ARTIFICIAL INTELLIGENCE AND CYBER RESILIENCE IN THE BANKING SECTOR. A NEW ERA IN RISK MANAGEMENT AND FINANCIAL PROTECTION

Corina-Ionela DUMITRESCU[1], Adelina – Elena BĂDESCU[1], Iuliana GRECU[1], Nicoleta NICULESCU[1]

[1] National University of Science and Technology POLITEHNICA Bucharest, Bucharest University Centre

Artificial Intelligence (AI) has become a crucial component in enhancing cyber resilience within the European banking sector. The rapid digital transformation has brought about significant cyber risks, necessitating advanced solutions for data protection, business continuity, and maintaining customer trust. AI plays a vital role in real-time anomaly detection, risk anticipation, and automated incident response, thereby optimizing threat defence and financial risk management through predictive analytics. Despite its benefits, AI's integration poses challenges related to data protection and ethical decision-making, requiring strict compliance with European and international legislation such as GDPR, NIS2 Directive, Basel III regulations, and the AI Regulation.

This study offers a descriptive analysis and examines AI's impact on cyber resilience, highlighting its technological advantages and legal implications in the banking sector. Innovative models for AI implementation are explored to develop effective security and financial risk management mechanisms, emphasizing the need for proactive threat detection, operational efficiency, and adaptability to evolving cyber threats.

Key words*:* Key words; Key words; Key words; Key words; Key words.

JEL Classification Codes: G32, K24, O33

1. INTRODUCTION

Artificial Intelligence (AI), alongside cyber resilience, has ascended as a cornerstone of the contemporary banking infrastructure, reflecting its profound importance in addressing the multifaceted challenges characterising the digital era. The inexorable acceleration in the frequency, sophistication, and scope of cyber threats has positioned financial institutions at a precarious juncture, where operational continuity, data integrity, and customer trust are continually jeopardised. In this complex environment, the strategic adoption of AI-driven systems emerges not merely as a defensive mechanism but as an imperative for maintaining systemic stability and competitive robustness. The unparalleled capabilities of AI in processing voluminous datasets with experience, discerning latent risks through predictive modelling, and orchestrating automated, dynamic response mechanisms underscore its transformative role. These technological advancements empower banking entities to establish secure defences and adapt to the ever-evolving cyber threat landscape. This discourse seeks to elucidate the pivotal role of AI in cultivating an agile, secure, and reliable banking ecosystem while systematically investigating innovative paradigms to integrate AI into cybersecurity protocols and risk management frameworks, thereby ensuring resilience and operational excellence in the financial domain.

The principal motivation underlying this study arises from the accelerating digital transformation within the European banking sector and the simultaneous intensification of sophisticated cyber threats. As financial institutions increasingly depend on digital infrastructures to enhance operational efficiency and improve customer experience, they simultaneously expose themselves to vulnerabilities that threaten business continuity, compromise sensitive data, and undermine public confidence. This research is to address the pressing need to incorporate Artificial Intelligence (AI) as an essential tool for strengthening cyber resilience. By capitalising on AI's advanced capabilities in real-time anomaly detection, predictive analytics, and automated incident response, the study aims to reinforce financial institutions' defences against these dynamic threats. Moreover, the investigation is driven by the dual imperative of leveraging AI's technological potential while adhering to stringent regulatory frameworks such as GDPR, Basel III, and the AI Act, which safeguard ethical practices and data protection. This motivation underscores the critical necessity for innovative models designed not only to secure digital infrastructures but also to align with established legal and ethical standards.

The particularity of this study lies in its holistic exploration of the convergence of technology, cybersecurity, and regulatory compliance within the banking sector. While existing research frequently concentrates on the operational applications of AI technologies, this study explores further into their implications for enhancing proactive threat detection, operational efficiency, and adaptability to emerging cyber risks. Additionally, the research emphasises the development of scalable mechanisms that can be implemented by diverse financial institutions, ranging from commercial banks to investment entities, regardless of their size or regional focus. By incorporating descriptive analyses alongside innovative paradigms for AI-driven security, the study ensures its pertinence not only to European markets but also to a broader international audience facing analogous challenges in digital transformation. Through its multifaceted approach, the study distinguishes itself as an essential contribution to both academic and industry discourse, laying the groundwork for the creation of a resilient, secure, and efficient financial ecosystem.

2. ARTIFICIAL INTELLIGENCE AND CYBER RESILIENCE

During 2020, the activity of the Romanian banking sector was marked by vulnerabilities (Brînză, Dumitru, 2021). Embracing digitalization is no longer a choice. It's a necessity. A new digital era that is accessible to all holds the potential to shape a more inclusive, resilient, and sustainable world for generations to come. Global digital transformation is moving at lightning speed. Today, digitalization is beyond a mere trend; it has become a core component in the operational blueprint for many organisations. It empowers businesses to streamline operations, enhance customer experiences, and open new possibilities (Oancea, 2023).

The accelerated evolution of digital technologies has led to a significant expansion of data and media, reshaping economic activities as well as cybersecurity strategies. With this transition, both major opportunities and critical vulnerabilities that can be exploited by malicious actors have been highlighted. The increase in the sophistication of cyberattacks has demonstrated the need for advanced protection methods, and artificial intelligence (AI) has established itself as a fundamental solution in this area. The use of AI in the identification and prevention of threats allows for the rapid analysis of massive volumes of data and the immediate reaction to potential risk, thus contributing to increasing the cyber resilience of digital infrastructures (Aslam, 2024).

The exponential increase in the number of cyberattacks has led to the need to adopt more flexible, fast and effective solutions for the protection of digital systems. The introduction of AI in the field of cybersecurity has brought about a significant change in the way threats are detected and responded to. Unlike traditional methods, AI-based security systems can anticipate

and neutralize attacks autonomously, using advanced machine learning and predictive analytics techniques (Kumar et al., 2023).

Globalization of the economic and financial relations and their complexity have led to the multiplication of risks banking activities are subjected to, the instability and challenges are much more frequent now, when the banking system has interdependence connections and joint regulations (Rădulescu, 2018). The financial sector in our country consists of commercial banks, participation banks, development banks and investment banks (Esre, Kapusuzoglu, Ceylan, 2022). Banks should adopt proactive strategies to identify, assess and mitigate risks (including financial, operational, reputational and regulatory risks). These strategies include the use of advanced risk models and the creation of a dedicated risk management department (Hagiu, Bărbulescu, 2023).

In this context, AI algorithms enable proactive threat detection by analysing behavioural patterns and identifying anomalies in traffic. Security Information and Event Management (SIEM) systems, integrated with User and Entity Behaviour Analytics (UEBA) technologies, analyse suspicious activity and correlate it with historical data to prevent complex cyberattacks. These are essential solutions for establishing an effective security incident response and minimising the time required to investigate.

