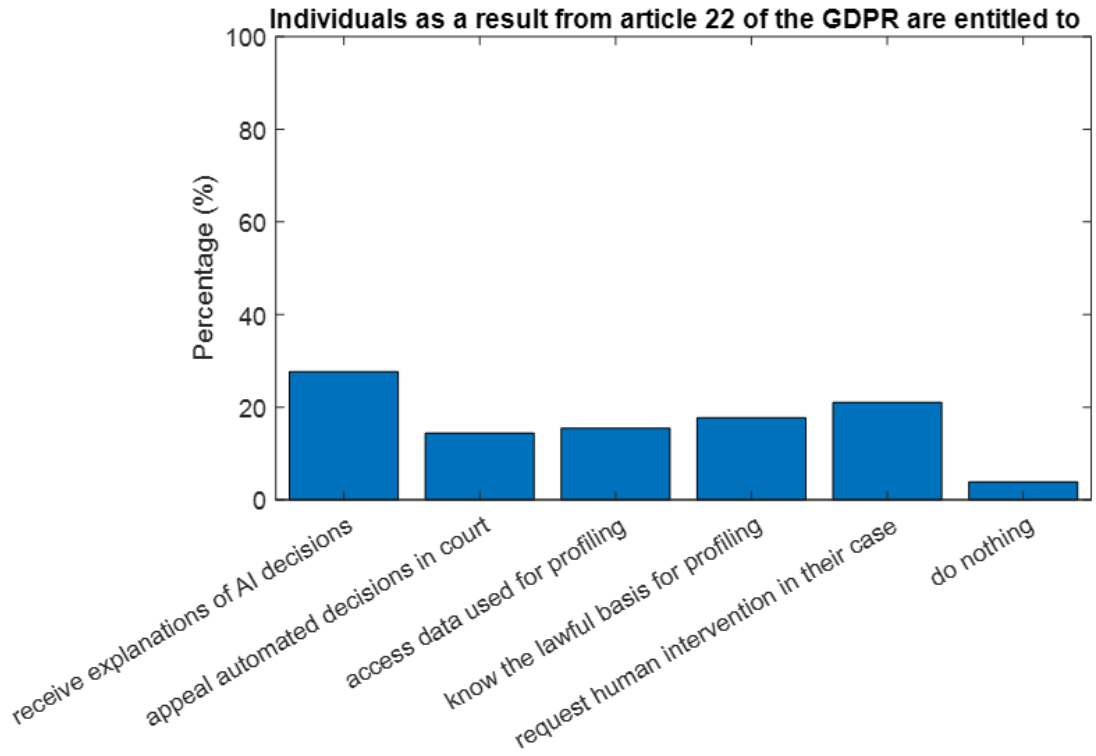

Figure 14: Article 22 and GDPR entitlements - understanding individuals' rights in automated decision-making.

Moving on to the participants that lack knowledge of the GDPR legislation, it is important to consider public opinion regarding the legal responsibilities that businesses have when collecting, using, and storing customer financial data. This will give us important insights into how people generally view data privacy and security. As Figure 15 points out, the idea that businesses should be required by law to comply with customer requests for data erasure received the majority of responses, garnering 28%. This viewpoint most likely reflects people's desire for control over their personal data, especially in circumstances where they might not be aware of specific data protection laws. Furthermore, 20% of respondents stressed the significance of customers being notified by businesses in the event of a data breach involving their personal data. Regardless of any specific awareness of the notification obligations for data breaches in data protection legislation, this response is consistent with a general desire for openness and customer protection. Moreover, 16% of the respondents agreed that businesses had a duty to give clients information about how their personal data was used in a simple and understandable way. This viewpoint contends that despite their lack of understanding of the specific legal requirements for data openness, customers value clear communication from businesses. Only 8% of respondents, on the other hand, highlighted the requirement under the law

