UDK 343.9.024:336.7]:004.8(4-672EU)
343.9.024:336.7]:004.8(73)

DOI: https://doi.org/10.46763/BSSR25252567v

ADAPTING TO NEW REALITIES: FINANCIAL CRIMES AND EMERGING AI TECHNOLOGY IN GLOBAL AND EU PERSPECTIVE

Igor VULETIĆ[1]

Full Professor, Josip Juraj Strossmayer University of Osijek,
Faculty of Law, Croatia
E-mail: ivuletic@pravos.hr

Dunja DUIĆ[2]

Associate Professor, Josip Juraj Strossmayer University of Osijek,
Faculty of Law, Croatia
E-mail: dduic@pravos.hr

Abstract

The increasing integration of artificial intelligence (AI) and machine learning (ML) in financial markets has brought both opportunities and risks. While AI-driven tools enhance efficiency and profitability, they also introduce potential threats, particularly in the realm of financial crimes. This paper explores the role of AI in financial markets, focusing on its potential to facilitate fraudulent activities such as market manipulation, price fixing, and collusion. The unpredictability of AI, coupled with its ability to autonomously make trading decisions, raises complex legal and regulatory challenges.

A key issue discussed is the difficulty in attributing criminal liability when AI autonomously engages in illicit financial activities. Traditional legal frameworks rely on human intent (*mens rea*) as a cornerstone of financial crime prosecution. However, AI-driven misconduct challenges this notion, as existing laws are often inadequate in addressing cases where no clear human perpetrator can be identified. Through a comparative legal analysis of the US, UK, and European legal systems, this

[1] ORCID: 0000-0001-5472-5478.

[2] ORCID: 0000-0002-3838-413X.

paper highlights the limitations of current regulations in holding AI developers, financial institutions, or corporate entities accountable for AI-induced financial crimes.

Furthermore, the study examines recent regulatory developments, such as the EU's AI Act and Market Abuse Directive, assessing their effectiveness in mitigating AI-related financial crime risks. While these regulations enhance consumer protection and introduce oversight mechanisms, they fail to address the criminal liability of AI developers and users adequately. The paper concludes that legal reforms are necessary to adapt financial crime laws to the evolving technological landscape, particularly by considering new models of liability that encompass negligent or reckless AI-driven financial misconduct.

Keywords: *Artificial intelligence, financial crime, market manipulation, legal liability, AI regulation, autonomous trading agents.*

1. INTRODUCTION

The use of Artificial Intelligence (AI) in the financial sector unquestionably has numerous advantages, but therre are risks as well. One of these risks relates to criminal law liability for fraud and similar criminal conduct that constitutes financial crimes. The possibility of abuse can occur due to the involvement of AI in the financial sector, especially through methods such as market manipulation, price fixing and collusion. These methods imply the participation of an AI system designed to perform search tasks rather than people performing these tasks.

Problems arise when such systems, with the ability to learn from its surroundings and received data, start emitting information with the purpose of intentionally leading the contracting party down the wrong path. Some research has shown that such AI could master techniques of sending fictitious orders (which will never be performed) and concluding fictitious transactions, with the aim of defrauding good-faith third persons and gaining profit. This could occur due to the fact that AI is programmed to, among other things, find the most profitable business models. Therefore, it could be probable that an AI software recognises the conclusion of fictitious transactions as the most profitable option and then operates accordingly. Furthermore, there is the possibility of various types of illegal manipulations on the stock market, through the dissemination of false information on the value of shares by autonomous trading agents.

This paper provides an analyses of autonomous trading agents as an emerging potential threat for the financial sector. We discuss whether modern criminal law has proper tools in dealing with these new types of economic crime. Considering that these crimes are committed on the internet and therefore could have cross border consequences, we compare relevant US and EU law and EU Member States national laws and draw conclusions on the adequateness and flaws of the existing legal framework (Jung and Lee, 2017, p. 88). Finally, we distinguish EU legislation applicable to this incidents.

2. AI, financies and financial crime risk

Complex financial operations, such as stock trading, have been conducted by humans for decades. Typically, individuals who have successfully engaged in this profession have come from the ranks of exceptionally intelligent minds, adept in economics and mathematics. However, since the early nineties of the last century, there has been a gradual, and then increasingly pronounced, shift in this area of financial operations towards investors turning to the use of sophisticated Artificial Intelligence (AI) and Machine Learning (ML) tools that are being developed (Cliff and Rollins, 2013).