Romania, as a developing economy in Eastern Europe, is increasingly embracing artificial intelligence as a pivotal tool for digital transformation, particularly within its banking sector. The strategic integration of AI technologies is not merely limited to improving operational efficiency but extends to fortifying cybersecurity resilience against the continually escalating sophistication of cyber threats. Banking institutions in Romania are progressively deploying machine learning algorithms to analyse behavioural patterns and detect anomalies, thus enabling proactive identification and mitigation of potential risks. AI-driven solutions, such as intelligent chatbots that enhance customer interaction and automated tools for assessing credit risks, have become indispensable components of the banking landscape. Furthermore, the adoption of stringent European legislative frameworks, including GDPR and other normative acts, underscores Romania's commitment to ensuring data protection, regulatory compliance, and transparency in decision-making. Beyond the financial domain, Romania has witnessed promising advancements in the application of AI across various sectors, such as healthcare, where AI systems are transforming diagnostic precision, and education, where personalised learning platforms are gaining traction. However, apart from these advancements, Romania is facing critical challenges, including a limited number of skilled professionals and modest/insufficient investment in AI-driven startups, which stymie its ability to compete with global AI frontrunners.

On the contrary, leading economies, such as the United States and Germany, are setting benchmarks in AI adoption by leveraging substantial investments in research, development, and infrastructure to transform their digital ecosystems. The financial sector in the United States exemplifies the cutting-edge application of AI technologies, with real-time fraud detection systems, predictive analytics, and robotic process automation (RPA) redefining operational frameworks while simultaneously enhancing user experience. Germany, with its emphasis on ethical AI deployment, is aligning its technological advancements with sustainable development goals, incorporating AI into green finance initiatives that resonate with the European Union's broader agenda for environmental sustainability. Meanwhile, Asian power centres, notably China and South Korea, use AI on an unequalled scale, integrating it into national security measures, urban planning, and infrastructural development. China has pioneered the use of AI in facial recognition technologies for customer verification and algorithmically driven investment strategies within its financial sector, while South Korea has emerged as a global leader in fintech innovations and AI-driven digital banking solutions. The disparity in AI adoption between

Romania and these global leaders highlights the significant influence of economic resources, infrastructural capacity, and policy frameworks in dictating the pace and the depth of digital transformation initiatives. Nonetheless, Romania's focused approach towards cybersecurity and compliance offers a valuable pattern for smaller economies aspiring to navigate the complexities of AI integration while safeguarding ethical and lawful practices. (Malatji, M. and Tolah, A., 2024)

2.1. Definition and Role of Artificial Intelligence

Artificial intelligence (AI) is a field of computer science focused on developing systems capable of performing human-like cognitive tasks, such as pattern recognition, natural language processing, and autonomous decision-making. In the banking sector, AI has become essential for digital transformation, significantly impacting the automation of operational processes, the optimization of financial services, and cybersecurity measures (Russell and Norvig, 2020). AI applications include detecting financial fraud through real-time transaction analysis, managing credit risks by assessing customer reliability and personalizing the customer experience through intelligent chatbots. From a legal point of view, the use of AI is regulated by normative acts such as GDPR, AMLD5, NIS Directive 2, AI Act and DORA Regulation, which impose strict requirements on data protection, cybersecurity and decision-making transparency.

AI brings major advantages in cybersecurity, helping to increase operational efficiency and scalability of protection. Machine learning algorithms can process massive amounts of data much faster than would be possible manually, ensuring a constant level of surveillance and reducing the time and costs associated with detecting threats. By training on vast sets of historical attack data, AI achieves a high degree of accuracy in differentiating legitimate from malicious traffic and enables automated response to incidents, such as the immediate isolation of a compromised host, minimizing remediation time. AI's ability to continuously evolve makes it a valuable tool in the dynamic cyber environment, adapting to new attack patterns and facilitating a high level of proactivity for the security of organizations.

From a legal point of view, the use of AI in banking risk management and automated processes is subject to strict regulations on data protection, cybersecurity and decision-making transparency. Among the most relevant normative acts applicable in the European Union are, table 1.

Table 1. Normative acts applicable in the European Union

Regulation	Obligations	The role of AI
GDPR (EU Regulation 2016/679)	Processing and securing of personal data, transparency, explanations, right to human intervention	Compliance with the principles of transparency and explanations
Directive (EU) 2015/849 (AMLD5)	Prevention of money laundering and terrorist financing, monitoring of suspicious transactions	Real-time analysis of financial flows, detection of money laundering schemes
NIS 2 Directive (EU 2022/2555)	Security of networks and information systems, protection of critical IT infrastructures	Cyber threat detection, continuous monitoring of computer networks
Artificial Intelligence Act (AI Act)	Classification of AI systems according to risk level, algorithmic transparency	Risk assessment, credit approval, fraud detection
DORA Regulation (EU 2022/2555)	Digital operational resilience, robust cybersecurity measures	Automated detection and response to cyber threats, operational risk management

Source: Authors' contribution

2.2. Advantages of Using AI in Cybersecurity

A major advantage of using AI in cybersecurity is the increased efficiency and scalability of protection. AI algorithms can automate time-consuming tasks such as triaging alerts and analyzing logs, allowing analysts to focus on strategic activities. AI processes massive amounts of data quickly, providing continuous surveillance and optimizing the organization's resources (Csernatori & Mavrona, 2022).

AI accelerates the detection and response to cyber threats by analyzing network traffic and user behaviour in real-time to flag anomalies or indicators of attack (Leitner & Singh, Kraaij, & Zsámboki, 2024). Deep learning algorithms detect and neutralize threats with high accuracy, reducing the number of false alarms and response time. AI incident response automation minimizes remediation time by quickly isolating compromised hosts.

AI systems are continuously adapting to new attack patterns, learning from the new data they receive. Machine learning algorithms update internal models based on new information, ensuring that the defiance system remains relevant in the face of changing threats. AI handles data on a scale, extracting knowledge from millions of security events to constantly refine the detection model. Continuous learning provides proactivity and resilience in cybersecurity, preventing future incidents more effectively.

2.3. Cyber Resilience: A Strategic Priority

Cyber resilience is the ability of financial institutions to anticipate, prevent, detect, respond and recover quickly from a cyberattack, ensuring the continuity of operations and protecting critical infrastructures (Csernatori and Mavrona, 2022). In an ever-evolving digital landscape, cyberattacks are becoming increasingly sophisticated, and the banking sector must adopt proactive security strategies to maintain customer trust and comply with international data protection and cybersecurity regulations (Leitner & Singh, Kraaij, & Zsámboki, 2024).

The reason why banks have an active role in risk management is due to their role in the economic system (Yilmaz, Ceylan, Kapusuzoglu, 2021). Financial institutions must implement advanced real-time monitoring mechanisms to detect any suspicious activity or anomaly in the IT infrastructure. Artificial intelligence-based technologies allow the analysis of network traffic and the identification of unusual behaviour, thus preventing unauthorized access (Csernatori and Mavrona, 2022). Machine learning algorithms can detect and neutralize cyber threats with superior accuracy and speed, thereby reducing potential damage before it occurs. GDPR requires financial institutions to adopt proactive security measures, including advanced cyberattack detection systems, to protect customer data (Brennan, 2024).