for businesses to immediately correct inaccurate personal data. This lower proportion might be a sign that less attention is being placed on data accuracy, possibly as a result of a lack of knowledge about the rights to data correction provided by data protection laws. Despite potential unfamiliarity with data protection regulations like the GDPR, the 12% response supporting the customer's right to be provided with a copy of all personal data reflects a significant emphasis on data transparency and individual control. Similarly, 12% of respondents acknowledged that customers have the right to object to the use of their personal information at any time. This suggests that some people value their autonomy when using their data, even if they might not be aware of the exact data protection rules that allow such rights. Finally, 4% of respondents stated that none of the aforementioned requirements ought to be placed on businesses handling customer financial data. This minority reaction may be a result of divergent views on the scope of legal responsibilities placed on businesses in the lack of familiarity with data protection laws. This question demonstrates that people respect open communication from businesses, value their right to data erasure and breach notification, and, to varied degrees, understand the need of data protection. In order to promote a more informed approach to data privacy and security, the question results highlight the significance of increasing awareness about data protection rights and obligations.

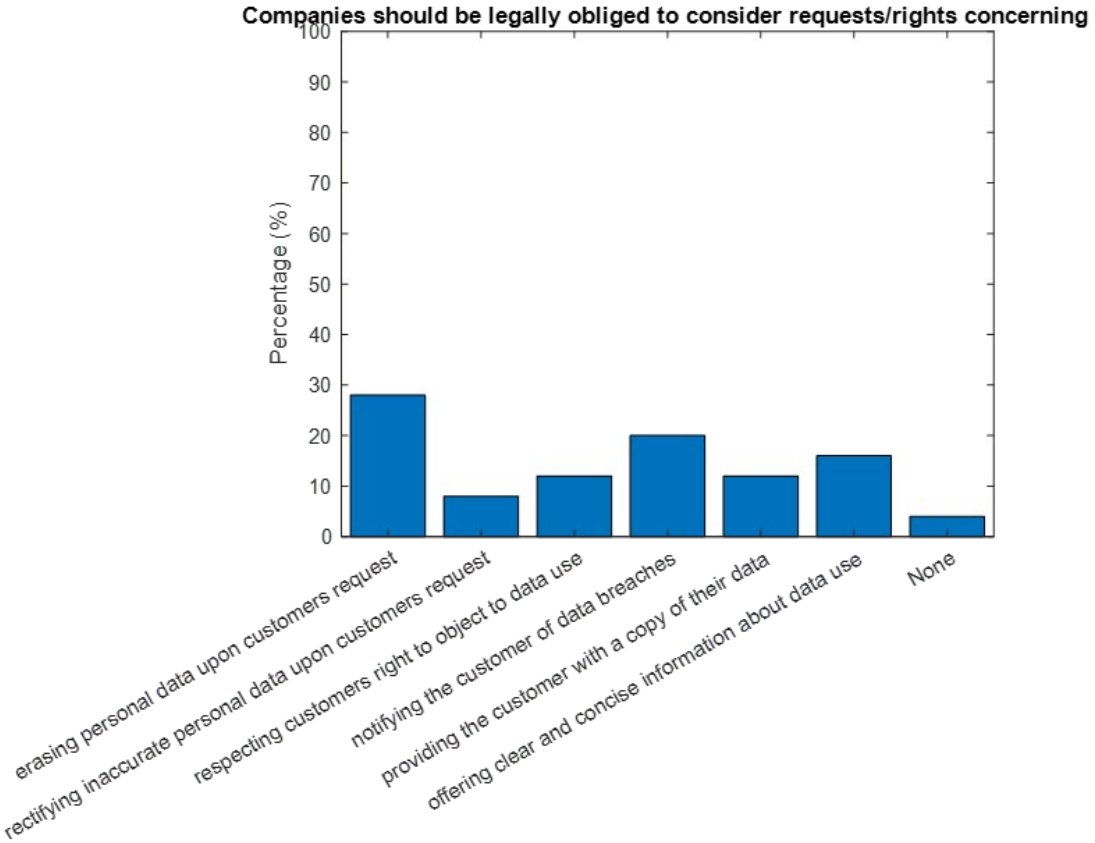

Figure 15: Legal obligations for companies handling financial data.