These are tools that enable even greater profit in shorter periods, capable of making quick and precise decisions, thereby significantly enhancing the efficiency of financial operations, delivering higher profits to investors, and reducing expenses. It is most commonly emphasized that autonomous trading agents are able to react to information significantly faster than humans and that they quickly develop patterns of efficient behavior based on repetition. On the other hand, there is a warning that it is difficult to predict how they will act in the event of unexpected circumstances that significantly deviate from the usual pattern (Easley et al, 2012, p. 19).

One of the first such examples is described by Gode and Sunder. They conducted a notable study on automated trading algorithms, particularly focusing on the dynamics of markets and the performance of such algorithms. They demonstrated that even simple algorithms, which they referred to as ‘zero-intelligence’ traders, could generate outcomes comparable to or even better than those of human traders. Their findings challenged the prevailing notion that sophisticated AI-based trading strategies were necessary for success in financial markets. Gode and Sunder’s work underscored the importance of market dynamics and the potential effectiveness of straightforward trading methods (Dhananjay and Sunder, 1993, p. 119). Soon after, several similar studies followed, continuing to develop and refine the concept of autonomous trading, with the aim of identifying the most efficient model for generating profit (Cliff and Rollins, 2013).

Today, highly precise tools have already been developed, capable of recognizing patterns in financial markets, learning from experience, and incorporating knowledge from various sources into a specific financial strategy (Abraham et al, 2003, p. 18). Such tools, for example, are used in the Forex

Market Melvin and Norrbin, 2017, p. 3) which nowdays represents one of the largest financial markets and, due to its enormity and continuous 24-hour operation, practically has no choice but to turn to autonomous trading.

In literature, certain ethical issues associated with the use of autonomous systems are particularly highlighted. It is cautioned that programmers and manufacturers should take care to incorporate certain ethical principles into the system (Wellman and Rajan, 2017, p. 609). However, at the same time, it is warned that ethics is a highly relative category, depending on the intelligence of the individual, upbringing, education and experience. An interesting example that can be cited here is a study related to autonomous vehicles, which is not the topic of discussion in this paper but can serve as an illustration. An anonymous online survey asked citizens about moral choices in traffic scenarios. They were asked if they'd buy a car programmed to save passengers or reduce casualties, most chose passenger safety (Bonnefon et al, 2016, p. 1573). This contrasts with earlier agreement that reducing casualties was more moral. It shows morality is relative and hard to define (Dennet, 1994, p. 105).

The potential for financial crime perpetrated through AI/ML tools for autonomous trading is recognized in criminological literature. It distinguishes between situations where a particular AI/ML tool is used as a means of commission, implying human intent behind it, and situations where the AI/ML tool itself malfunctions without malicious human involvement (Caldwell et al, 2020). An example of the latter scenario is provided by a case where a tool, programmed to always choose the most profitable course of action, decides to engage in fraud, market manipulation, price fixing, collusion or similar punishable behavior because it recognizes such conduct as the most profitable (King et al, 2020, p. 97). However, such analyses are still largely theoretical and devoid of concrete examples at present. Below, we will present several cases from the American financial market, which can be categorized as situations where AI/ML mechanisms autonomously caused significant financial losses.

In September 2012, US Securities and Exchange Commission issued a cease-and-desist order against Hold Brothers On-Line Investment Services for engaging in manipulative trading activities through offshore high-frequency trading accounts from January 2009 to September 2010. The activities involved 'spoofing' and 'layering,' where orders to buy or sell securities were placed and canceled to manipulate prices and deceive investors. 'Spoofing' involves placing orders and then canceling them to execute trades in the opposite direction, while 'layering' entails placing a sequence of limit orders at progressively increasing or decreasing prices to create artificial fluctuations in demand and price. Once trades occur at manipulated prices, the layered orders are withdrawn. The main distinction between these scams and traditional 'pump-and-dump' schemes is the speed and electronic execution involved. The manipulative activity occurred in just 839 milliseconds, making it impossible for a human trader to accomplish manually (Kirilenko and Lo, 2013, p. 61).

The ‘Flash Crash’ incident, refers to a sudden and significant drop in the US financial markets that occurred on May 6, 2010, within a short period of about 33 minutes. During this time, the Dow Jones Industrial Average experienced its largest intraday point decline in history, and there were extreme fluctuations in stock prices, with some trading at unusually low or high values. Regulatory agencies investigated the crash and determined that it was not caused by one single failure but rather by a combination of factors. These factors included automated trading algorithms, high-frequency trading practices, arbitrage activities, and strategies employed by market makers. These elements all came together to create a situation of extreme volatility in the financial markets Kirilenko and Lo, 2013, pp. 62-63; Borch, 2016, p. 350).

