ARTIFICIAL INTELLIGENCE AND KEY RISK INDICATORS IN CYBER FRAUDS PREVENTION

Gabriel NIȚĂ[17]

Larisa GĂBUDEANU[18]

Cosmin Constantin CERNAEANU[19]

Gabriel Mărgărit RAICU[20]

Mircea Constantin ȘCHEAU[21]

Abstract:

Due to increasing economical impact due to the cyber fraud phenomenon, payment institutions allocate considerable resources to prevent this. An adequate implementation of risk indicators coupled with preventive mechanisms can lead to a decrease of losses. The protection mechanisms engineered through artificial intelligence could be a proper solution, but there are no specific legal requirements and frameworks for implementation and liability for such tools, aside from general cyber security, data protection and cyber-crime legal provisions. In this article we analyzed the impact of such preventive measures from multiple perspectives, including economical and legal. Our contribution entails a proposal for compliance evaluation of artificial intelligence tools for cyber fraud prevention, monitoring and adjustment thereof through analysis of the key risk indicator evolution over time.

Keywords: *risk management; risk-based prioritization; cyber fraud governance; damage prevention; financial protection*

JEL classification: *D81, K24, O31*

Introduction

According to a study by (World Economic Forum, 2022), cyber risk is one of the major global challenges. Financial institutions hold a significant amount of sensitive information (customers' personal and credit card details, bank account details, financial transactions) and financial assets, making them attractive targets for cyber criminals.

This form of operational risk refers to threats and vulnerabilities associated with cyber security and is characterized by a variety of manifestations: attacks on customer data, cyberattacks against financial institutions to gain access to and control over information systems, social engineering attacks, ransomware attacks etc.This types of cyberattacks can have significant financial consequences for both consumers and financial institutions, but can also lead to loss of customer

[17] *PhD Candidate, Babes-Bolyai University, Cluj, România. ORCID: 0009-0001-4940-7851.*
[18] *PhD Candidate, Babes-Bolyai University, Cluj, România. ORCID: 0000-0002-2562-5344.*
[19] *PhD Candidate, University of Craiova, România*
[20] *PhD Candidate, Constanta Maritime University, România, ORCID: 0000-0001-5956-7368.*
[21] *PhD, University of Craiova / Constanta Maritime University, România. Email: mircea.scheau@edu.ucv.ro / mircea.scheau@cmu-edu.eu . ORCID: 0000-0002-3847-5998.*

confidence and loss of reputation for banks.

For these reasons, the cyber fraud prevention process must focus on regulating and mitigating the cyber risks associated with this type of criminal behaviour. Risk indicators play a crucial role in fraud prevention at payment institutions. They help financial institutions identify and manage potential threats and risks associated with transactions and payments, helping to increase the sustainability of financial institutions by protecting their assets and reputation, customers, reducing costs and legal risks, and adapting to the evolving cyber security environment.

Current dynamics and trends in cyber fraud, however, make it difficult to prevent this criminal behaviour, as traditional security mechanisms are no longer sufficient and effective in protecting data and systems against new threats in the digital space. The existing legal framework and bodies responsible for cyber security often fail to keep pace with developments in cybercrime.

These new challenges require tailored and innovative responses, and the deployment of AI-enabled cyber defence systems may be an appropriate solution. The combination of traditional security technologies and the advanced capabilities of artificial intelligence technology can provide stronger protection against the increasingly complex and dynamic phenomenon of cyber fraud. Artificial intelligence capabilities compensate for the asymmetry between current cybersecurity mechanisms and the innovative methods used by cybercriminals to commit cyber fraud. Artificial intelligence technology helps to increase the detection rate of cyber fraud and is highly effective in identifying anomalies and irregular patterns.

The potential of artificial intelligence lies in identifying new or complex fraud schemes, monitoring transactions or analysing unique behavioural patterns in the user authentication process at a higher level than the current mechanisms implemented by financial institutions. Despite the benefits associated with the new technology, the excessive or predominant use of artificial intelligence tools in detecting, reducing or preventing fraudulent activities carries a number of risks arising from the lack of accuracy of the data processed and the technical imperfections of systems incorporating artificial intelligence, with negative consequences in providing erroneous decisions and increased exposure to cyberattacks.

The integration of artificial intelligence technology into operational risk management in the context of cyber fraud brings an advanced level of detection, prevention and protection against cyber threats, thus contributing to the increased efficiency and sustainability of financial institutions in the face of evolving cyber risks.

The lack of an adequate legal framework and the fragmented regulation or use of artificial intelligence systems in fraud prevention in the financial-banking sector complements the operational and technological risks. The current regulations do not expressly address artificial intelligence, applying provisions of several pieces of legislation adopted at european level (e.g. PSD2 Directive, NIS2 Directive, DORA Regulation, Cybersecurity Act, GDPR Regulation) or national level, thus making it necessary to update the regulatory framework in line with technological developments or to adopt specific legislation on artificial intelligence (e.g. proposed AIA Regulation and PSD3 initiative).

This interdisciplinary study analyses some of particularities, strengths and limitations of the artificial intelligence technology in the prevention of operational risks associated with cyber fraud in the financial-banking sector, as well as the impact of the existing regulatory framework and legislative proposals at European level, that affect the integration of artificial intelligence systems in policies and mechanisms for preventing this phenomenon in financial institutions.

The article is organized further as follows. section two presents the description of the problem from different angles, section three describes data and methodology, sections four introduce the results and proposals for adjusting the regulations and the final section presents the conclusions, the limits and future research directions.

Description of the Problem

The literature review highlights scientific concerns in analysing the potential and impact of artificial intelligence technology in preventing cyber threats. In this sense, we consider it eloquent the map in figure 1 that we managed to build using tools and databases in which we analyzed the prominence of keywords, objectives, hypotheses of interest for the present study and the relations between them.

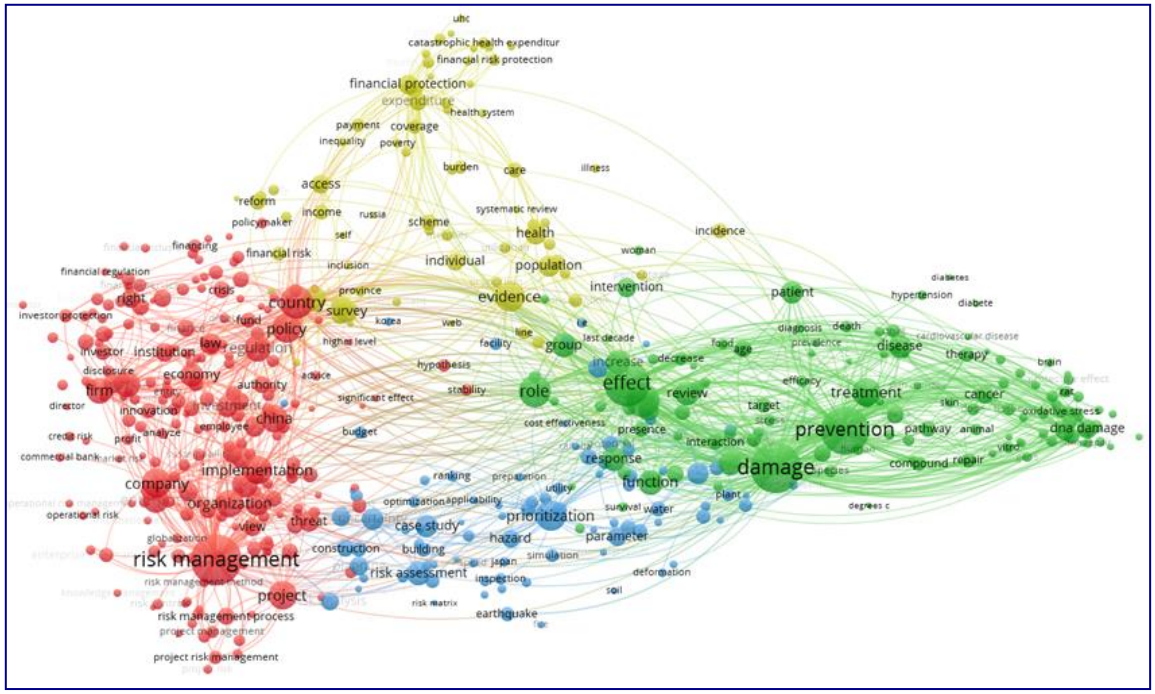

Figure 1 – Map of relevant articles reported to the keywords

Source: Authors'processing using the Web of Science database

Researchers (Ahsan et al., 2022; Zang et al., 2022; Zeng, 2022; Tao et al., 2021; Sarker et al., 2020; Pupillo et al., 2019; Wirkuttis and Klein, 2017; Azhar, 2016) have generally focused on the interactions between artificial intelligence technology and cybersecurity, highlighting the new technology's contributions to substantially improving traditional cybersecurity practices. The relationship between artificial intelligence technology and cyber security is ambivalent: on the one hand, artificial intelligence systems are increasingly used to help detect, prevent and respond to cyber threats; on the other hand, cyber security can be the cornerstone of ensuring safety and trust in artificial intelligence systems. Recent studies (Kaur et al., 2023; Capuano, 2022; Naik et al., 2022; Mathew, 2021; Wiafe et al., 2020) have highlighted the significant contribution of cybersecurity systems enabled by artificial intelligence technology especially in relation to the prevention and detection of cybersecurity incidents: unauthorised access, malware, cyber fraud, phishing, DDos attacks, cryptojacking, zero-day attack, privilege escalation and others.