In Figure 16, the perspectives on the requirements that businesses should take into account when analyzing a customer's financial situation exclusively using AI and without any human intervention is depicted. The idea that businesses should be required by law to comply with customer requests for data deletion received the largest percentage of support, with 47% of respondents in favour. Even when AI is the only entity making decisions, this finding reflects individual's demand for

ownership over their personal data. Their right to erase data is consistent with the principle of data privacy and individuals' rights, stressing the value of customer autonomy. Furthermore, 23.5% of the respondents believe that it is crucial to give customers the right to object depending on their unique circumstances. Additionally, an equal proportion of participants (23.5%) emphasized the customers' right to request information about the process through which an algorithm reached an automated decision. These two results are indicative of the fact that individuals appreciate the ability that their unique circumstances are considered when AI algorithms make decisions about them and also stress the importance of transparency for individuals, especially when AI systems may affect their financial situation. However, only 6% of respondents think that businesses shouldn't be required to do anything if the algorithm is necessary for contractual reasons, meaning that even in situations where AI is the sole-decision maker, according to a minority of the sample, contractual necessity should take priority over personal data protection rights. In general, the results indicate that individuals appreciate having control over their data, being able to object under special circumstances, and the importance of transparency in AI-driven decisions.

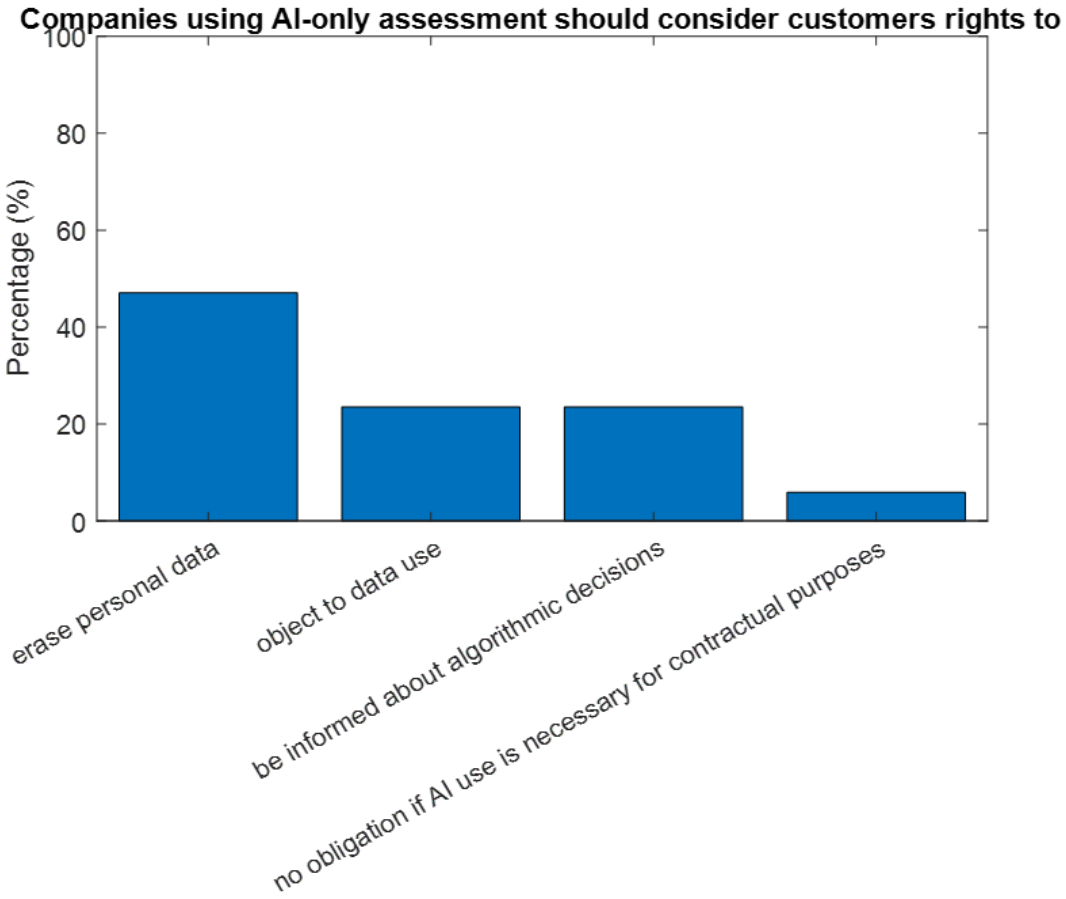

Figure 16: Legal obligations for companies using only AI in assessing customer financial situation.

Added to these findings, both the GDPR and the draft AI Act specifically outline the need for training. Currently, many working DPOs are not fully aware of the AI act and the people who develop AI are not sufficiently aware of the need for Privacy by Design or data protection as evidenced from the survey.

Summary of Findings

The survey conducted by members of the Fin-AI Cost Action (CA19130) provides valuable insights into the state of AI adoption, research, and data protection awareness among academics and professionals in the financial industry. The distribution of respondents revealed a balanced representation from both academia and industry, with the majority of industry respondents working in banks, where the likelihood of processing personal data is high. This highlights the relevance of the survey's findings, as the financial sector deals with large quantities of personal data and has many privacy and security challenges.