Similar incident occured on May 18, 2012, during Facebook’s highly anticipated Initial Public Offering (IPO), NASDAQ experienced significant technical glitches. NASDAQ is one of the largest stock exchanges in the world. NASDAQ uses computerized systems to facilitate trading, and it is known for listing many technology and internet-related companies (Kandel and Marx, 1997, p. 61). The systems were unable to handle the heavy trading volume, resulting in delays in calculating the opening trade. This delay allowed for new orders and cancellations to enter the system, causing further complications and uncertainty. The glitches were attributed to a race condition in the software, the unpredictable order of events where new orders conflicted with the print of the opening trade. Despite the scheduled 11:00 am start, the opening occurred 30 minutes late, with traders facing delays and uncertainty even after the market formally opened. The technical issues persisted for hours, resulting in unfilled orders and unintended purchases. These problems led to significant financial losses for traders, overshadowing the otherwise successful IPO of Facebook. The system was supposed to quickly figure out how much potential buyers should pay for Facebook shares when trading started. But because so many people wanted to buy or sell Facebook shares, the system was really slow. It took longer than usual to figure out the prices, causing a delay of about 30 minutes. During this delay, some changed their minds about buying or selling, which made things even more complicated. This delay caused confusion and made it hard for buyers to know what was happening with their orders. Some orders did not get filled at all, and some buyers ended up buying or selling more shares than they wanted. This caused a lot of frustration and financial losses for many traders (Kirilenko and Lo, 2013, pp. 63 – 63).

These incidents reveal the deficiencies and potential risks associated with the use of AI/ML tools for trading. It is important to highlight the issue of criminal liability, considering that these cases can result in or have already resulted in significant financial damage, for which the perpetrator, if he/she were human, would typically be criminally prosecuted. However, this matter is much more complex here because it involves the use of special mechanisms the behavior of which is, truth be told, unpredictable even to the creators of such systems. For example, one study suggests that AI/ML trading systems rely solely on knowledge extracted from the data they are fed. This means that poor data quality, flawed inferences, as well as unpredictable and sudden market changes can have a negative impact on the performance of such tools. In this sense, the actions of such systems can be quite unpredictable and unexpected for the people behind them (Borch, 2022, p. 1). This brings us to the problem of proving guilt, as understood in criminal law. More will be said about this in the next chapter, where a comparative analysis of different systems will determine whether economic criminal law provides an appropriate response to the problem of guilt when the *actus reus* is carried out by an AI/ML trading agent.

3. Use of AI in financial sector in EU

The majority of regulators are in the initial phases of formulating governance principles or providing guidance tailored specifically to AI for financial institutions. Within the EU, there are bodies tasked with monitoring emerging risks for both consumers and financial institutions, as well as overseeing new and existing financial activities. These bodies also implement necessary measures aimed at enhancing consumer protection, ensuring market safety and stability, and fostering regulatory practice convergence. European Banking Authority (EBA), the European Securities and Markets Authority (ESMA) and the European Insurance and Occupational Pensions Authority (EIOPA) are collectively referred to as the European Supervisory Authorities (ESAs). The European Securities and Markets Authority (ESMA) addressed the issue of Big Data as early as 2018. However, in this report, the entire risk associated with the use of AI is addressed as if it will be resolved by the implementation of Geenral Date Protection Regulation (GDPR), which we now understand is not the case (Joint Committee of the European Supervisory Authorities, 2018).

Establishing a foundational and future-oriented legal framework for the utilization of AI is today a top priority for European regulators. In its White Paper on Artificial Intelligence dated in 2020, the Commission committed to fostering the adoption of artificial intelligence while addressing the risks associated with particular uses. The Commission put forward a legal framework for artificial intelligence, which seeks to mitigate the risks posed by certain AI applications through a series of regulations centered on upholding fundamental rights and ensuring safety (European Commission, 2020). On September 28, 2022, based on the 2020 White Paper, the Commission presented the Proposal for an Artificial Intelligence Liability Directive (AILD)(AI Liability Directive, 2022). The new AI Liability Directive in the EU aimed to clarify consumers' capacity to pursue remedies for product liability stemming from faulty or harmful AI products. Nonetheless, in February 2025, the AI Liability Directive (AILD) was withdrawn as part of the EU's new effort to streamline the regulatory framework for businesses. However, while the AI Act addresses fundamental rights, the Product Liability Directive covers software, including AI, applies only to material damages. The AILD aimed to bridge this gap. The issue of how liability should be allocated within the complex AI value chain remains an important question. We must acknowledge that the primary driver behind this expedited withdrawal of AILD proposal was political: just as regulating AI was an attractive policy objective in the previous Commission term, the current climate favours deregulation of this technology.