Automating incident response is essential, reducing the time it takes to identify and isolate threats. Financial institutions need to implement Security Orchestration, Automation, and Response (SOAR) platforms that enable automatic detection and isolation of compromised systems to prevent the spread of the attack, implement automated playbooks for incident management, and integrate with security operations centres for effective incident response coordination (Leitner and Singh, Kraaij and Zsámboki, 2024).

Banking institutions must implement advanced data backup and recovery solutions, using redundancy and cloud computing technologies to maintain operational continuity. The NIS 2 Directive, DORA and the AI Act require business continuity measures on financial institutions, including regular testing of disaster recovery plans to ensure the optimal functioning of IT systems and minimise losses caused by cyberattacks (Csernatori and Mavrona, 2022).

Cyber resilience is a strategic priority for banking institutions, having a direct impact on financial security and customer trust. By adopting advanced technologies based on artificial intelligence, automation and continuous monitoring, banks can detect and neutralize threats in

real-time, reducing the impact of cyberattacks. Compliance with European regulations, such as GDPR, NIS 2 Directive, DORA, AI Act, and Basel III, is essential to ensure a safe and stable financial environment (Leitner & Singh, Kraaij, & Zsámboki, 2024).

The use of artificial intelligence in the banking sector raises numerous legal challenges, having a significant impact on data protection, cybersecurity and the compliance of financial institutions with international regulations. While AI brings considerable benefits by automating processes, reducing operational risks and increasing the efficiency of financial systems, the use of these technologies must comply with strict rules on algorithmic transparency, privacy protection and financial information security.

European and international regulations impose a well-defined legal framework for the use of AI in banking, ensuring both consumer protection and the stability of financial systems. These rules are essential to prevent the misuse of artificial intelligence in automated lending decisions, financial risk assessment and fraud detection. Banks must implement AI solutions in a way that complies with the principles of transparency, accountability and fairness of decision-making algorithms.

The General Data Protection Regulation (GDPR) encompasses one of the strictest regulations applicable to the use of artificial intelligence in the banking sector, setting clear requirements for the processing of personal data and the protection of users' rights. It imposes an obligation on financial institutions to ensure the transparency of the algorithms used in customer behavioral analysis, financial risk assessment and automated decision-making. The GDPR guarantees the right of data subjects to request explanations of decisions made exclusively based on machine learning algorithms, as well as the possibility to challenge these decisions. The regulation provides for strict measures to prevent algorithmic errors and discrimination (Brennan, 2024).

To comply with the requirements imposed by the GDPR, banking institutions must implement rigorous technical and organizational measures to protect user data and prevent its misuse. These measures include the use of advanced encryption systems, anonymization and pseudonymization of personal data, as well as the development of periodic audit mechanisms of artificial intelligence algorithms to ensure compliance with the regulations in force. Banks must also carry out data protection impact assessments (DPIAs) before the deployment of AI systems to analyse the risks of automated processing and adopt measures to mitigate them.

In the event of a successful cyberattack or incident caused by an error in the AI system, the legal responsibility lies mainly with the banking institution using that system. AI does not have a legal personality, so the bank (as a data controller and owner of the infrastructure) bears responsibility for technological failures. The Court of Justice of the European Union (CJEU) recently issued an important ruling on what constitutes "automated individual decision-making" under Article 22 of the GDPR. The CJEU ruled in the SCHUFA case (Case C-634/21) that the data controller must implement appropriate security measures and is directly liable if a breach leads to the compromise of personal data (Brennan, 2024). This case shows the broad interpretation of liability: providers of automated services essential to third-party decisions may also be liable under the GDPR.

The Basel III regulations, drafted by the Basel Committee on Banking Supervision, impose strict standards on financial risk management and the stability of the international banking system. In the context of the use of artificial intelligence, these regulations include requirements on transparency and interpretation of risk analysis algorithms, so that the predictive models used in assessing customer creditworthiness and managing credit portfolios comply with financial prudential principles. According to Basel III, banks must ensure that AI systems integrated into risk management processes undergo rigorous and validated tests to avoid negative effects on financial stability. In addition, the use of AI in financial stress analysis and systemic

risk modelling must be carried out in compliance with prudential supervisory requirements imposed by national and international banking authorities.

3. LEGAL IMPLICATIONS OF THE USE OF AI IN THE BANKING SECTOR

The integration of artificial intelligence in the banking sector is essential, helping to automate processes, reduce operational risks and increase the efficiency of financial systems. However, the use of AI raises important legal challenges related to data protection, cybersecurity and compliance with international regulations.

European and international regulations impose a rigorous legal framework for the use of AI in banking, ensuring both consumer protection and the stability of financial systems. Banks must implement AI solutions that comply with the principles of transparency, accountability and fairness of decision-making algorithms. These rules are essential to prevent the misuse of AI in automated lending decisions, financial risk assessment and fraud detection.

The General Data Protection Regulation (GDPR) and the NIS 2 Directive set strict requirements on data security and protection, obliging banks to adopt rigorous technical and organizational measures. These measures involve advanced encryption systems, anonymisation and pseudonymisation of data, and regular auditing mechanisms for AI algorithms. The GDPR guarantees the right of data subjects to request explanations and challenge automated decisions, preventing algorithmic errors and discrimination.

The legal responsibility in the event of a cyberattack or AI error lies with the banking institution using the system. The Court of Justice of the European Union has clarified that the data controller is responsible for the data compromise and must implement appropriate security measures. Basel III regulations impose strict standards on the transparency and interpretation of risk analysis algorithms, ensuring financial prudence.

AI is profoundly altering the financial domain within the banking sector, redefining methodologies in credit evaluation, portfolio management, and customer interaction. Through the deployment of predictive algorithms underpinned by advanced machine learning capabilities, banks are now able to conduct solvency analyses with incomparable precision, thereby mitigating risks associated with loan defaults and enabling the formulation of tailored credit solutions that align with the unique financial profiles of each customer. Moreover, AI-driven predictive models are revolutionising portfolio management by integrating vast datasets to uncover nuanced market trends, correlations, and forecasts, thus equipping financial institutions with actionable intelligence to optimise investment strategies.

The beginning of AI has democratized access to sophisticated financial tools previously exclusive to high-net-worth individuals. AI-powered virtual assistants now offer personalized financial management support, ranging from dynamic budgeting advice to strategic investment planning and retirement portfolio optimisation. Fraud detection mechanisms, once based on traditional frameworks, have been significantly enhanced through AI-based anomaly detection systems capable of identifying complex irregularities in transaction patterns, safeguarding both institutions and clients.