Artificial intelligence technology is also having a major impact on the effective implementation of cyber governance in the financial and banking sector, revolutionising the way financial risks are managed. The authors (Bozic, 2023; Josyula et al., 2023; Berrada et al., 2022; Lindqvist and Khailtash, 2022; Fares et al., 2022; Fritz-Morgenthal et al., 2022; Milojević and Redzepagic, 2021; Leo et al., 2019; Soni, 2019; Aziz and Dowling, 2018) generally demonstrate the potential of the new technology to support financial institutions in analysing credit risk, financial transactions, protecting personal data or managing operational risks associated with cyber fraud. Considerable research (Mytnyk et al., 2023; Rutskiy et al., 2023; Btoush et al., 2023; Aziz and Andriansyah, 2023; Chang et al., 2022; Bao et al., 2022; Raj and Choudhary, 2022; Priya and Saratha, 2021; Erdoğan et al., 2020; Ryman-Tubb et al., 2018) has been conducted on the contribution of artificial intelligence technology

to fraud prevention at financial institutions by preventing and detecting suspicious or fraudulent transactions. The relationship in our own vision between artificial intelligence and financial risk management is presented in figure 2.

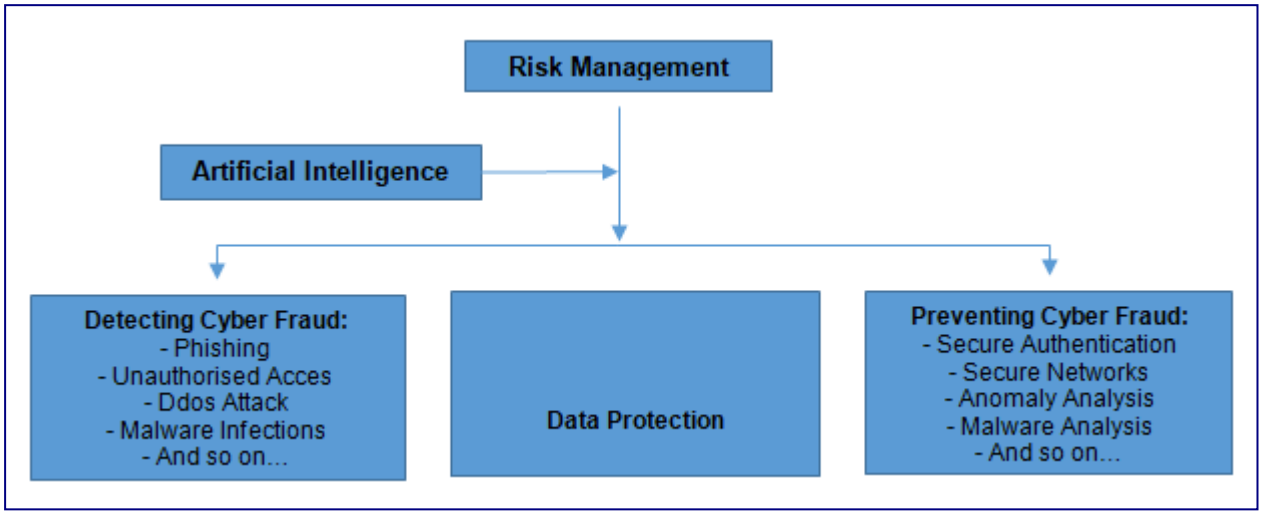

Figure 2 – Artificial Intelligence and Financial Risk Mnagement

Source: Authors' processing

It is important that in the implementation of artificial intelligence in risk management at the level of financial institutions, attention should also be paid to the aspects of ensuring digital operational resilience provided for in specific legal instruments, with some authors assessing compliance with the provisions of the GDPR (Mantelero, 2019; Jackson, 2019; Wachter et al., 2017), the Cybersecurity Act (Casarosa, 2022; Calliess and Baumgarten, 2020), the proposed AIA Regulation (Floridi L., 2022; Smuha et al., 2021) and the DORA Regulation (Alibrandi et al., 2023; Krüger and Brauchle, 2021; Pavlidis G., 2021).

The literature has also addressed the major issues, gaps and limitations in the use of artificial intelligence techniques to prevent cyber threats and therefore cyber fraud. With the ability to process large amounts of data and make decisions without human oversight, intelligence systems still pose significant risks related to data privacy and vulnerability to cyber-attacks, further exacerbating cybersecurity threats (Hendrycks et al., 2022; Kaminski, 2023; Scherer, 2016). Artificial intelligence technology can also be exploited by cyber actors for criminal purposes (Choras and Wozniak, 2022; Blauth et al., 2022; Ciancaglini et al., 2020; Comiter, 2019; Brundage et al., 2018), contributing to the sophistication and diversification of the tools used by cyber actors to commit cybercrime: AI-malware, AI-assisted hacking, custom social engineering attacks, passing cybersecurity filters.

Preventing risks associated with artificial intelligence involves multiple technical, legal and ethical approaches: transparency and explainability, data protection and privacy, artificial intelligence algorithm auditing and accountability, regulations and standards. The doctrinal approaches from this perspective alternate from the analysis of ethical frameworks for the governance of artificial intelligence (Fjeld et al., 2020; Jobin et al., 2019), the adoption of strict regulations based on risk assessment to the adequacy (de Almeida et al., 2021; Schuett, 2023) of regulatory frameworks protecting human rights (Mantelero, 2022; Yeung, 2019; Latonero, 2018; Raso. et al., 2018).

The results of the literature review indicated that the use of artificial intelligence systems in fraud prevention is increasing, but can still be seen as a new phenomenon requiring further research on the potential of the new technology in assessing and identifying risk indicators associated with cyber fraud and the impact of the new legal instruments adopted at European level (PSD3 proposal and DORA Regulation) to ensure digital operational resilience with regard to such instruments.

Methodology and Data

In order to be able to come up with proposals for improving the general framework regarding artificial intelligence and key risk indicators in cyber frauds prevention, we start from a few hypotheses within some objectives that we state in the following, the results to be centralized in the next chapter. Also, in this chapter we will present some concrete examples, through which to highlight the statements. However, we must mention, that the issues analyzed can be approached from different other angles, this aspect being mainly determined by the context and the goals that want to be achieved.

Objective 1 (O1) – Identifying the impact of artificial intelligence and related key risk indicators on cyber fraud prevention

Hypothesis 1. (H1.1). (Regarding O1) – Current dynamics and trends in cyber fraud create difficulties in preventing this criminal behaviour.

Key Risk Indicators (KRIs) is a tool for measuring a potential risks who can provide data and prioritize the response to various threats.

The risk profile of an organization can be established with the help of these changing measurement tools.

We can have a look now to the five KRIs for really understand the potential risk should be aware of: Scope of attack surface, Presence of malware, Unpatched or misconfigured systems, Third party risk and Financial Exposure.

Scope of attack surface - This first tool refers to the identification of the risk in the digital environment, scanning the attack surface is a first method in this sense, making an automatic inventory.

Presence of malware - Obtaining visibility in malware activity is critical to reducing your companies' cyber risk exposure.

Unpatched or misconfigured systems - A misconfigured system can be a significant indicator of risk.

Third party risk - By monitoring the group of suppliers, you collaborate with, you can identify and reduce this relational risk.

Financial Exposure - The management of an organization must allocate sufficient resources and a significant expertise in order to manage the cyber risk and to be aware of the impact of a possible ransomware attack.

According to **(**The National Institute of Standards and Technology, 2023), the Cyber Security Framework includes 5 important functions: Identification, Protection, Detection, Response and Recovery. Identification offers raise awareness of cyber security risk for people, assets, systems, capabilities and data. The protection function refers to the implementation of appropriate measures to limit the impact of a potential cyber security event. The Detect function means the timely identification of Cyber Security problems. The Response function refers to the appropriate activities taken in the event of a Cyber Security incident. The Recovery function helps in the timely recovery of affected operations following a Cyber Security incident.

Opportunities and barriers by using AI in cyber fraud detection - an insurance companies' case.

As risk management systems have failed to keep up with highly sophisticated security attacks, industries around the world have witnessed a rapid and sudden increase in the number of cyber-attacks and all this phenomenon started since the onset of the COVID-19 pandemic.