The Market Abuse Regulationand Market Abuse Directiveestablishes a 'dual-track' system for addressing market manipulation, offering both administrative and criminal liability avenues based on the severity of the violation. Thus, each case must be assessed individually to determine the appropriate course of action (Azzutti, 2022). According to Art. 5 of the Market Abuse Directive, Member States have to take the necessary measures to ensure that market manipulation constitutes a criminal offence, at least in serious cases and when committed intentionally.

For the topic that we discussed, the applicable law in the EU would be Distance Marketing of Consumer Financial Services Directive (Distance Marketing of Consumer Financial Services Directive, 2002).The European Commission passed a legislative proposal for the new Directive regarding financial services contracts conducted remotely on May 11, 2022. Finally, the European Parliament ratified the proposed Directive during its initial reading on October 5, 2023. The Directive entered into force on October 23, 2024. Member States have to implement the new Directive within 30 months from the date of its entry into force.

For such enhancment of consumer safeguards, and establishtment of fair competition for financial services conducted online, over the phone, or through other remote marketing channels, it is important that Distance Marketing of Consumer Financial Services Direcitve provides users (consumers) with the right to request human intervention when he or she interacts with the trader through fully automated online interfaces, such as chatbots, robo-advice, interactive tools or similar means. Specificaly, Art. 16d of the Directive states : "Member States shall ensure that, in the event that the trader uses online tools, the consumer shall have a right to request and to obtain human intervention at the pre-contractual stage, and in justified cases after the distance contract has been concluded (Directive 2023/2673, Article 16)." We can conclude that when this Directive is fully implemented, contractual protection for users of autonomus trading agents will be strengthened; however, it does not ensure criminal liability of producers and distributors of AI/ML instruments. As algorithmic trading technology advances in sophistication and complexity, the Market Abuse Regulation and Market Abuse Directive Risk Regulation are becoming outdated due to the continual and remarkable progress in Artificial Intelligence fields with little development in EU legislation in this regard (Bajakić, 2024).

In the Artificial Intelligence Regulation, known as the AI Act, the European Comission endeavors to offer developers, providors and users precise guidelines and responsibilities concerning particular AI applications. The AI Act is a comprehensive legal framework designed to govern the development and utilization of AI systems across various sectors, including finance (Floridi, 2021, p. 216). The AI Act employs a customized risk-based approach. The European Parlimanet has voted in favour of the AI Act in March 2024 and it is expected to come into force before the 2024 EU elections. The AI Act will be applied within 24 months of its entry into force, with the provisions on banned AI systems already taking effect within six months of the regulation coming into force.

The AI Act categorises the risks of specific uses of AI into four different levels: unacceptable risk, high risk, limited risk, and minimal risk (Mazzini, Scalzo, 2023b). The AI Act lacks a singular and consistent definition for terms like 'financial sector' or 'financial institutions'. Instead, it appears to encompass a variety of definitions scattered throughout numerous legal frameworks (Mazzini, Scalzo, 2023a). According to the Annex III of the AI Act, financial entities are prohibited from utilizing AI systems for customer verification processes that employ biometric categorization based on sensitive customer attributes, such as race or gender. The utilization of systems that manipulate human behavior and exploit vulnerabilities, including factors like age or disability, will be deemed unacceptable in customer interactions. Consequently, financial institutions will be required to meticulously choose the AI systems employed in customer dealings to avoid infringing upon fundamental rights or participating in prohibited practices as mentioned above (Łączkowski, 2024). The regulation specifically identifies, pursuant to Annex III point 5(b) of the the AI Act, AI systems meant for assessing individuals' creditworthiness or determining credit scores will be determined to be 'high-risk AI systems. This means that before deploying AI systems to evaluate creditworthiness, banks must consider the potential impact of these systems on the fundamental rights of citizens (Sciarrone Alibrandi, et al, 2023). Financial institutions opting to utilize such systems will be required to "monitor the performance of high-risk AI systems and promptly inform their supplier or distributor of any identified risks or incidents, employ high-risk AI systems in compliance with accompanying operational guidelines, retain incident logs automatically generated by the AI system if they are under their control, ensure that designated human overseeing the high-risk AI systems possess the requisite competence, training, authority, and support and maintain logs automatically generated by the high-risk AI system as part of the documentation mandated by relevant financial services legislation" (Artificial Intelligence Act,2024, Arts 10 -15) .