In the field of financial risk management, regulations such as Basel III underscore the critical importance of rigorously testing and validating AI-based models used in credit risk evaluation and systemic risk predictions. These requirements aim to ensure that AI systems not only comply with prudential supervisory standards but also contribute to the overall stability of the global banking system. Furthermore, AI's application in financial stress testing and systemic risk modelling is aligned with the predominant objective of proactively identifying vulnerabilities that could impact financial institutions, fostering resilience in the face of market disruptions.

Nonetheless, the integration of AI within the financial domain needs cautious oversight to address potential challenges associated with automated decision-making. Financial institutions are tasked with ensuring ethical practices, preventing biases embedded within algorithmic models, and adhering to stringent regulatory frameworks that demand transparency, accountability, and fairness. As artificial intelligence continues to reshape the banking landscape, its transformative potential in financial management must be balanced against the imperatives of compliance and responsible innovation, defining a new era for the financial services sector.

3.1. AI Challenges in the Context of European Regulations

The General Data Protection Regulation (GDPR) is one of the strictest sets of regulations applicable to the use of artificial intelligence in the banking sector, setting clear requirements for the processing of personal data and the protection of users' rights. Financial institutions are required to ensure the transparency of the algorithms used in customer behavioural analysis, financial risk assessment, and automated decision-making. The GDPR guarantees the right of data subjects to request explanations of decisions made solely based on machine learning algorithms and to challenge these decisions. The regulation imposes strict measures to prevent algorithmic errors and discrimination.

For GDPR compliance, banking institutions must implement rigorous technical and organizational measures to protect user data and prevent its misuse. Among the measures are the use of advanced encryption systems, anonymization and pseudonymization of personal data, as well as the development of periodic mechanisms for auditing artificial intelligence algorithms. Data Protection Impact Assessments (DPIAs) must be carried out before the deployment of AI systems to analyse the risks of automated processing and adopt measures to mitigate them.

The Court of Justice of the European Union ("CJEU") recently ruled in the SCHUFA case (Case C-634/21) that the data controller is responsible for the compromise of personal data and must implement appropriate security measures. This decision expands the interpretation of liability to include providers of automated services essential to a third party's decisions under the GDPR. The general tendency is not to leave "grey areas" – whether a cyber incident is caused by an external attacker or a flaw in the defence algorithm, the bank and its management can be held liable if they have not taken reasonable precautions.

The Basel III regulations, drafted by the Basel Committee on Banking Supervision, impose strict standards on financial risk management and the stability of the international banking system. In the context of the use of artificial intelligence, these regulations include requirements on transparency and interpretation of risk analysis algorithms, so that the predictive models used in assessing customer creditworthiness and managing credit portfolios comply with financial prudential principles. According to Basel III, banks must rigorously test and validate AI systems to avoid negative effects on financial stability. The use of AI in financial stress analysis and systemic risk modelling must comply with prudential supervisory requirements imposed by national and international banking authorities.

A major challenge in the use of AI is establishing liability in the event of a cyberattack or AI error. Traditional cybersecurity systems are managed and supervised directly by human operators, making liability clearly defined in the event of an incident. AI, operates with a high degree of autonomy, making decisions based on machine learning algorithms without direct human intervention. This autonomy raises the question of establishing liability in the event of an attack that is not detected or prevented by AI. The GDPR and the NIS 2 Directive set out general data protection and cybersecurity obligations, but do not explicitly clarify who is liable for cyber incidents caused by errors in AI systems, leaving room for complex litigation.

3.2. Compliance and Audit: Technical and Organisational Measures in the Implementation of AI

Internal governance of AI systems. Banking institutions must implement a robust governance framework for regulatory compliance when integrating AI into cybersecurity operations. A key first step is the clear designation of internal responsibilities: for example, the creation of an AI Governance Board or the extension of the mandate of the Operational Risk Board to also oversee AI-related risks. This should include experts in IT, security, legal compliance and data protection, who regularly assess the performance and risks of the AI systems used (including ethical and fair aspects). It is also recommended to appoint a Data Ethics/AI Officer or assign these responsibilities to the existing Compliance Officer, to oversee the implementation of the AI Act and GDPR requirements concerning AI. Many large banks globally have already created internal principles for the responsible use of AI and procedures for approving new algorithmic models before production, which is also becoming good practice in the EU.

In line with the requirements of NIS2 and DORA, banks must implement a minimum set of technical measures to protect networks and data regardless of whether AI can be used, table 2. AI integration does not replace these basic measures but complements them. Key measures include:

Table 2. Technical cybersecurity measures

Aspect	Details
Data encryption	Transforming data into a format that is not readable by unauthorized persons. This involves the use of advanced encryption algorithms to ensure data privacy and integrity, even if other security mechanisms fail.
Symmetric encryption	Using the AES (Advanced Encryption Standard) algorithm to encrypt the data stored on the bank's servers. AES is recognized for its high security and is widely used in industry to protect sensitive data.
Asymmetric encryption	Implement RSA encryption to protect client-server communications. RSA uses a key pair (public and private) to ensure the confidentiality and integrity of the data transmitted, being an effective method of asymmetric encryption.
Legislation	DORA and NIS2 require sensitive data to be protected through encryption. These regulations emphasize the importance of using AES encryption for stored data and TLS encryption for data in transit, thus ensuring the protection of information against unauthorized access.
Access control	Multi-factor authentication (MFA) for critical systems, ensuring that only authorized personnel can access or intervene with AI-powered security tools. Both the NIS2 and DORA legislative frameworks emphasize the importance of strict access control and multi-factor authentication.
Network monitoring	Use of AI/ML Intrusion Detection/Prevention solutions for continuous network monitoring and anomaly detection. These solutions help identify suspicious activity and prevent intrusions, contributing to the overall security of the network.
Monitoring tools	Using tools like Snort or Meerkata to monitor network traffic and detect suspicious activity. These tools allow the correct configuration and tuning of monitoring systems to define thresholds and have rapid alarm reaction procedures.
Vulnerability management	Including AI systems in the patch management cycle, promptly applying security updates to the AI platforms and ML libraries used and performing regular vulnerability scans to identify and fix system weaknesses.

Scanning Tools	Using tools such as Nessus or OpenVAS to perform regular scans of the network and identify vulnerabilities. These tools are essential for managing vulnerabilities and applying security updates promptly.
Network segmentation	Rigorous testing of security solutions in isolated environments before they are deployed on live systems to avoid unintended disruption. Network segmentation and rigorous testing are necessary to prevent unintentional disruptions and ensure the proper functioning of security systems.

Source: Authors' contribution

Beyond technology, compliance also requires the right internal procedures and policies, table 3.

Table 3. Organisational and procedural measures

Policies	Description
Privacy by design and security by design	The system collects only the necessary data, stores it in secure form and deletes it according to the calendar, in order to comply with the GDPR principles.
Periodic algorithmic audit	Periodic independent audits to verify accuracy, robustness to attacks, and fairness of models. The traceability of decisions is a key aspect audited.
Training and awareness	The bank's staff must be trained in the specifics of AI. NIS2 mentions "cyber hygiene practices and security training."