Opportunities- Claim Predictions- Artificial intelligence can be used to estimate insurance claims. Against phishing, the NLP application is used, which recommends the interaction of people with machines. Through NLP, large amounts of data can be scanned regarding e-mail conversations. It is possible to identify certain patterns regarding malicious behavior by recording all e-mails entered into the organization's network.

Barriers – Cyber risks – Artificial intelligence includes damage assessment, human resources, IT or legislative changes. AI systems being very fast can learn about regulations, laws or changes, decisions can also be made quickly. The major concern relates to when decisions can actually be made by AIs as well as their accountability. The use of AI to filter data can pose a real threat to customer privacy when it comes to media accounts, internet searches, or terms and conditions obtained directly from credit card companies. Time restrictions are required on the use of this confidential information.

Discrimination Based on Characteristics - Serious threats of bias are prohibited by the anti-discrimination rules by which statistics can disparage some protected attributes. There is an Equality legislation Act (United Kingdom Government, 2010) that prevents insurers from using certain algorithms that offer discrimination based on physical characteristics.

According to (Comming, 2023), The Financial Conduct Authority (FCA) sent a warning to companies in the financial sector regarding AI fraud activity**)**. The phenomenon has grown a lot in the last period both in sophistication and scope, cyber-attacks as well as identity fraud have become a real danger. The FCA also promotes the benefits of AI, but mentions the need for better cyber regulations. The risks of fraud, deepfake, have been highlighted by the FCA. The CEO of FCA, Nikhil Rathi, which mentioned the fact that the entire financial services sector could be disrupted by artificial intelligence "in ways and on an unprecedented scale". Must be taken important measures against the ever-growing frauds based on AI. He also said: ,,As AI continues to be adopted, investment in fraud prevention and operational and cyber resilience will need to accelerate simultaneously".

Cybercriminals are keeping their attacks under the radar with methods of taking money, without security teams finding out, through bitcoin payment requests, according to new research into scam activity.

The Benefits and Limitations of Using AI and Machine Learning for Fraud Detection

Fraud Detection Machine Learning

Fraud detection is the process by which fraudulent activities are identified and prevented within a company. In table 1 we present some examples of cybersecurity detection systems that operate in a different way and thus prove that the same problem can be solved - partially, because it is difficult to say that there is a universal detection system.

Traditional detection methods are inflexible and rigid, which makes it almost impossible to correctly adapt to new types of fraud. AI and ML have revolutionized the fraud detection process. Large amounts of data can be analyzed in real time, fraudulent activity being able to detect patterns and anomalies.

Table 1

Examples of cybersecurity detection system

Amazon Guard Duty	IBM Watson for Cybersecurity	Cylance Protect	Splunk User Behavior
It is a system based on artificial intelligence that detects cyber threats in real time and analyzes Amazon CloudWatch (AWS) logs.	It is another powerful AI-based threat detection system through which data is analyzed from multiple sources such as security alerts or logs. If traditional security systems can miss certain threats, IMB Watson for Cybersecurity can identify them.	This system uses ML to detect and prevent cyber threats. Its predictive type can block malicious processes before they are executed on the final point.	The specification of this system refers to identifying and responding to anomalous behavior in a network. Internal threats related to employees who access certain sensitive data are identified.

Source: Authors' processing

Another powerful application of AI and ML in fraud detection is the detection of anomalies, by identifying unusual patterns of behavior. If a customer suddenly makes large purchases from a new location, this could be a sign of fraud. Vision artificial is a powerful tool in fraud detection because it uses computer vision to analyze images and videos, counterfeit goods can be detected by watching surveillance footage to identify people.

Hypothesis 1.2 (H1.2). (Regarding O1) - The use of artificial intelligence in cyber fraud prevention will lead to a significant increase in fraud detection rates.

Artificial intelligence, especially machine learning (ML) can have a decisive, significant role in the discovery of information from data. ML automates the process of prioritizing relevant data, finding and contextualizing processes in the life cycle of information, these refer to detection of dark web forum posts that lead to a data breach. Processes can be improved by using ML, and specialists, security analysts can treat, remediate or identify new attacks, helping in this sense to quickly develop responses and an understanding better of cyber-attacks.

The most sophisticated algorithms are used to recognize patterns before they are infiltrated into the system, to identify the smallest behaviors, changes in ransomware attacks or to detect malware. AI has a superior predictive intelligence through which it processes natural language in order to manage data, by analyzing studies, news or published articles. Security teams understand better, in this sense, prevention strategies, cyber-attacks or anomalies, as cyber criminals are always in trend with trends. Threats specific to a certain industry or global threats are identified by the Cyber Security systems powered by AI.

Data fraud or account takeover is a risk due to the fact that robots are a substantial part of internet traffic, but organizations can be helped in this sense by AI and ML through a much better understanding of website traffic and through a differentiation between human users, good robots or bad robots.

Objective 2 (O2) - Analysis of the existing legal framework with impact on the use of artificial intelligence in fraud prevention and proposals for improvement of fraud detection legal provisions

Hypothesis 2.1 (H2.1). (Regarding O2) - The existing legal framework and bodies responsible for cyber security often do not keep pace with developments in cybercrime

The exponential increase in bank cyber fraud is explained by the inefficiency and insufficiency of traditional detection and prevention methods (mainly due to a low detection rate, lack of resilience and autonomy), requiring innovative and intelligent mechanisms adapted to the new cyber threat architectures. Clear policies and procedures are also needed, which unfortunately either do not exist or are not properly implemented. The size of the institutional architecture for cyber security involves several bodies in fraud prevention, which is why there is a fragmented approach in tackling the criminal phenomenon and leads to under-reporting of incidents by users due to mistrust and confusion in reporting to the competent authorities. For these reasons, a rethink of the institutional framework is needed.

As there is a pressing societal need to prevent such criminal conduct, priority should be given to strengthening the capacity of cybersecurity bodies by developing solutions incorporating new digital technologies or enhancing cooperation with private parties that have implemented such programmes.

Prevention is one of the most effective ways to combat bank cyber fraud, but this process needs to be adapted to cyber realities and artificial intelligence technology may be the right solution.

The combination of traditional security technologies and the advanced capabilities of artificial intelligence technology provide stronger protection against the increasingly complex and dynamic phenomenon of cyber fraud. According to (European Union Agency for Cybersecurity, 2020) report, *"AI Cybersecurity Challenges. Threat Landscape for Artificial Intelligence"*, artificial intelligence systems can be an advanced tool in cybersecurity by developing more effective security controls and facilitating law enforcement efforts to better respond to cybercrime, including analysis of the exponential growth of Big Data in the context of investigations as well as crime in the misuse of artificial intelligence.

The value and opportunities of artificial intelligence in cybersecurity has been highlighted and contained in a number of policy legal instruments. At European Union level, Directive (EU) 2022/2555 (or NIS 2 Directive) of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148, the EU Cyber Security Strategy for the Digital Decade and the EU Security Union Strategy, highlight that artificial intelligence or machine learning systems are useful to strengthen the capabilities and security of networks and information systems against cyberattacks. In the same vein, the UK's National Cyber Security Strategy (2022), Germany's Cyber Security Strategy (2021) and Italy's National Cyber Security Strategy for 2022-2026 (2022) highlight the usefulness of integrating artificial intelligence techniques into cyber defence systems.

Artificial intelligence models can help automate cybersecurity, ensuring predictability and ensuring an effective response to cyber threats. Systems enabled by artificial intelligence technology are used for automated malware analysis, intrusion detection (by automatically identifying user access), spam detection, mobile (android) malware detection, botnet detection, advanced ("next-gen") antivirus software development, security breach prediction, authentication and password protection, phishing detection, network traffic monitoring (to identify anomalies), identification of vulnerable areas, data encryption.

According with (European Union Agency for Cybersecurity, 2021), while artificial intelligence helps substantially improve cybersecurity practices, at the same time, facilitates new forms of attacks and further exacerbate security threats.

Regarding the GDPR, we can say that GDPR has certain limitations: it is not global, it contains specific rules for certain types of automated individual decision-making, but not for collective decisions, the vague provisions of the GDPR will facilitate the process of "de-identification" (anonymisation, pseudonymisation), it leaves Member States free to adopt or supplement provisions at national level, which leads to conflicting interpretations, does not provide the right to explain all algorithmic decisions, but only those that have a legal or significant effect.

It should be noted that not all artificial intelligence applications use personal data and therefore some uses may not have privacy implications, in which case the provisions of Regulation (EU) 2018/1807 of the European Parliament and of the Council on on a framework for the free flow of non-personal data in the European Union become applicable.