One notable observation from the survey is the relatively low level of knowledge regarding explainable AI (xAI) among the industry respondents, especially in the banking sector. With only 31% of industry participants demonstrating knowledge of xAI principles, it suggests a need for more education and awareness initiatives regarding the importance of transparency and accountability in AI systems, particularly in industries dealing with personal data like banking data. Given the requirements of the General Data Protection Regulation (GDPR), which grants individuals the right to an explanation for automated decision-making, the lack of xAI knowledge in the banking industry is a concerning finding that calls for improvement in promoting understanding and compliance with GDPR principles.

The survey also shed light on the widespread adoption of AI in the financial sector, with a significant percentage of industrial respondents using AI systems in their work or considering it essential to their business. This indicates the high applicability of AI technologies in the financial industry, where AI plays a crucial role in processing vast amounts of data, including personal data. Given this scenario, it becomes even more critical to ensure that AI systems comply with data protection regulations like GDPR, emphasizing the need for targeted AI training initiatives in the financial sector to bridge the skills gap and promote responsible AI development.

On the academic front, the survey findings revealed varying levels of AI engagement among respondents. While some researchers primarily focus on AI in their research (22%), others incorporate AI elements into their broader research endeavours intermittently (36%), indicating the interdisciplinary nature of AI's impact. However, a small minority (4%) reported not having engaged in any AI-related research, underscoring the need to foster AI literacy and research opportunities across disciplines to harness the full potential of AI-driven advancements.

Furthermore, the survey demonstrated a discrepancy between respondents' self-perceived AI expertise and their actual knowledge of xAI. This emphasizes the importance of ongoing education and awareness-raising to equip professionals with the necessary tools to create transparent and accountable AI systems. To address this disparity, institutions and policymakers must establish comprehensive AI training programs, particularly focused on the GDPR requirements and AI's impact on data privacy and security.

The survey's results also highlighted the high level of awareness of the GDPR among respondents, showcasing a growing recognition of the legislation's significance in safeguarding data privacy rights and regulating data processing. However, specific knowledge of GDPR provisions remains limited, indicating the need for more comprehensive training initiatives to ensure GDPR compliance, particularly in the context of AI and Fintech. Strengthening GDPR training can lead to a more responsible and ethical use of AI, promoting transparency, and safeguarding individuals' data privacy rights.

Finally, the survey respondents' perspectives on the legal obligations for businesses handling financial customer data further emphasized the importance of data protection, transparency, and individual control. Customers' rights to data erasure, breach notification, and transparency in AI-driven decision-making were strongly supported, reflecting a desire for greater control over personal data and the need for openness and accountability in AI processes.