Source: Authors' contribution

In the context of AI, this means training on how models work, what risks they have (including bias, and errors), how to interpret the results generated by AI, and how to intervene when needed. An organizational culture that understands AI will reduce the risk of operational errors (e.g., employees do not blindly decide AI is infallible) and facilitate compliance (employees more easily recognize when an AI output seems inappropriate or possibly discriminatory and will report).

AI failure response plan: In addition to the classic cyber incident response plan, banks should have procedures in place for a critical AI system becoming unavailable or giving major errors. For example, if an AI monitoring transactions starts generating false alarms en masse, there must be a *fallback* procedure (temporarily switching to a manual system or fixed rules) until the issues are fixed. These plans ensure continuity and avoid decision-making chaos caused by a possible *algorithm glitch*.

Regulatory oversight and trends: The financial sector is anyway heavily regulated and supervised, and the introduction of AI attracts the attention of the relevant authorities: the European Central Bank (through the supervisory mechanisms), the European Supervisory Authorities (EBA, ESMA, EIOPA) and national authorities (NBR, ASF in Romania) are adjusting the guidelines to cover the use of AI. For example, the EBA stressed that machine learning models used by banks in capital calculation (IRB models) need to comply with the same validation requirements as traditional models, highlighting the need for explainability and control of these models within the regulatory framework.

More broadly, financial authorities coordinate with data protection authorities to jointly address AI oversight. A recent trend is the creation of innovation hubs or regulated *sandboxes* where banks can test AI solutions under the supervision of the authorities, receiving feedback on compliance risks. Specific auditing standards are also being discussed – for example, ISO

standards or European standards for AI risk management in finance could emerge, based on which banks can be certified. Consumers also play a role, directly or indirectly: public pressure for the ethical use of AI has led to tougher legislative initiatives (such as the AI Act being geared towards *consumer protection*) and bank advertising by highlighting *"fair AI"* or *"AI Ethics"* as an element of trust.

4. THE ROLE OF ARTIFICIAL INTELLIGENCE IN THE BANKING SECTOR FROM THE PERSPECTIVE OF RESILIENCE AND BANK RISK MANAGEMENT

Artificial intelligence is an emerging technology with a significant impact on cyber resilience and risk management in the banking sector. Its ability to analyze big data in real time, detect anomalies, and proactively prevent cyberattacks makes it an essential tool for protecting financial infrastructure and reducing operational vulnerabilities. By using sophisticated machine learning and predictive analytics algorithms, AI enables banks to optimize cyberattack prevention strategies and build capacity for emerging threats. In an increasingly technology-dependent economic environment, the use of AI in banking is becoming a key component of security strategies and compliance with international regulations.

One of the most important applications of AI in the banking sector is **anomaly detection**, which is based on the behavioural analysis of users and financial flows to identify suspicious activity in real-time. Machine learning algorithms can recognize normal trading patterns and flag any deviations from these patterns, which helps prevent financial fraud and cyberattacks. For example, if a regular customer makes transactions within a certain time frame and from a certain geographical location, and the system detects an unusual transaction from another region or at an atypical time, it can activate an automatic alert mechanism and block the temporary operation until the user's identity is confirmed. This type of active monitoring helps banks prevent fraud attempts, such as phishing attacks or unauthorized use of bank cards.

In addition to detecting anomalies, AI plays a key role in **risk assessment**, giving banks the ability to analyze and anticipate the possibilities of financial threats. Financial institutions' predictive AI system models identify high-risk authorities before they become problematic for the credit portfolio. For example, by analyzing financial history, payment behaviour, and economic trends, AI can establish an accurate risk score for each customer, which helps adjust lending strategies and prevent losses caused by loan defaults. This foresight is essential for the stability of the banking system and for ensuring compliance with Basel III regulations, which impose strict standards on credit risk management.

Another area where AI is demonstrating significant impact is **the automation of the security process**, which reduces response time to cyber incidents and improves banks' operational efficiency. AI systems can quickly identify and isolate cyberattacks by automatically activating protection mechanisms such as restricting access to certain systems or deploying multi-factor authentication solutions. These technologies are integrated into banks' IT infrastructure through the **Security Orchestration, Automation, and Response (SOAR)** platform, which allows efficient incident management and reduces the impact of attacks on financial operations. In addition, the deployment of AI systems in the field of cybersecurity is in line with the **NIS 2 Directive**, which requires banking institutions to protect against cyberattacks and make them report security incidents quickly.

As artificial intelligence becomes an indispensable component of banking systems, there is also a need for strict regulation to ensure the ethical and safe use of this technology. **The Artificial Intelligence Act (AI Act)** proposes a clear legal framework for the use of AI in the financial sector, classifying AI systems according to the level of risk and imposing strict

transparency and audit requirements. Banking institutions must comply with these regulations to prevent the misuse of algorithms and protect consumers' rights.

The integration of artificial intelligence into the financial risk management process is firmly rooted in theoretical principles emphasising the importance of real-time data analysis, proactive risk identification, and adherence to stringent regulatory frameworks. AI enhances traditional risk management pillars—risk identification, assessment, and mitigation—by leveraging advanced machine learning capabilities and predictive analytics. These systems allow financial institutions to detect anomalies, assess risks with unparalleled precision, and implement dynamic mitigation strategies. By continuously analyzing transactional data and user behavior, AI enables institutions to identify potential fraud or systemic vulnerabilities promptly, preventing escalations that could compromise financial stability. Furthermore, the deployment of automated processes, such as those integrated into Security Orchestration, Automation, and Response (SOAR) platforms, improves operational efficiency and aligns with directives like NIS 2, ensuring rapid response and compliance with international regulations.

From a regulatory perspective, robust governance mechanisms are essential to ensure the ethical deployment of artificial intelligence within the financial sector. Regulatory frameworks, such as the Artificial Intelligence Act, establish clear guidelines by categorising AI systems based on risk and imposing stringent transparency and audit requirements. These measures are completed by innovation hubs and regulatory oversight, which balance technological advancement with systemic risk mitigation by enabling controlled experimentation with AI solutions under regulatory supervision. Theoretical literature underscores the necessity of transparency, explainability, and ethical accountability in AI applications, ensuring consumer protection and fostering trust (Toma and Drazenovic, 2024). Synthesising these insights, it is obvious that the integration of AI into financial risk management transforms traditional practices, reinforcing resilience, advancing operational efficiency, and safeguarding the broader goals of financial stability and ethical responsibility.

4.1. Examples of AI Implementation in Risk Management

Within the European Union, regulatory regulations and financial institutions are actively collaborating to integrate AI-based solutions into banking risk management. Their advanced use, such as machine learning and predictive analytics, enables technology banks to improve supervisory mechanisms, anticipate system threats, and ensure compliance with international regulations. In this context, several initiatives have been developed at the European level to make AI an essential tool for supervising and optimising financial processes.