It is debatable to what extent artificial intelligence can ensure the integrity, confidentiality and availability of computer data and how it can contribute to ensuring a sufficient level of cyber security, given that this technology can represent a vulnerability (incorrect algorithm, technical flaws that can be exploited by cyber criminals) or threat (algorithm can develop cyberattacks).

To prevent vulnerabilities, the Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act/AIA) and amending certain Union legislation (COM/2021/206 final) of 21.04.2021 complements the need to specify cyber security requirements for artificial intelligence based on a certification scheme under the proposed European cyber security certification framework. The certification process ensures that specific artificial intelligence technologies comply with security standards not only in the area of product safety but also in the area of cyber security.

The forthcoming AIA proposes a risk-based approach to artificial intelligence systems (unacceptable risk, high risk, limited risk, minimal risk), rather than a rights-based approach as in the GDPR. The European Commission proposes that national competent market surveillance authorities oversee the new rules, while the creation of a European Artificial Intelligence Council will facilitate their implementation and stimulate the development of artificial intelligence standards.

The proposed Artificial Intelligence Regulation overlaps in relation to the certification process with Regulation (EU) 2019/881 of the European Parliament and of the Council on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). Although the AIA suggests a possible path towards mutual recognition of certifications, a closer analysis of the provisions and a comparison of the underlying features of the certification mechanisms shows that

the different approaches taken in the two acts may undermine the objective of certification mechanisms as trust-building and transparency tools.

Similarly, the proposal for a Regulation on Artificial Intelligence overlaps in relation to the conformity assessment procedure with the Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, COM(2022) 454 final (Cyber Resilience Act). This legal instrument strengthens cybersecurity rules to ensure more secure hardware and software products, and its provisions are extended to artificial intelligence applications.

The proposed new EU regulatory framework for artificial intelligence has been the subject of criticism and debate in the technological and legal community. Some critics, like (Tadeo, 2021) argue that the proposed Regulation could limit innovation and progress of new technology by placing strict rules and requirements on developers and users. The proposed Regulation focuses on compliance assessment and less on fundamental rights impact assessment on perspective of (Smuha et al., 2021) and is out of sync with the provisions of other EU legislation (such as the GDPR legislation - it does not provide for data subjects' rights and the authorities where complaints can be lodged). Also (Smuha et al., 2021) states that the provisions of the future Regulation only offer providers the possibility to assess risks, there are no provisions for sanctions in case of non-compliance and no authorities to supervise this process, while compliance of artificial intelligence products with private standards presents risks (Ebers et al., 2021).

Hypothesis 2.2 (H2.2). (Regarding O2) - The importance of the legal framework developed by PSD3 and DORA on the use of artificial intelligence in the prevention of cyber fraud

The (European Banking Authority, 2022) report, *"Risk Assessment of the European Banking System"*, highlights that 83% of banks across Europe are already exploring artificial intelligence applications, while 12% are testing such tools. In view of the large-scale integration of artificial intelligence techniques in the financial-banking sector, coupled with the risks associated with the new technology, through a series of publicly available technical reports, financial regulators (Cakzolan, 2021; The Organization for Economic Cooperation and Development, 2021; Financial Stability Institute, 2021;, European Central Bank, 2021; European Banking Federation, 2021), have highlighted the need to adopt a specific regulatory framework in this area.

For these reasons, also the (European Commission, 2021) highlights in its report *"Study on the relevance and impact of artificial intelligence for company law and corporate governance"* that the financial sector is one of the segments of the European market where clear rules are needed to regulate artificial intelligence. The capabilities of artificial intelligence tools would ensure higher levels of digital operational resilience of the EU financial system and reduce the number and average cost of incidents.

So far, only a few regulatory provisions at European level seem to be relevant to the adoption of artificial intelligence applications in the financial-banking sector, namely: Directive (EU) 2015/2366 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 (or PSD2); Regulation (EU) 2022/2554 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (or DORA); Proposal for a Directive on payment services and electronic money services in the Internal Market amending Directive 98/26/EC and repealing Directives 2015/2366/EU and 2009/110/EC, COM (2023) 366 final (or PSD3); Proposal for a Regulation on payment services in the internal market and amending Regulation (EU) No 1093/2010, COM (2023) 367 final (or PSR); and Regulation (EU) 2023/1114 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (or MiCA).

The DORA Regulation was prompted by the absence of detailed and comprehensive rules on digital operational resilience for financial entities, given their high reliance on ICT services (including artificial intelligence applications) and their vulnerabilities to cyberattacks. The adoption of the Regulation as a regulatory instrument ensures, on the one hand, the creation of a common legal framework for Member States and, on the other hand, the avoidance of fragmented approaches at national level in order to ensure the digital operational resilience of the financial sector in the

European Union. Although it does not expressly address artificial intelligence applications used by financial entities in the prevention of operational risks associated with cyber fraud, the definition of ICT risks in Article 3(5) is comprehensive and may be appropriate to include risks related to new technology.

In order to ensure consistency in relation to the ICT risk management requirements applicable to the financial sector, the Regulation covers the majority of regulated financial entities at Union level implementing AI-assisted cyber fraud prevention tools, in addition to third party ICT providers. For financial entities, the comprehensive approach suggested by the DORA implies first of all ensuring full compliance of implemented technologies with the relevant regulatory framework: Art. 5 - governance and organisation, Art. 6-18 - ICT risk management framework, and Art. 24-27 - testing of ICT tools and systems. This requirement will be particularly important for the governance of artificial intelligence systems used by financial entities, given the absence of a set of rules specifically related to these tools in the context of preventing cyber fraud.

In accordance with Article 5, where artificial intelligence systems are being used, it is expected that financial institutions will amend existing governance processes or create specific artificial intelligence process to address risks which may arise from artificial intelligence decision making. This is particularly important where high risk AI systems are being used and/or where personal data is processed by artificial intelligence. Referring to the provisions of Articles 6-18, security policies and procedures implemented in accordance with de requirements of DORA should look also address artificial intelligence specific concerns and risks, alongside security requirements for the broader ICT network across the financial services business.Practically, the services provided using artificial intelligence tools in a financial services context will include a number of types of services considered by DORA as ICT services, such as data monitoring, data processing and decision support services.

The provisions of the DORA set out specific steps for the governing bodies of financial entities to guide and adapt the risk management framework associated with cyber fraud and to ensure compliance when using AI-assisted prevention tools. It should be noted, however, that in this case the legal framework proposed by the future AIA Regulation on the certification of high-risk artificial intelligence systems does not synchronise with the provisions of the DORA. The coexistence of multiple legal frameworks applicable to the certification process of artificial intelligence systems may lead to legal uncertainty. At doctrinal level, it is considered by (Latonero, 2018; Mantelero, 2018) that is premature to regulate the certification process of artificial intelligence systems, given a number of unknown risks, and the Human Rights Impact Assessment (HRIA) is proposed as a tool during the life cycle of artificial intelligence systems.

Criticisms of the framework introduced by the DORA mainly concern the fact that many financial entities already have to comply with many different regulations or ICT guidelines. In the 2019 edition of its regulatory summary, the (World Bank Group, 2019) identified twenty-eight pieces of legislation, standards, guidelines and supervisory documents that have been issued by EU standard-setting bodies on cybersecurity for the financial sector. Twenty-five of the existing twenty-eight documents have been introduced since 2016, demonstrating the EU's focus on this topic in recent years. To these are added a plethora of authorities with fraud prevention competences that only dilute the fight against cyber threats, thus reconfiguring the institutional framework.

The DORA also does not set out exactly which financial institutions will have to carry out these advanced tests, delegating this task to the competent authorities (EBA, ESMA and EIOPA).

PSD2 was the first European regulation in the financial services sector to specifically specify concrete requirements for cyber security and ICT risk management. Since the adoption of Directive (EU) 2015/2366, the market for retail payment services has undergone significant changes, largely related to the increasing use of cards and other digital means of payment, the declining use of cash and the growing presence of new players and services, including e-wallets and contactless payments. The COVID-19 pandemic and the transformations it has brought to consumption and payment practices have increased the importance of secure and efficient digital payments.

The European Commission, taking into account market developments, has announced in its Communication COM (2020) 592 final on an EU Retail Payments Strategy the launch of a comprehensive review of the application and impact of Directive (EU) 2015/2366. Thus, through a

study on the application and impact of Directive (EU) 2015/2366, the (European Commission, 2023), analysing the main trends affecting the payments market and the performance of the Directive in terms of relevance, effectiveness, efficiency, consistency and added value at EU level, identified four fundamental problems, despite the achievements of PSD2, as follows: consumers are at risk of fraud and lack confidence in payments, the open banking sector operates imperfectly, supervisors in EU Member States have inconsistent powers and obligations, there is an uneven playing field between banks and non-bank PSPs.

For these reasons, on 28.06.2023, the European Commission published the proposals for the third Payment Services Directive (PSD3) and the new Payment Services Regulation (PSR).