In conclusion, the survey findings highlight several key areas for concern and improvement in the realm of AI adoption, research, and data protection. The results underscore the importance of ongoing education and awareness initiatives to bridge the knowledge gaps and promote responsible and ethical AI development[4]. Additionally, targeted AI training, particularly in the financial sector, is crucial to address the skills gap and ensure GDPR compliance. By fostering a culture of transparency, accountability, and data protection, the AI community can build trust among users, encourage responsible AI development, and navigate the evolving regulatory landscape with confidence.

Conclusion: A Symbiotic Coexistence

In conclusion, the theoretical exploration of the future of data protection and artificial intelligence necessitates a nuanced understanding of the interplay between technological innovation and data protection. This understanding should be informed by various academic lenses, including deontological ethics, dynamic systems theory, and sociocultural constructivism. These theoretical perspectives envision a symbiotic coexistence of robust AI innovation and stringent data protection within the European Union.

The success of this coexistence hinges on the effective integration of risk-based regulatory frameworks, as exemplified by the EU AI Act and the lessons learned from the GDPR. The EU's pioneering regulatory efforts, encapsulated in these landmark pieces of legislation, provide a roadmap for navigating the complex terrain of AI innovation and data protection.

Reconciliation of these two seemingly opposing forces requires a deliberate and informed approach that acknowledges the inherent tension between the drive for AI innovation and the ethical and legal obligations to protect personal data. The EU, with its leadership role in data protection and AI regulation, has a unique opportunity to shape this discourse and influence global norms and practices.

This theoretical exploration provides a pathway for future research and policy development that ensures the coexistence of ground-breaking AI innovations and the protection of personal data. By embracing this narrative, Europe can navigate the challenges of the digital future, fostering an ecosystem that simultaneously values innovation and upholds the fundamental rights of its citizens. The role of future leaders in this journey is crucial, as they will be at the forefront of maintaining Europe's position as a global leader in the symbiosis of AI innovation and data protection.

[4] **Data availability statement:** These data are under restricted access due to the sensitivity of the subject material. To access the data, please complete a Data Request Form for Research Purposes, sign it, and send it to maria.moloney@ucd.ie. Researchers will be asked to provide a description of the intended use of the data and agree to the terms of use as outlined in the request form. Data access will be granted for teaching and research purposes under ISSDA terms and conditions.

References

Agarwal, A., Singhal, C., & Thomas, R. (2021, March). *AI-powered decision making for the bank of the future.* Retrieved from McKinsey and Company: https://www.mckinsey.com/~/media/mckinsey/industries/financial%20services/our%20insights/ai%20powered%20decision%20making%20for%20the%20bank%20of%20the%20future/ai-powered-decision-making-for-the-bank-of-the-future.pdf

Cai, Y., Zhang, X., & Chen, W. (2021). Application of Explainable Artificial Intelligence in Financial Education: An Empirical Study of Credit Scoring. *Journal of Financial Research, 6*, 143-159.

CEDPO's AI Working Group. (2023, March 18). *The Confederation of European Data Protection Organisations.* Retrieved from www.cedpo.eu: https://cedpo.eu/wp-content/uploads/20221219-CEDPO_Opinion_AI_Act_DPO.pdf

Chishti, S., & Barberis, J. (2016). *The Fintech book: The financial technology hand-book for investors, entrepreneurs and visionaries.* John Wiley & Sons.

Crowe, S. (2017, February 3). *Asilomar AI Principles: 23 Tips for Making AI Safe.* Retrieved April 2023, from Robotics Business Review: https://www.roboticsbusinessreview.com/rbr/asilomar_ai_principles_23_rules_for_making_ai_safe/

European Commission. (2018). *High-level expert group on artificial intelligence*. Retrieved April 2023, from Shaping Europe's digital future: https://digital-strategy.ec.europa.eu/en/policies/expert-group-ai

European Commission. (2019a). *The Digital Markets Act: ensuring fair and open digital markets.* Retrieved from The European Commission: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en

European Commission. (2019b). *The Digital Services Act: ensuring a safe and accountable online environment.* Retrieved from European Commission: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en

European Commission. (2020). *White Paper on Artificial Intelligence - A European approach to excellence and trust.* Brussels: European Commission.