- **The European Central Bank (ECB) and the Prudential Supervisory System**

The European Central Bank (ECB) uses artificial intelligence (AI) to supervise and manage risks in the banking sector. The ECB uses machine learning algorithms and big data to monitor financial institutions in real-time, identifying problems and providing recommendations for correcting them.

An important area of application of AI in the ECB is the detection of suspicious financial transactions and the fight against money laundering. AI analyses financial flows to identify activities at risk of money laundering or terrorist financing, under the Directive (EU) 2015/849.

AI is also used to model credit risks and prevent the accumulation of toxic assets. AI algorithms analyze borrowers' credit profiles and anticipate default risks, allowing banks to adjust lending strategies and optimize financial portfolios.

The ECB uses AI to automate the verification of banks' compliance with prudential regulations. Predictive models analyse the financial data reported by banks and compare them with the requirements imposed by CRD IV (Directive 2013/36/EU), detecting irregularities and

providing recommendations for correcting them. It recommended that commercial banks implement AI-based solutions in several key areas, such as behavioural analysis of access to their systems, fraud detection, automated reporting, and customer creditworthiness assessment.
By integrating AI into prudential supervision and risk management processes, the ECB contributes to creating a safer and more transparent banking system, improves banks' ability to detect and prevent risks, and facilitates compliance with European law.

- **The European Banking Authority (EBA) and Predictive Models for Financial Stability**

The European Banking Authority (EBA) plays a crucial role in strengthening European financial stability through strict risk management guidelines. The EBA recognises the importance of artificial intelligence (AI) in assessing risks and optimising prudential supervision, given the rapid evolution of digital technologies. The EBA has developed guidelines on the use of AI in bank stress tests, capital and liquidity assessments, anticipation of systemic risks and prevention of financial crises.

AI is used to assess banks' resilience in extreme economic scenarios, detect systemic financial vulnerabilities and model liquidity risks. Machine learning algorithms enable continuous monitoring of cash flows, adjustment of investment and financing strategies, and compliance with Basel III regulations.

The EBA uses AI to analyse historical data and significant economic events, identifying institutions exposed to macroeconomic risks and structural dysfunctions in the European banking system. Deutsche Bank, BNP Paribas and Santander Bank are examples of institutions that have implemented AI solutions recommended by the EBA for optimizing capital reserves, detecting liquidity risks and assessing solvency.

Commercial banks need to implement advanced AI solutions for risk scenario modelling, capital and liquidity valuation, and predictive algorithm transparency. The EBA's ICAAP and ILAAP guidelines are essential for ensuring compliance with international regulations.

By integrating AI into risk management and stress tests, EBA contributes to the stability of the European banking system, improving banks' ability to react to emerging risks and facilitating compliance with international regulations.

- **European Commission (EC) and AI Regulation in Finance**

The European Commission has developed a legislative framework to regulate the use of artificial intelligence (AI) in the financial sector, aiming to achieve a balance between innovation, security and consumer protection. The AI Act, the first piece of legislation dedicated to artificial intelligence at the European Union level, classifies AI systems according to the level of risk, imposing strict requirements. This legislative framework sets clear standards for the transparency and explainability of algorithms, and compliance with data protection regulations (GDPR).

In the area of cybersecurity, the NIS 2 Directive strengthens cybersecurity requirements for financial institutions by imposing mandatory measures to protect digital infrastructures against cyberattacks (EU Regulation 2016/679). This directive regulates how banks deploy AI-enabled solutions, forcing them to adopt advanced practices for monitoring and defending information systems.

A key aspect regulated by the AI Act is the establishment of transparency requirements for AI models, obliging banks to implement solutions that allow the explainability of automated decision algorithms. Financial institutions are required to provide clear documentation on the operation of AI systems used in lending processes, risk analysis or fraud detection.

Another aspect is the monitoring of compliance with AI standards, forcing banking institutions to comply with the data protection and cybersecurity requirements imposed by the

GDPR. These regulations ensure that AI systems collect, process, and store data responsibly, protecting users' rights and privacy.

In the field of cybersecurity, the NIS 2 Directive imposes strict measures to protect IT infrastructures, strengthening the resilience of banks' IT systems. Financial institutions are required to implement automated detection and response solutions to cyberattacks, using machine learning algorithms to identify and prevent threats in real-time. This directive obliges banks to adopt robust cyber defence strategies (European Commission, 2025).

The European Commission has also set up a supervisory mechanism to regularly assess the impact of the use of AI in the financial sector, identifying systemic risks stemming from AI and implementing corrective measures.

To comply with the requirements of the AI Act and the NIS 2 Directive, commercial banks must adopt advanced AI audit mechanisms, ensuring compliance with the requirements of transparency and explainability of algorithms. Financial institutions are required to deploy robust AI solutions to minimize the risk of biased automated decisions and ensure fairness in decision-making (European Banking Authority, 2025).

Banks must adopt rigorous measures to protect their information, aligning with the principles of the GDPR. These measures include data encryption, ethical management of personal information, and ensuring the right to challenge decisions made automatically by AI.

The integration of artificial intelligence into financial risk management has been thoroughly examined within both theoretical paradigms and empirical studies, highlighting substantial progress in the ability of banking institutions to mitigate uncertainties and enhance resilience. Theoretical discourse emphasises the capacity of artificial intelligence to model complex risk scenarios through the utilisation of predictive analytics and machine learning algorithms, thereby empowering institutions to anticipate market volatility, credit risks, and operational vulnerabilities. Empirical evidence verifies these assertions, demonstrating the efficacy of artificial intelligence in practical applications, such as fraud detection and stress testing, in which its ability to process extensive datasets in real-time proves indispensable. (Talaat., Medhat, and Shaban, 2025) For example, machine learning models have been effectively employed to detect patterns indicative of unusual behaviour in financial transactions, thereby significantly reducing instances of fraud. Furthermore, the deployment of artificial intelligence aligns with established principles of systemic risk management by facilitating continuous monitoring and adaptive responses to emerging threats, thereby fostering a proactive approach to ensuring financial stability. By synthesizing insights derived from theoretical and empirical investigations, the implementation of artificial intelligence emerges as a pivotal component of contemporary risk management strategies, providing a robust framework to address both traditional and emerging financial risks.

4.2. AI Deployment Models for Increasing Cyber Resilience

Cyberattacks are also a cause for concern. If, at present, this risk is shared and managed by commercial banks managing depositors' accounts, this risk should be managed exclusively by the central bank as the sole administrator. Obviously, the central bank will benefit from the competition of the best experts in the field, but the risk assumed would be immeasurable (Panțoiu, 2022).