Compared to the PSD2 Directive, the PSD3 framework introduces certain authorisation requirements for payment institutions setting out specific rules on security controls and mitigating measures in the field of information and communication technology, aligned with the DORA provisions. Thus, the security control and mitigation measures (whether or not assisted by artificial intelligence technology) referred to in Article 3(3)(j) indicate how the natural or legal person being registered will ensure a high level of digital operational resilience in accordance with Chapter II of Regulation (EU) 2022/2554, in particular as regards technical security and data protection, including for the ICT software and systems used by the natural or legal person being registered or by the undertakings to which all or part of its activities are outsourced. To this end, in accordance with Article 3(5)(a), EBA will develop draft regulatory technical standards to specify: the information to be provided to the competent authorities in the application for authorisation of payment institutions.

Artificial intelligence technology it is used to detect suspicious or fraudulent transactions in real time. By analysing behavioural patterns and historical data, artificial intelligence can more effectively identify unusual or potentially dangerous activity and alert banks or payment service providers to prevent fraud. Correlatively, contributes to strengthening data security and privacy protection, which are essential under PSD3. AI technologies can be used to monitor and protect customers' financial and personal data, thus contributing to compliance with data protection regulations. Last but not least, the new technology helps banks and payment service providers better assess risks and comply more effectively with PSD3 requirements. Through data analytics, artificial intelligence helps to identify and manage cybersecurity risks and assist in appropriate reporting to regulators.

Results

According to (Weigand, 2023), when AI and automation are adopted by attackers, the speed of these types of attacks will be higher and the number of them will increased. In July of this year, 50,000 more attacks were detected in July than in May 2023. Traditional techniques (firewall, antivirus software or IDS) are no longer sufficient and effective in protecting systems against new threats in the digital space, state (Ahsan et al, 2022; Sarker et al., 2020; Wirkuttis and Klein, 2017; Li, 2018).

Due to fraud, which is an ever-increasing problem, companies lose billions of dollars annually. To reduce this phenomenon, artificial intelligence and automatic learning are often used, in order to substantially improve fraud detection capabilities. Fraud mechanisms for all Internet banking and card transactions present features that can help detect fraud, such as location of payment initiation, payment dates, account holder behavior during payment transactions or different characteristics of payments (unusually large payments, transfers to other jurisdictions), relevant historical data about electronic transactions from the systems and platforms involved in the payment or transaction process (algorithms can learn past fraudulent behavior or detect new types of fraud). Data quantity and accuracy are crucial to the effectiveness of e-fraud prevention intelligence tools. For detection of fraud, predictive modeling is one of the most powerful applications of AI and ML. The great advantage is the identification of fraud before it occurs.

Artificial intelligence and machine leaning will strongly influence the future of fraud detection, they will constantly improve, which will facilitate their prevention and detection. However, there are also real concerns about the use of AI and ML regarding confidentiality and bias. It is recommended to

collaborate with specialized companies and specialists to analyze massive amounts of data in real time by identifying anomalies and models that can lead to fraudulent activities.

As long as technology has started to play an increasingly important role in our lives, the threat of cybercrime can represent a significant challenge for governments, companies or even individuals. As conventional cyber security measures try to keep up and to control this phenomenon, the criminals becoming more prepared and more refined for this reason, the use of artificial intelligence began to open new technological developments and cyber security systems, aimed at combating cyber-crime.

Artificial intelligence capabilities compensate for the asymmetry between current cybersecurity mechanisms and the innovative methods used by cybercriminals to commit cyber fraud. The integration of artificial intelligence with traditional technical security measures is revolutionizing cyber fraud detection and prevention systems, with algorithms able to quickly and accurately processing large volumes of information to find suspicious transactions and patterns of fraudulent activity. Artificial intelligence models can help automate cybersecurity, ensuring predictability and ensuring an effective response to cyber threats. Artificial application can be found for intelligence purposes for automatic analysis of, intrusion detection (by automatically identifying user access), spam detection, mobile (android) malware detection, botnet detection, development of advanced ("next-gen") antivirus program), prediction of security breaches, authentication and password protection, phishing detection, network traffic monitoring (to identify anomalies), identification of vulnerable areas, data encryption. However, there are also limitations in the use of artificial intelligence technology in the process of cyber fraud prevention, mainly caused by the lack or insufficiency of data sets regarding the innovative schemes of cyber criminals, as well as by the legislative conditions in the matter of personal data processing.

The ability to process large amounts of data and make decisions without human oversight, artificial intelligence systems pose significant risks related to data privacy and vulnerability to cyberattacks. As artificial intelligence systems collect and process significant amounts of data, there is a risk of intentional manipulation through breaches of technical security measures or accidental leaks of data that can later be used to commit other cybercrimes (identity theft, computer fraud, etc.). The technical imperfections of artificial intelligence systems increase the risk of exposure to cyberattacks (adversarial attacks). In addition to these technical security challenges, there are ethical concerns around artificial intelligence decision-making and lack of regulation.

Table 2

Table on regulations concerning the use of artificial intelligence technology in cyber fraud prevention

Legislation	Scope	Regulatory act	Regulatory initiative	Recommendations
GDPR Regulation	Protection of personal data processed by artificial intelligence systems in the context of cyber fraud prevention	X		-introduction of the right to explainability of systems integrating artificial intelligence technology -introducing the right to contest algorithmic decisions -requiring institutions to regularly monitor the performance of artificial intelligence algorithms to identify any deviations or errors -setting up national supervisory bodies for the processing of personal data in the context of artificial intelligence
DORA Regulation	Digital operational resilience of AI-enabled cyber	X		-integration of provisions in a single European Cybersecurity legislation for a secure digital transformation and an

	fraud prevention systems			increased level of cyber resilience of financial sector -organisation of a data system used to train algorithms in the process of preventing cyber fraud in the financial-banking sector
AI Act	Classification and conformity assessment of artificial intelligence systems incident to the cyber fraud prevention process		X	-making risk assessment mandatory for financial institutions implementing high-risk AI-enabled systems (including those aimed at preventing cyber fraud) -the establishment of specific authorities to supervise this process -establishing legal compliance standards for artificial intelligence products, as private ones present risks -the supervisory powers over the provisions of the AIA should be vested in national artificial intelligence bodies rather than data protection agencies
PSD3 Directive	Strengthening the resilience of the payments sector		X	-stipulation of sanctions in case of non-implementation of appropriate cyber security measures by natural or legal persons -additional references on ensuring digital operational resilience to the entire cybersecurity certification framework in place at European level, not just DORA

Source: Authors' processing

To address these concerns, it is more than necessary to adopt specific requirements for cyber security, data privacy and ethical use of artificial intelligence technology. In this sense, as a personal contribution to improve the general framework, we present in table 2 a set of recommendations, whose necessity we try to explain in the following.

Referring to data privacy, Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR), while not expressly addressing artificial intelligence systems, contains a number of provisions relevant to the new technology. The GDPR introduces a set of definitions and principles that are not only unique, but also creates an ecosystem for new technologies, including artificial intelligence according to (Papakonstantinou and de Hert, 2022), and can be considered the first legal instrument on artificial intelligence according to (Nemitz, 2022). The GDPR has been driven by the development of new technologies (similar to the earlier adoption of Directive 95/46/EC on the protection of personal data, driven by Internet developments).

The GDPR regulations applicable to artificial intelligence concern the traditional data protection principles contained in Articles 5, 6 and 22: fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, limitation of automated decisions. Given the nature, scope, context and purposes of the processing, where a type of processing, in particular that based on the use of artificial intelligence, is likely to result in a risk to the rights and freedoms of the natural person, Articles 35 and 36 of the GDPR require the data controller to assess the impact of the processing of personal data. This assessment ensures transparency and protection in the processing of personal data. Moreover, the provisions of Articles 42 and 43 require certification mechanisms in order to guarantee the protection of personal data in the processing by means of artificial intelligence applications.

In this article we refer to the DORA and PSD3 provisions. The DORA regulation and the PSD3 proposal are part of the Digital Finance Package, which includes a new digital finance strategy for the EU financial sector, integrating digital technologies or information and communication

technologies in the financial sector, taking a risk-based approach in the interest of consumers. While the PSD3 proposal places an obligation on electronic payment service providers to prevent cyber fraud, the DORA Regulation lays down uniform requirements for the security of networks and IT systems that support financial entities' fraud prevention operational processes.

DORA aims to introduce a harmonised and comprehensive digital operational resilience framework for European financial institutions, setting out explicit requirements for addressing and mitigating ICT and cyber risks, including those associated with artificial intelligence tools used in cyber fraud prevention.

The proposal for a Directive on payment and electronic money services in the internal market amending Directive 98/26/EC and repealing Directives (EU) 2015/2366 and 2009/110/EC (or PSD3) focuses on the authorisation and supervision of payment institutions, but also lays down obligations on payment institutions to prevent cyber fraud. It should be noted that the PSD3 provisions in the area of cyber fraud prevention are closely related to the provisions of the DORA Regulation.