European Commission. (2020c). *White Paper on Artificial Intelligence - A European approach to excellence and trust.* Brussels: European Commission.

European Commission. (2022b). *The Digital Europe Programme.* Retrieved from The European Commission: https://digital-strategy.ec.europa.eu/en/activities/digital-programme

European Parliament. (2021, July 1). *AIDA Working Paper on 'AI and Financial Services'.* Retrieved from https://www.europarl.europa.eu/: https://www.europarl.europa.eu/cmsdata/239714/Working%20Paper%20on%20AI%20and%20Financial%20Services.pdf

European Parliament. (2022, June 28). *The Dutch childcare benefit scandal, institutional racism and algorithms*. Retrieved from Parliamentary question - O-000028/2022 - European Parliament: https://www.europarl.europa.eu/doceo/document/O-9-2022-000028_EN.html#def1

Gartner Group. (2019, November 5). *Gartner Predicts The Future of AI Technologies.* Retrieved from Gartner.com: https://www.gartner.com/smarterwithgartner/gartner-predicts-the-future-of-ai-technologies

He, Y., Shi, H., & Deng, C. (2019). Explainable Artificial Intelligence for Fintech Applications. *The 2019 IEEE 5th International Conference on Computer and Communications (ICCC)* (pp. 59-63). IEEE.

Hope, A. (2021, July 20th). *Almost All Organisations Suffered At Least One Data Breach in Past 18 Months, The State of Cloud Security Report Found.* Retrieved from CPO Magazine: https://www.cpomagazine.com/cyber-security/almost-all-organisations-suffered-at-least-one-data-breach-in-past-18-months-the-state-of-cloud-security-report-found/

Hornuf, L., Klus, M. F., Lohwasser, T. S., & Schwienbacher, A. (2021). How do banks interact with fintech startups? *Small Business Economics, 57*, 1505-1526.

Hu, J., Yu, J., & Zhao, Y. (2020). xploring Explainable Artificial Intelligence for Fraud Detection in Fintech. *Journal of Risk and Financial Management, 13*(8), 172.

IAPP. (2018, May 25). *GDPR Compliance Guide.* Retrieved from www.iapp.org: https://iapp.org/media/pdf/resource_center/GDPR-Compliance-Guide.pdf

IEAI. (2021, February). *The Global AI Ethics Consortium on Ethics and the Use of Data and Artificial Intelligence in the Fight Against COVID-19 and other Pandemics.* Retrieved April 2023, from IEAI Institute for Ethics in Artificial Intelligence: https://www.ieai.sot.tum.de/global-ai-ethics-consortium/

IEEE.org. (2016). *IEEE*. Retrieved from The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems: https://standards.ieee.org/industry-connections/ec/autonomous-systems/

Jia, X., Huang, O., & Dai, T. (2020). Explainable AI and Financial Decision-Making: A Literature Review. *Journal of Big Data, 7*(1), 1 - 23.

Laneret, N., Tielemans, J., & Zenner, K. (2022, July 12). EU Artificial Intelligence Act Proposal: What could it change? (M. D. Isabelle Roccia, Interviewer) LinkedIn.com. Retrieved from https://iapp.org/news/video/eu-artificial-intelligence-act-proposal-what-could-it-change/

Li, Y., & Han, J. (2020). Explainable Artificial Intelligence for Financial Risk Management: Challenges and Opportunities. *Journal of Financial Data Science, 2*(4), 143-156.

Liang, X., & Yang, Y. (2021). Explainable artificial intelligence (XAI) in finance education: Evidence from a financial forecasting course . *Journal of Financial Education, 47*(2), 128-142.