In an increasingly complex digital environment that is vulnerable to cyberattacks, the use of artificial intelligence has become a fundamental element in strengthening the security and operational resilience of banking institutions. The ability of AI systems to analyze the massive volume of data in real, detect emerging threats, and automate the response to cyber incidents gives banks a strategic advantage in protecting the time of their digital infrastructure. The

implementation of these technologies, table 4, allows financial institutions to optimize defence processes against cyber threats, thus ensuring operational continuity and compliance with international regulations.

Table 4. AI Application

AI Application	Description	Benefits	Technologies
Automatic detection of cyber threats	Recognizing suspicious patterns in network traffic, user behavior, and financial activities to identify cyberattacks before they cause significant damage.	Prevention of phishing, malware, ransomware, and DDoS attacks. Elimination of false alarms and rapid intervention in real cases.	SIEM, SOC
Automating Cyber Incident Response	Quickly identify an attack, automatically isolate the compromised system and implement the necessary measures to limit its impact.	Reducing the time to detect and remediate incidents, limiting financial and reputational losses, and prioritizing threats.	SOAR
Predictive Models for Risk Assessment	Estimate the likelihood of an attack by analyzing historical data on security incidents, cyberattacks, and exploited vulnerabilities.	Developing attack simulation scenarios, assessing the impact on the IT infrastructure, identifying weaknesses and creating customized protection strategies.	
Implementing Blockchain for Transaction Security	Improving the security and transparency of financial transactions through the blockchain's decentralized architecture and advanced encryption mechanisms.	Robust protection against financial fraud, elimination of risks associated with unauthorized data changes, and automation of transaction validation processes.	Blockchain, smart contracts
Compliance with European Regulations	Implementation of explainable and periodic AI solutions, aligned with the rules imposed by the AI Act and the NIS 2 Directive.	Preventing major disruptions in the event of an attack, strengthening cyber incident management mechanisms, and implementing AI continuous operation strategies.	

Source: Authors' contribution

Implementing artificial intelligence in banks' cybersecurity strategies is an essential step in ensuring the protection of digital infrastructures and reducing the risks associated with cyberattacks. By using automated threat detection systems, automating incident response, predictive risk assessment models, and integrating blockchain to secure transactions, financial institutions can achieve a high degree of cyber resilience.

In addition to the technological benefits, compliance with European regulations is an essential aspect of the responsible use of artificial intelligence in banking. As cyber technologies become increasingly sophisticated, banks must adopt a proactive approach, based on innovation and advanced security, to protect all customer data, as well as the stability of the entire financial system.

The integration of artificial intelligence into banks' cybersecurity frameworks yields profound financial advantages, fundamentally altering the dynamics of risk mitigation and operational efficiency. By deploying cutting-edge AI-driven systems, financial institutions can significantly limit the frequency and severity of cyber threats, thereby mitigating the direct financial repercussions of data breaches, operational interruptions, and reputational damage that may otherwise cause substantial attrition in customer and investor confidence. The inherent

automation in advanced cybersecurity processes facilitates incomparable cost-efficiencies, reducing dependency on manual oversight and enabling the strategic reallocation of institutional resources toward innovation-focused initiatives, such as the enhancement of service delivery models and the development of competitive product offerings. Moreover, the reinforcement of digital infrastructures through AI not only amplifies stakeholder trust but also raises the institution's position in capital markets by increasing its solvency and ensuring compliance with stringent regulatory mandates. In this context, the adoption of AI systems transcends mere operational enhancement, emerging as a pivotal instrument for ensuring long-term fiscal stability and positioning financial entities as benchmarks of resilience and innovation within an increasingly volatile global threat landscape.

5. CONCLUSIONS

The integration of artificial intelligence into the cybersecurity strategies of banks constitutes a critical foundation for safeguarding digital infrastructures and reducing the risks associated with cyberattacks. The deployment of AI systems for automated threat detection, automated incident response, predictive models for risk assessment, and the incorporation of blockchain technology to secure financial transactions enhances the cyber resilience of financial institutions. These advanced solutions facilitate the establishment of robust defense mechanisms capable of preventing and mitigating the impact of cyberattacks on IT infrastructure.

From the perspective of banking management, the adoption of AI-driven cybersecurity measures carries significant implications. Improved security protocols reinforce customer trust, which is vital for retaining and attracting clientele in a highly competitive financial sector. The automation of cybersecurity processes not only reduces operational costs but also optimises resource allocation, allowing human resources to focus on strategic initiatives and customer engagement. Moreover, AI-powered analytics provide actionable insights into emerging threats, enabling the management to make data-driven decisions and swiftly adapt to an evolving risk environment.

In addition to the technological advancements afforded by artificial intelligence, compliance with European regulations, such as the AI Act and the NIS 2 Directive, is indispensable for the responsible application of AI in the banking sector. Financial institutions are required to implement explainable AI solutions and enhance cyber incident management mechanisms to comply with the transparency and fairness mandates imposed by these regulations. Adopting a proactive approach grounded in innovation and advanced security measures is imperative for the protection of customer data and the maintenance of financial system stability amidst increasingly sophisticated cyber threats. Banking executives must ensure that AI systems are ethically deployed to prevent discriminatory practices and support sustainable sectoral growth. These developments underscore the necessity of balancing technological innovation with strategic management and regulatory compliance in contemporary banking practices.

In anticipation of future developments, financial institutions must strategically emphasise the establishment of advanced adaptive artificial intelligence systems capable of dynamically learning and evolving in response to emergent cyber threats. Such systems would ensure a perpetually robust defence mechanism to counteract the escalating sophistication of cyberattacks. Furthermore, fostering collaborative synergies between banking entities, regulatory authorities, and technological innovators is essential for the formulation of standardised frameworks that seamlessly integrate artificial intelligence within cybersecurity infrastructures, thereby enhancing sector-wide resilience. Projections underscore the imperative of allocating resources towards the research and implementation of quantum-resistant encryption technologies, complemented by

state-of-the-art advancements in AI-driven fraud detection methodologies. These innovations are poised to redefine the cybersecurity paradigm, offering unparalleled precautions for sensitive financial data and transactional processes. By concomitantly embracing ethical AI practices and aligning operational strategies with evolving regulatory landscapes, financial institutions will not only ensure compliance but also establish a global benchmark for security innovation and operational excellence within the financial domain.

The financial implications of integrating artificial intelligence into cybersecurity strategies are considerable. By safeguarding digital infrastructures, banks not only reduce the direct costs associated with cyberattacks, such as data breaches and system interruption, but also mitigate reputational risks that could lead to customer loss and decreased market share. Enhanced security measures foster greater trust among investors and stakeholders, thereby improving the institution's solvency and access to capital markets. Furthermore, the automation of cybersecurity processes enables cost efficiencies by reducing reliance on manual interventions, freeing up resources that can be redirected towards revenue-generating initiatives such as product innovation and service optimisation. These financial outcomes underscore the strategic importance of embedding AI-driven solutions into the core framework of banking operations, ensuring both resilience and profitability in an increasingly competitive financial landscape.