As in the case of DORA, PSD3 does not expressly refer to artificial intelligence systems. We appreciate, however, that artificial intelligence technology can be a valuable resource in implementing and complying with the requirements of the Proposal PSD3 and in developing innovative security solutions and financial services.

It must be understood very clearly that the applicability of the concepts can affect the financial field, public and private, equally badly or well, up to the rolling phenomenon that can affect all other fields with only a small step, and that is why the analysis and adopting measures capable of responding to as many threats as possible.

Conclusions

The field of Artificial Intelligence research is not new, the first notions being publicly presented in 1956 and it has been defined as an important section of exploration for several companies involved in the development of innovative technology. For a long time it was seen as an exclusive domain, difficult to interpret and especially to implement. The evolution was not necessarily linear, exponential or sinusoidal, nor was it directly proportional to the technological evolution, because it depended to a large extent on the importance given by the mathematicians who managed to identify the interconnection formulas on levels. The development of capabilities allowed the significant increase in the processing of a large amount of data in shorter periods, making possible not only the delivery of results, but also their collection from different sources, which led to an efficiency of the processes. The resources were available in the 20th century to a limited number of entities, the dynamics of the private environment, reallocation and mixed projects providing accessibility for the general public, both at the investor, owner and user level.

Collecting data from different sources is a powerful tool for acquisition, but poisoning or maliciously affecting them can cause significant damage through contamination. Machine Learning, as a sequel to Artificial Intelligence, must be trained so that it can distinguish between malicious or fake sources and genuine sources. For this, the initially loaded data set must be sufficiently consistent and the subsequent surveillance managed by humans or by programs designed in this sense, must be particularly focused, so that it can prevent unwanted intrusions or diversions from the purpose for which it was built.

In our specific case, Artificial Intelligence can interpret Key Risk Indicators in Cyber Frauds Prevention, but this does not exclude in any case that criminal actors use the same Artificial Intelligence to build attack schemes and to develop strategies to deceive the indicators, to results or to penetrate systems whose purpose is to protect against malicious or fraudulent actions. One of the measures to prevent, treat and combat the potential negative effects, is to regulate the domain, by this understanding the elaboration and alignment at the international level of normative acts, procedures for implementing the norms and of course, punitive measures in case they are not respected the legal provisions. This desire is also justified by the fact that the virtual space, to which Artificial Intelligence belongs as much as the field of Cyber Fraud, has no borders and depends

asynchronously on the time factor. In order for all the measures that we have presented and that we support to have the intended effect, it is absolutely necessary to create at the international level the appropriate mechanisms for verification, control and rapid intervention of the competent institutions, which have prerogatives in combating the criminal phenomenon. In this context, the proposals that we have presented in the the article become all the more important, the more noticeable, at the time of the preparation of this study, is a phenomenon of chaotic promotion, development and exploitation of Artificial Intelligence.

It must be understood and accepted that almost any innovation can be used, both for positive and negative purposes, both as defense tools and as attack tools

Future Directions

The limits of the study are determined by a lack of sufficient knowledge of the actual situation, because algorithms and technologies capable of acquiring, analyzing and processing information are continuously being developed, their purpose defying declared a priori and defying necessarily presented to the common public.

The future direction of study aims to identify as many concepts as possible that are the basis of MLtraining and the development of AI in order to be able to make a comparison in order to establish common points, differences and potential directions of action, precisely to come in support general efforts to combat the criminal phenomenon.

Acknowledgments

Author Contributions: Conceptualization, G.N, L.G., C.C.C., G.M.R. and M.C.Ș.; Methodology, G.N., L.B. and C.C.C.; Formal analysis, G.N., L.B. and C.C.C.; Investigation, G.N. and C.C.C.; Resources, G.N. and C.C.C.; Data curation and analysis G.N., L.B., C.C.C. and G.M.R.; Writing original draft preparation, G.N, L.G., and C.C.C.; Writing review and editing, G.M.R. and M.C.Ș.; Visualization, G.N, L.G., C.C.C., G.M.R. and M.C.Ș.; Supervision, L.B., G.M.R. and M.C.Ș.; Project administration, M.C.Ș. Funding acquisition, N/A.

Conflicts of Interest: The authors declare no conflict of interest

Data Availability Statement: The data used in this analysis are public

Funding: This research received no external fundings

Acknowledgment: This paperwork was carried out under the auspices of CNFIS-FDI-2023-F-0580 project, entitled "The development of the institutional capacity for research of the UMC by expanding the activities of scientific support and sustainability in conditions of regional resilience".

Bibliography

Agenzia per la Cybersicurezza Nazionale, Strategia Nazionale di Cybersicurezza 2022-2026, Published June 01, 2022, https://www.acn.gov.it/strategia-nazionale-cybersicurezza.

Ahsan, M., Nygard, K.E., Gomes, R., Chowdhury, M. (2022), Cybersecurity Threats and Their Mitigation Approaches Using Machine Learning – A Review, Journal of Cybersecurity and Privacy, 2(3), pp. 527-555.

Azhar, I.M. (2016), How Artificial Intelligence Is Changing Cyber Security Landscape and Preventing Cyberattacks: A systematic review, International Journal of Creative Research Thoughts, 4(2), pp. 659-662.

Alibrandi, A.S., Rabitti, M., Schneider, G. (2023), The European AI Act's Impact on Financial Markets: From Governance to Co-Regulation, European Banking Institute Working Paper Series no. 138, Frankfurt am Main.

Aziz, L.A.R., Andriansyah, Y. (2023), The Role Artificial Intelligence in Modern Banking: An Exploration of AI-Driven Approaches for Enhanced Fraud Prevention, Risk Management, and Regulatory Compliance, Reviews of Contemporary Business Analytics, 6 (1), pp. 110-132.

Aziz, S., Dowling, M. (2018), Machine Learning and AI for Risk Management, in Lynn, T. (ed.), Disrupting Finance, Palgrave Studies in Digital Business & Enabling Technologies, Rennes, pp. 33-50.

Bao, Y., Hilary, G., Ke, B. (2022), Artificial Intelligence and Fraud Detection, Innovative Technology at the Interface of Finance and Operations, in Babich, V., Birge, J.R., Hilary, G. (eds) Innovative Technology at the Interface of Finance and Operations. Springer Series in Supply Chain Management, 11, pp 223-247.

Berrada, I.R., Barramou, F.Z., Alami, O.B. (2022), A review of Artificial Intelligence approach for credit risk assessment, 2022 2nd International Conference on Artificial Intelligence and Signal Processing (AISP), Vijayawada, India, pp. 1-5.

Blauth, T.F., Gstrein, O.J., Zwitter, A. (2022), Artificial Intelligence Crime: An Overview of Malicious Use and Abuse of AI, IEEE Access, 10, pp. 77110-77122.

Božić, V. (2023), The Role of Artificial Intelligence in Risk Management, https://www.researchgate.net/publication/370005124_THE_ROLE_OF_ARTIFICIAL_INTELLIGENCE_IN_RISK_MANAGEMENT, [Accessed September 12th 2023].

Brundage, M., Avin, S., Clark, J., Toner, H. et al. (2018), The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation, https://arxiv.org/abs/1802.07228, [Accessed June 16th 2023].

Btoush, E.A.L.M., Zhou, X., Gururajan, R., Chan, K.C., Genrich, R., Sankaran, P. (2023), A systematic review of literature on credit card cyber fraud detection using machine and deep learning, PeerJ Computer Science, 9, https://peerj.com/articles/cs-1278.pdf, [Accessed September 14th 2023].

Calliess, C., Baumgarten, A. (2020), Cybersecurity in the EU The Example of the Financial Sector: A Legal Perspective, German Law Journal, 21, pp. 1149-1179.

Calzolari, G. (2021), Artificial Intelligence market and capital flows, Study for the Special Committee on Artificial Intelligence in a Digital Age, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg,https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662912/IPOL_STU(2021)662912_EN.pdf.

Casarosa, F. (2022), Cybersecurity certification of Artificial Intelligence: a missed opportunity to coordinate between Artificial Intelligence Act and the Cybersecurity Act, International Cybersecurity Law Review, 3, pp. 115-130.

Capuano, N., Fenza, G., Loia, V., Stanzione, C. (2022), Explainable Artificial Intelligence în Cybersecurity: A Survey, IEEE Acces, 10, pp. 93575-93600.

Chang, V., Doan, M.T., Di Stefano, A., Sun, Z., Fortino, G. (2022), Digital payment fruad detection methods in digital ages and Industry 4.0, Computer and Electrical Engineering, 100, https://www.sciencedirect.com/science/article/abs/pii/S004579062200046, [Accessed September 19th 2023].