Liu, Y., & Zhu, F. (2021). GDPR-Compliant Explainable Artificial Intelligence: A Review of the State-of-the-Art. *IEEE Transactions on Emerging Topics in Computing, 1*(1).

Mantelero, A. (2021). The future of data protection: Gold standard vs. global standard. *Computer Law & Security Review, 40*.

Maran, A., Pallavicini, A., & Scoleri, S. (2021). *Chehyshev Greeks: Smoothing Gamma without Bias.* Retrieved from https://arxiv.org: https://arxiv.org/pdf/2106.12431v1.pdf

Martin, B., Langenberg, D., & Kemp., S. (2020). Designing and Developing Explainable AI Systems for GDPR Compliance. *The 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (pp. 1-9). Austria: IEEE.

Maurer, T., & Nelson, A. (2021, March 21). *The Global Cyber Threat.* Retrieved from The International Monetary Fund: https://www.imf.org/external/pubs/ft/fandd/2021/03/pdf/global-cyber-threat-to-financial-systems-maurer.pdf

Molnár, B., Tarcsi, Á., Baude, F., Pisoni, G., Ngo, C. N., & Massacci, F. (2020, November). Curriculum guidelines for new Fintech Master's Programmes. In 2020 18th International Conference on Emerging eLearning Technologies and Applications (ICETA) (pp. 470-474). IEEE.

Mitchell, T. (1997). *Machine Learning.* McGraw Hill.

Pisoni, G., Molnár, B., & Tarcsi, Á. (2021). Data science for finance: Best-suited methods and enterprise architectures. Applied System Innovation, 4(3), 69.

Pun, A. (2023, February 3rd). *Fintech in 2023, the expert opinion and investor outlook*. Retrieved from EU Startups: https://www.eu-startups.com/2023/02/fintech-in-2023-the-expert-opinion-and-investor-outlook/

Qian, F., Liu, Y., & Fan, C. (2021). Exploring the role of explainable artificial intelligence in financial risk management education. *Journal of Financial Education, 47(2),, 47*(2), 109-127.

Rigby, A., Melo, E., Espinar, A. L., Carlucci, E., & Preciado, L. (2022). *A triple threat across the Americas: 2022 KPMG Fraud Outlook.* KPMG. Retrieved from https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2022/01/fraud-survey.pdf

Sartor, G., & Lagioia, F. (2020). *The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence.* Panel for the Future of Science and Technology (STOA), European University Institute of Florence. Brussels: Directorate-General for Parliamentary Research Services (EPRS) of the Secretariat of the European Parliament. Retrieved April 18, 2023, from https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf

Singh, A., & Bajaj, K. K. (2019). Impact of Explainable Artificial Intelligence on Consumer Behavior in the Era of GDPR. *Tthe 3rd International Conference on Computational Science and Technology (ICCST)* (pp. 1 - 6). IEEE.

The European Commission. (2020b, May). *The Pivotal Role of Rseah and Innovation in Artificial Intelligence Policy.* Retrieved from The European Commission: https://research-and-innovation.ec.europa.eu/system/files/2020-06/ec_rtd_ai-pivotal-role.pdf

Thomas, R. (2021, May 18). Retrieved from Introduction: Building the AI bank of the future | McKinsey: https://www.mckinsey.com/industries/financial-services/our-insights/introduction-building-the-ai-bank-of-the-future#/

Tsang, L., Wang, K., Combs, K., Blankstein, S., Du, B., & Kvedar, J. (2022). A Cross-Border Regulatory and Public Policy Analysis of Machine Learning and Artificial Intelligence: The Future of AI in Life Sciences. *ntellectual Property & Technology Law Journal, 34*(10), 3 - 11.

Turrini, L., Sartor, F., & Nalin, M. (2020). Explainable Artificial Intelligence: A Legal Perspective. *Computer Law & Security Review, 38, 38*.