REFERENCES

1. Andrea G. Rodríguez (2022). *The link between artificial intelligence and cybersecurity: assessing the European Union's approach*. Carnegie Endowment for International Peace (Sept. 2022) carnegieendowment.org
2. Ahmad M. Manasrah et al. (2024). *Advancing cybersecurity: a comprehensive review of AI-based detection techniques*. Journal of Big Data , 11(95) journalofbigdata.springeropen.com
3. Arner, D. W., Barberis, J., & Buckley, R. P. (2017). *FinTech, RegTech, and Reconceptualizing Financial Regulation*. *Northwestern Journal of International Law & Business, 37* (3), 371-413. - FinTech, RegTech and the Reconceptualization of Financial Regulation by Douglas W. Arner, Janos Nathan Barberis, Ross P. Buckley: SSRN
4. Brînză, D. E., Dumitru, M. I., (2021). The impact of the covid-19 pandemic on non-performing loans in the banking sector, Scientific Bulletin – Economic Sciences, Volume 20/ Issue 1, POLITEHNICA Bucharest, Romania
5. CJEU decision in the SCHUFA case (2023) on automated credit scoring, clarifying the application of art. 22 GDPR and transparency/personal protection obligations
6. DORA Regulation – digital operational resilience in the financial sector and the relationship with NIS2
7. EBA report & analyses – use of AI in the EU banking sector, risks identified (lack of explainability, discriminatory potential) and measures taken (increased human control) eba.europa.eu
8. Esre, A., Kapusuzoglu, A., Ceylan, N. B., (2022). *Participation banking and its contributions to the turkish economy*. Scientific Bulletin – Economic Sciences, Volume 21 / Special Issue EtaEc 2022, POLITEHNICA Bucharest, Romania
9. European Commission (2020). EU Cybersecurity Strategy for the Digital Decade. Joint Communication JOIN (2020) 18 final, Brussels, 16 Dec 2020 - ccdcoe.org
10. ENISA (2023). Artificial intelligence and cybersecurity: challenges and recommendations. Report of the European Union Agency for Cybersecurity Artificial Intelligence and Next Gen Technologies | ENISA
11. Faust Oparente Executive Director – European Insurance and Occupational Pensions Authority (EIOPA) *EU AI AND DATA FRAMEWORKS The EUROFI Magazine* | Ghent 2024 | eurofi.net AI Act and its impact on the European financial sector - EIOPA
12. Georg Leitner et al. (2024). *The rise of artificial intelligence: benefits and risks for financial stability*. ECB Financial Stability Review, May 2024. (Box A: Implications of AI for cyber risk) ecb.europa.eu

13. General Data Protection Regulation (2016). GDPR, Recital 49 – Network and information security as a legitimate interest
14. General Data Protection Regulation (GDPR) – Art. 22 and 15(1)(h) (automated decisions and the right to explanation)
15. Hagiu, A., Bărbulescu, M., (2023). *The importance of corporate governance in the banking system*, Scientific Bulletin – Economic Sciences, Volume 22/ Issue 1, POLITEHNICA Bucharest, Romania
16. Michaela Prucková (2021). *The EU's new cybersecurity package: ambitious proposals, bold tasks and deeper cooperation*. CCDCOE – Commentary on the EU Cybersecurity Strategy (Dec 2020) ccdcoe.org
17. Masike Malatji., & Alaa Tolah. (2024). *Artificial intelligence (AI) cybersecurity dimensions: a comprehensive framework for understanding adversarial and offensive AI*. AI and Ethics, 5, 883–910. https://link.springer.com/article/10.1007/s43681-024-00427-4
18. NIS2 Directive – cybersecurity requirements and management accountability in essential entities
19. Oancea, O., E., M., (2023*). Understanding consumer behaviour in a digital age*, Scientific Bulletin – Economic Sciences, Volume 22/ Issue 2, POLITEHNICA Bucharest, Romania
20. Panțoiu, A., (2022). *Banking aspects in the current economic context*, Scientific Bulletin – Economic Sciences, Volume 21/ Issue 1, POLITEHNICA Bucharest, Romania
21. Proposed Artificial Intelligence Act – classification of high-risk AI systems and transparency/explainability obligations for the financial sector
22. Proposed AI Liability Directive – aimed at closing gaps in civil liability for harm caused by AI systems
23. Raluca Csernatoni and Katerina Mavrona (2022). The Artificial Intelligence and Cybersecurity Nexus: Taking Stock of the European Union's Approach - *EU Cyber Direct – EU Cyber Diplomacy Initiative's New Tech in Review* -The Artificial Intelligence and Cybersecurity Nexus: Taking Stock of the European Union's Approach | Carnegie Endowment for International Peace
24. Rădulescu, M., (2018). *Developments of the Romanian Banking Sector after the Financial Crisis*, Scientific Bulletin – Economic Sciences, Volume 17/ Issue 1, POLITEHNICA Bucharest, Romania
25. Russell, S., & Norvig, P. (2020). *Artificial Intelligence: A Modern Approach* (4th ed.). Pearson. - Russell, S. J., & Norvig, P. (2020). Artificial Intelligence A Modern Approach (4th ed.). Pearson. - References - Scientific Research Publishing
26. Sándor Gardó et al. (2024). *Implications of Artificial Intelligence for Cyber Risk: A Blessed and a Curse*. ECB – Financial Stability Review (May 2024, Box A) ecb.europa.eu
27. Talaat, Fatma M., Medhat, T., and Shaban, W. M. (2025). *Precise fraud detection and risk management with explainable artificial intelligence*. Neural Computing and Applications. https://link.springer.com/article/10.1007/s00521-025-11396-y
28. TechDispatch EDPS (2023) – "Explainable AI", the importance of explainability for data protection and the risks of opaque systems in areas such as lending edps.europa.eu
29. The European Parliament and the Council of the EU (2023). Regulation (EU) 2024/1689 (AI Act) on a harmonised approach to artificial intelligence. Official Journal of the EU L257 (1 Aug 2024)
30. The European Parliament and the Council of the EU (2022). Directive (EU) 2022/2555 (NIS 2) on measures for a high common level of cybersecurity in the Union. Official Journal of the EU L333 (27 Dec 2022)
31. Toma Hamed., and George Drazenovic. (2024). *Impact of Artificial Intelligence on Investment: A Narrative Review*. *Algorithms for Intelligent Systems* (pp. 275–286). Springer. https://link.springer.com/chapter/10.1007/978-981-99-8438-1_20
32. Vasiliki Paschou (2024). *NIS2 vs. DORA: Common Differences and Misconceptions NIS2 vs. DORA: Common Differences and Misconceptions* | activeMind.legal
33. Yilmaz, C., Ceylan, N. B., Kapusuzoglu, A., (2021). *Evaluation of the credit risk outlook in the turkish banking sector*, Scientific Bulletin – Economic Sciences, Volume 20/ Issue 2, POLITEHNICA Bucharest, Romania.