Choras, M., Wozniak, M. (2022), The double-edged sword of AI: Ethical Adversarial Attacks to counter artificial intelligence for crime, AI and Ethics, 2, pp. 631-634.

Ciancaglini, V., Gibson, C., Sancho, D., McCarthy, O., Eira, M., Amann, P., Klayn, A., McArdle, R., Beridze, I. (2020), Trend Micro Research.

Comiter, M. (2019), Attacking Artificial Intelligence, Belfer Center for Science and International Affairs, Harvard Kennedy School.

Cumming, A. (2023), AI has the change to disrupt the financial services sector, Business Leader LTD, https://www.businessleader.co.uk/ai-has-the-change-to-disrupt-the-financial-services-sector/, [Accessed September 29th 2023]

de Almeida, P.G.R., dos Santos, C.D., Farias, J.S. (2021), Artificial Intelligence Regulation: a framework for governance, Ethics and Information Technology, 23, pp. 505-525.

Ebers, M., Hoch, V.R.S., Rosenkranz, V., Ruschemeier, H., Steinrötter, B. (2021) The European Commission's Proposal for an Artificial Intelligence Act – A Critical Assessment by members of the Robotics and AI Law Society, Multidisciplinary Scientific Journal, 4, pp. 589-603.

European Union Agency for Cybersecurity (ENISA), Artificial Intelligence Cybersecurity Challenges. Threat Landscape for Artificial Intelligence, https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges, Published December 15, 2020.

European Union Agency for Cybersecurity (ENISA), Securing Machine Learning Algorithms, https://www.enisa.europa.eu/publications/securing-machine-learning-algorithms, Published December 04, 2021.

Erdoğan, I., Kurto, O., Kurt, A., Bahtıyar, Ş. (2020), A New Approach for Fraud Detection with Artificial Intelligence, 2020 28th Signal Processing and Communications Applications Conference (SIU), Gaziantep, pp.1-4.

European Banking Authority, Risk Assessment of the European Banking System, Published December 2022, https://www.eba.europa.eu/sites/default/documents/files/document_library/Risk%20Analysis%20and%20Data/Risk%20Assessment%20Reports/2022/RAR/1045298/Risk%20Assessment%20Report%20December%202022.pdf.

European Banking Federation, EBF Position Paper on the EC Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), Published September 27, 2021, https://www.ebf.eu/wp-content/uploads/2021/09/EBF_045345-EBF-Position-Paper-on-AI-Regulation-proposal.pdf.

European Central Bank, Opinion of the European Central Bank of 29 December 2021 on a proposal for a regulation laying down harmonised rules on artificial intelligence (CON/2021/40), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021AB0040.

European Commission, High Representative of the Union For Foreign Affairs and Security Policy, Joint Communication to the European Parliament and the Council JOIN (2020) 18 final on EU Cyber Security Strategy for the Digital Decade, Published December 16, 2020, https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0.

European Commission, European Security Union Strategy, Published July 24, 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0605.

European Commission, Communication on Digital Finance Strategy for the EU COM (2020) 591 final, Published September 24, 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC059.

European Commission, Study on the relevance and impact of artificial intelligence for company law and corporate governance, Published June 2021, https://op.europa.eu/en/publication-detail/-/publication/13e6a212-6181-11ec-9c6c-01aa75ed71a1/language-en.

European Commission, A study on the application and impact of Directive (EU) 2015/2366 on Payment Services (PSD2), Published February 02, 2023, https://op.europa.eu/en/publication-detail/-/publication/f6f80336-a3aa-11ed-b508-01aa75ed71a1/language-en.

European Commission, Proposal for a Regulation of the European Parliament and of the Council Laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts COM (2021) 206 final, Published April 21, 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206.

European Commission, Proposal for a Directive of the European Parliament and of the Council on payment services and electronic money services in the Internal Market amending Directive 98/26/EC and repealing Directives 2015/2366/EU and 2009/110/EC, COM (2023) 366 final, Published June 28, 2023, https://eur-lex.europa.eu/resource.html?uri=cellar:e09b163c-1687-11ee-806b-01aa75ed71a1.0001.02/DOC_1&format=PDF.

European Parliament and the Council, Directive (EU) 2015/2366 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, Published November 25, 2015, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366.

European Parliament and the Council, Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Published April 27, 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R067.

European Parliament and the Council, Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), Published December 14, 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555.

European Parliament and the Council, Regulation (UE) 2022/2554 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011, Published December 14, 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R255.

Fares, O.H., Butt, I., Lee, S.H.M. (2022), Utilization of artificial intelligence in the banking sector: a systematic literature review, Journal of Financial Services Marketing, https://link.springer.com/article/10.1057/s41264-022-00176-7, [Accessed September 19th 2023].

Federal Ministry of the Interior, Building and Comunity, Cyber Security Strategy for Germany, Published August 2021, https://www.bmi.bund.de/EN/topics/it-internet-policy/cyber-security-strategy/cyber-security-strategy-node.html.

Financial Stability Institute, FSI Insights on Policy Implementation n. 35 - Humans Keeping AI in Check-Emerging Regulatory Expectations in the Financial Sector, Published August 2021, https://www.bis.org/fsi/publ/insights35.pdf.

Fjeld, J., Achten, N., Hilligoss, H., Nagy, A.C., Srikumar, I. (2020), Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-based Approaches to Principles for AI, The Berkman Klein Center for Internet & Society Research Publication Series, Harvard University.

Floridi, L. (2021), The European Legislation on AI: a Brief Analysis of its Philosophical Approach, Philosophy & Technology, 34, pp. 215-222.

Fritz-Morgenthal, S., Hein, B., Papenbrock, J. (2022), Financial Risk Management and Explainable, Trustworthy, Responsible AI, Frontiers in Artificial Intelligence, 5, https://www.frontiersin.org/articles/10.3389/frai.2022.779799/full, [Accessed September 12th 2023].

Hendrycks, D., Mazeika, M., Woodside, T. (2023), An Overview of Catastrophic AI Risks, https://arxiv.org/abs/2306.12001, [Accessed September 22nd 2023].

HM Government, National Cyber Strategy 2022, Published December 15, 2022, https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022.

Holmes, R., 5 Key Risk Indicators Your Organization Should Monitor, Published September 27, 2022, https://www.bitsight.com/blog/key-risk-indicators, [Accessed September 8th 2023].

Jackson, A., FCA issues warning to financial firms over AI fraud activity, Published July 14, 2023, https://cybermagazine.com/operational-security/fca-issues-warning-to-financial-firms-over-ai-fraud-activity, [Accessed September 5th 2023].

Jackson B.W. (2019), Cybersecurity, Privacy, and Artificial Intelligence: An Examination of Legal Issues Sorrounding the European Union General Data Protection Regulation and Autonomous Network Defense, Minnesota Journal of Law, Science and Technology, 21(1), pp. 169-206.

Jobin, A., Ienca, M., Vayena, E. (2019), Artificial Intelligence: the global landscape of ethics guidelines, https://arxiv.org/abs/1906.11668, [Accessed August 13th 2023].

Josyula, H.P., Vishnubhotla, D., Onyando, P.O. (2023), Is Artificial Intelligence an Efficient Technology for Financial Fraud Risk Management?, International Journal of Managerial Studies and Research, 11 (6), pp. 11-16.

Kaminski, M.E. (2023), Regulating the Risks of AI, Boston University Law Review, 103(5), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4195066, [Accessed August 23th 2023].

Kaur, R., Gabrijelčič, D., Klobučar, T. (2023), Artificial intelligence for cybersecurity: Literature review and future research directions, Information Fusion, 97, https://www.sciencedirect.com/science/article/pii/S1566253523001136, [Accessed August 23th 2023].

Krüger, P.S., Brauchle, J.P. (2021), The European Union, Cybersecurity, and the Financial Sector: A Primer, Carnegie Endowment for International Peace Publications Department, Washington.

Lane, L. (2022), Clarifying Human Rights Standards through Artificial Intelligence Initiatives, International & Comparative Law Quarterly, 71(4), pp. 915-944.

Latonero, M. (2018), Governing artificial intelligence: Upholding human rights & dignity, Data & Society Research Institute, New York.

Leo, M., Sharma, S., Maddulety, K. (2019), Machine Learning in Banking Risk Management: A Literature Review, Risks, 7(1), 29, https://www.mdpi.com/2227-9091/7/1/29, [Accessed August 28th 2023].

Li, J.H. (2018), Cyber security meets artificial intelligence: a survey, Frontiers of Information Technology & Electronic Engineering 19, pp. 1462-1474.

Lindqvist, P., Khailtash, D. (2022), The impact of AI on Banks' Risk Management Approach, KTH Royal Institute of Technology, Stockholm.

Lopes, C., The Future is Now: The Benefits and Limitations of Using AI and Machine Learning for Fraud Detection, Published April 13, 2023, [Accessed August 25th 2023].