Université de Montréal. (2017). *Montreal Declaration of Responsible AI*. Retrieved April 2023, from An initiative of Université de Montréal: https://www.montrealdeclaration-responsibleai.com/

Weaver, B. W., Braly, A. M., & Lane, D. M. (2021). Training Users to Identify Phishing Emails. *Journal of Educational Computing Research, 59*(6), 1015-1239.

World Economic Forum. (2020, January). *Shaping the Future of Artificial Intelligence and Machine Learning.* Retrieved April 2023, from World Economic Forum: https://www.weforum.org/projects/global-ai-action-alliance

Xue, W., Wang, Z., & Zheng, X. (2020). Teaching financial data analysis based on explainable artificial intelligence: A case study of stock price forecasting. *Journal of Financial Education, 46*(3), 193-207.

Yang, J., Zhu, X., & Pan, Y. (2021). Explainable AI in Credit Scoring. In D. Calvaresi, A. Najjar, M. Schumacher, & K. Främling, *Explainable, Transparent Autonomous Agents and Multi-Agent Systems* (pp. 177-191). Springer International Publishing.

Yu, L., Guo, X., & Fan, Z. (2019). Explainable Artificial Intelligence (XAI) in Fintech. *the 2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)* (pp. 764-768). IEEE.

Zhang, J., Y., Y., & Z, Z. (2021). Explainable Artificial Intelligence in Fintech: Opportunities and Challenges. *Journal of Business Research, 136*, 137-148.

Acknowledgements

This work has been supported by several institutions, each of which has provided vital resources and expertise to the research project.

Firstly, we acknowledge the COST Action CA19130 and COST Action CA21163, under the auspices of the European Cooperation in Science and Technology (COST). COST Actions provide networking opportunities for researchers across Europe, fostering scientific exchange and innovation. This has been particularly beneficial for this research project on financial econometrics.

We gratefully acknowledge the support of the Marie Skłodowska-Curie Actions under the European Union's Horizon Europe research and innovation program for the Industrial Doctoral Network on Digital Finance, acronym: DIGITAL, Project No. 101119635. Their significant contribution has been instrumental in advancing our research and fostering collaboration within the digital finance field across Europe.

We would like to express our gratitude to the Swiss National Science Foundation for its financial support across multiple projects. This includes the project on Mathematics and Fintech (IZCNZ0-174853), which focuses on the digital transformation of the Finance industry. We also appreciate the funding for the project on Anomaly and Fraud Detection in Blockchain Networks (IZSEZ0-211195), and

for the project on Narrative Digital Finance: a tale of structural breaks, bubbles & market narratives (IZCOZ0-213370).

In addition, our research has benefited from funding from the European Union's Horizon 2020 research and innovation program under the grant agreement No 825215 (Topic: ICT-35-2018, Type of action: CSA). This grant was provided for the FIN-TECH project, a training programme aimed at promoting compliance with financial supervision and technology.

Lastly, we acknowledge the cooperative relationship between the ING Group and the University of Twente. This partnership, centered on advancing Artificial Intelligence in Finance in the Netherlands and beyond, has been of great value to our research.

These partnerships and funding sources have greatly contributed to our ability to conduct rigorous and impactful research. Our findings are our own and do not necessarily represent the views of the supporting institutions.

Cal Muckley would like to acknowledge the financial support of Science Foundation Ireland under Grant Numbers 16/SPP/3347 and 17/SP/5447 and funding from the ADAPT Centre for Digital Content Technology, funded under the Science Foundation Ireland Research Centres Programme (Grant 13/RC/2106_P2), and co-funded by the European Regional Development Fund.

Codruta Mare acknowledges that this work was supported by the project “A better understanding of socio-economic systems using quantitative methods from Physics” funded by the European Union – NextgenerationEU and the Romanian Government, under National Recovery and Resilience Plan for Romania, contract no 760034/23.05.2023, cod PNRR-C9-I8-CF255/29.11.2022, through the Romanian Ministry of Research, Innovation and Digitalization, within Component 9, Investment I8”.

Disclaimer

The views expressed are those of the author and do not necessarily reflect those of the Piraeus Bank.