Mantelero A. (2019), Artificial Intelligence and Data Protection: Challenges and Possible Remedies, https://rm.coe.int/artificial-intelligence-and-data-protection-challenges-and-possible-re/168091f8a6, [Accessed July 23rd 2023].

Mantelero, A. (2022), Beyond data: human rights, ethical and social impact assessment in AI, Asser Press, Torino.

Mathew, A. (2021), Machine Learning in Cyber-Security Threats, International Conference on IoT based Control Networks and Intelligent Systems (ICICNIS 2020), https://ssrn.com/abstract=3769194, [Accessed September 2nd 2023].

Milojević, N., Redzepagic, S. (2021), Prospects of Artificial Intelligence and Machine Learning Application in Banking Risk Management, Journal of Central Banking Theory and Practice, 3, pp. 41-57.

Mytnyk, B., Tkachyk, O., Shakhovska,N., Fedushko, S., Syerov, Y. (2023), Application of Artificial Intelligence for Fraudulent Banking Operations Recognition, Big Data and Cognitive Computing, 7(2), 93, https://www.mdpi.com/2504-2289/7/2/93, [Accessed August 21th 2023].

Naik, B., Mehta, A., Yagnik, H., Shah, M. (2022), The impacts of artificial intelligence techniques in augmentation of cybersecurity: a comprehensive review, Complex & Intelligent Systems, 8, pp. 1763-1780.

Nemitz, P. (2018), Constitutional democracy and technology in the age of artificial intelligence, Royal Society Philosophical Transactions A, The Royal Society Publishing, https://royalsocietypublishing.org/doi/epdf/10.1098/rsta.2018.008, [Accessed August 21th 2023].

Papakonstantinou, V., de Hert, P. (2022), The Regulation of Digital Technologies in the E.U.: The law-making phenomena of ”act-ification”, ”GDPR mimesis” and ”EU law brutality”, Technology and Regulation Journal, pp. 48-60.

Pavlidis, G. (2021), Europe in the digital age: regulating digital finance without suffocating innovation, Law, Innovation and Technology, Volume 13, pp. 464-477.

Priya, G.J., Saradha, S. (2021), Fraud Detection and Prevention Using Machine Learning Algorithms: A Review, 2021 7th International Conference on Electrical Energy Systems (ICEES), Chennai, pp. 564-568.

Pupillo, L., Fantin, S., Ferreira, A., Polito, C. (2021), Artificial Intelligence and Cybersecurity. Technology, Governance and Policy Challenges, Centre for European Policy Studies (CEPS), Brussels.

Raj, R., Choudhary, S.P. (2022), Analysis of Artificial Intelligence Techniques for Prevention of Financial Fraud, International Journal of Engineering Research & Technology, 11 (2), pp. 171-177.

Raso, F., Hilligoss, H., Krishnamurthy, V., Bavitz,C.,Levin, K. (2018), Artificial Intelligence & Human Rights: Opportunities & Risks, Berkman Klein Center for Internet & Society Research Publication, University of Harvard.

Rutskiy, V., Aljarbough, A., Thommandru, A., Elkin, S., El Amrani, Y., Semina, E., Mishchenko, A., Sorokina, N., Tsarev, R. (2023), Prospects for the Use of Artificial Intelligence to Combat Fraud in Bank Payments, in Silhavy, R., Silhavy, P., Prokopova, Z. (eds) Data Science and Algorithms in Systems. CoMeSySo 2022. Lecture Notes in Networks and Systems, 597, pp. 959-971.

Ryman-Tubb, N.F., Krause, P., Garn, W. (2018), How Artificial Intelligence and machine learning research impacts payment card fraud detection: A survey and industry benchmark, Engineering Applications of Artificial Intelligence, 76, pp. 130-157.

Sahota, N., The Use of AI in Detecting and Preventing Cybercrime, Published March 16, 2023, https://www.neilsahota.com/the-use-of-ai-in-detecting-and-preventing-cybercrime/, [Accessed August 21st 2023].

Samhan, O., Artificial intelligence in the role of assessing cyber risk, Published March 22, 2023, https://www.wtwco.com/en-us/insights/2023/03/artificial-intelligence-in-the-role-of-assessing-cyber-risk, [Accessed September 18th 2023].

Sarker, I.H., Kayes, A.S.M., Badsha, S., Alqahtani, H., Watters, P., Ng, A. (2020), Cybersecurity data science: an overview from machine learning perspective, Journal of Big Data, 7(41), https://link.springer.com/article/10.1186/s40537-020-00318-5, [Accessed August 23th 2023].

Scherer, M.U. (2016), Regulating Artificial Intelligence Systems: Risks, Challenges, Competences, and Strategies, Harvard Journal of Law & Technology, 29(2), pp. 353-400.

Schuett, J. (2023), Defining the scope of AI regulations, Law, Innovation and Technology, 15(1), pp. 60-82.

Shearman, P. (2023), Key risk indicators in cyber security, https://red-goat.com/key-risk-indicators-in-cyber-security/#:~:text=Number%20of%20successful%2Funsuccessful%20login%20attempts%20Network%20traffic%20volume,and%20systems%20Social%20engineering%20attacks%20and%20phishing%20attempts, [Accessed August 27th 2023].

Smuha, N.A., Ahmed-Rengers, E., Harkens, A., Li, W., MacLaren, J., Piselli, R., Yeung, K. (2021), How the EU can achieve legally trustworthy AI: a response to the European Commission's proposal for an Artificial Intelligence Act, SSRN: https://ssrn.com/abstract=389991, [Accessed September 7th 2023].

Soni, V.D. (2019), Role of artificial intelligence in combating cyber threats in banking, International Engineering Journal for Research & Development 4 (1), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3654422, [Accessed September 10th 2023].

Taddeo, M. (2021), On The Risks of Trusting Artificial Intelligence: The Case of Cybersecurity, in Cowls, J., Morley, J. (eds) The 2020 Yearbook of the Digital Ethics Lab, pp. 97-108.

Tao, F., Akhtar, M.S., Jiayuan, Z. (2021), The future of Artificial Intelligence in Cybersecurity: A Comprehensive Survey, EAI Endorsed Transactions on Creative Technologies, 8(28), pp. 1-15.

The National Institute of Standards and Technology, Cybersecurity Framework, The Five Functions, Published April 12, 2018, https://www.nist.gov/cyberframework/online-learning/five-functions, [Accessed August 26th 2023].

The Organization for Economic Cooperation and Development, Artificial Intelligence, Machine Learning and Big Data in Finance: Opportunities, Challenges, and Implications for Policy Makers, Published August 11, 2021, https://www.oecd.org/finance/financial-markets/Artificial-intelligence-machine-learning-big-data-in-finance.pdf.

United Kingdom Government, Equality Act 2010, https://www.legislation.gov.uk/ukpga/2010/15 [Accessed August 29th 2023].

Wachter, S., Mittelstadt, B., Floridi, L. (2017), Why a Right to Explanation of Automated Decision-Making Does Not Exist in General Data Protection Regulation, International Data Privacy Law, 7(2), pp. 76-99.

Weigand, S., AI abuse grows beyond phishing to multistage cyberattacks, Published September 7, 2023, https://www.scmagazine.com/news/multistage-payload-attacks-it-team-impersonations-up-as-ai-adopted-at-large, [Accessed September 16th 2023].

Wiafe, I., Koranteng, F.N., Obeng, E.N., Assyne, N., Wiafe, A., Gulliver, S.R. (2020), IEEE Access, 8, pp. 146598-146612.

Wirkuttis, N., Klein, H. (2017), Artificial Intelligence in Cybersecurity, Cyber, Intelligence, and Security, 1(1), pp.103-119.

World Bank Group, Financial Sector's Cybersecurity: A Regulatory Digest, Published May 2019, http://pubdocs.worldbank.org/en/208271558450284768/CybersecDigest-3rd-Edition-May2019.pdf.

World Economic Forum, The Global Risks Report 2022, https://www.weforum.org/reports/global-risks-report-2022, [Accessed August 16th 2023].

Yeung, K., Howes, A., Pogrebna, C. (2019), AI Governance by Human Rights-Centred Design, Deliberation and Oversight: An End to Ethics Washing, in Dubber, M.D. (ed) The Oxford Handbook of Ethics of AI, Oxford University Press, pp. 76-106.

Zeng Y. (2022), AI Empowers Security Threats and Strategies for Cyberattacks, Procedia Computer Science 208, pp. 170-175.

Zhang, Z., Ning, H., Shi, F., Farha, F., Xu, Y., Xu, J., Zhang, F., Choo, K.K.R. (2022), Artificial intelligence in cyber security: reasearch advances, challenges, and opportunities, Artificial Intelligence Review 55, pp. 1029-1053.