In the recital of the latest version of the AI Act dated January 21, 2024, it is stated that Union legislation on financial services encompasses internal governance and risk management regulations applicable to regulated financial institutions during the provision of these services, including when employing AI systems**.** To ensure consistent implementation and enforcement of the obligations outlined in this Regulation and relevant Union financial services legislation, competent authorities responsible for overseeing and enforcing financial services regulations, notably those defined in the Directive on the taking-up and pursuit of the business of Insurance and Reinsurance, Directive on Insurance Distribution (Directive o Insurance Distribution, 2009), Directive on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms (Directive on access to the activity of credit institute, 2013) ,Regulation on prudential requirements for credit institutions and investment firms (2013)Directive on credit agreements for consumers (2008), and Directive on credit agreements for consumers relating to residential immovable property (2008),should be designated, within their respective jurisdictions, as competent authorities for supervising the implementation of this Regulation, including market surveillance activities concerning AI systems utilized or provided by regulated and supervised financial institutions, unless Member States opt to assign this market surveillance task to another authority. The recital specifically addresses credit institutions as they are listed in Annex III as high-risk AI systems but remains silent about all other financial services, except in the first sentence, where it refers to the already existing EU regulation regarding financial services (Artificial Intelligence Act, 2024, Recitle 80). The financial services are discussed in the Arts 17, 18 and 21 of the AI Act, all of which refer to the existing Union regulation of financial services : "subject to requirements regarding their internal governance, arrangements or processes under Union financial services" . (Artificial Intelligence Act, 2024, Article 18). Additionally, all EU legislation referenced in the recitals explicitly pertains to insurance and credit arrangements. However, it should be concluded that although the proposed regulation exclusively refers to alignment with EU legislation in the fields of insurance and credit arrangements, the Regulation will also apply to other financial services that utilize artificial intelligence, including autonomous trading agents. In order to clarify financial institutions that could be relevant as providers or users in the context of t the AI Act beyond the non-credit and non-insurance financial institutions, the AI Act could offer more precise guidance on how sector-specific requirements concerning internal governance and risk management intersect with the obligations outlined in the AI Act (Mazzini, Bagni, 2023a).

Recent research indicates a shared agreement on the core goals of the AI Act across various sectors, which can be condensed into four key aspects: fairness, sustainability, accuracy, and explainability**.** However, financial institutions must thoroughly assess the financial and organizational expenses associated with providing these services (Pamuk, et.al. 2024, 144). Because of the underdeveloped regulatory framework, the coordination and approval processes between financial entities and regulators can be prolonged. Specifically, conducting a comprehensive evaluation of AI-driven services and maintenance expenses relative to the enhancements achieved is imperative, regardless of whether the return on investment meets the criteria for financial institutions (Cao, 2020).

Given the difficulty in defining AI, a significant portion of what is labeled as AI in finance is not fundamentally novel but rather resembles statistical or econometric modeling techniques that have long existed (Bagattini, et.al, 2023). According to the Prenio and Yong study from 2021 many of the challenges associated with financial institutions' adoption of AI closely mirror those posed by traditional models. They highlight fairness-related issues as what is disinctive from the traditonal finacial model and explicitly tied to AI. For instance, ensuring the reliability of AI models aims to prevent discrimination resulting from inaccurate judgments. Furthermore, ensuring accountability and transparency in AI usage involves ensuring that data subjects are informed about data-driven decisions, the data utilized, its impact on decisions, and providing avenues for questioning and contesting these decisions (Yong, Prenio, 2021). Considering all above mentioned issues, it is concerning that the use of AI in the financial sector is not sufficiently regulated by the AI Act. Additionaly, mentioned EU legislation, both adopted and pending, indicates that the EU seeks to keep pace with the trends in technology and artificial intelligence development. In all the analyzed acts, the focus is on civil liability, with no provisions regulating criminal liability.

In the EU, financial institutions may find themselves balancing technological innovation with the legal obligation to adhere to market conduct rules and other regulatory standards. Meanwhile, financial supervisors confront the task of ensuring financial stability and market integrity by identifying and prosecuting algorithmic misconduct. Azzutti, Ringe, Stiehl indicete the possiblities of criminal liability by misconduct of the AI, stressing that we must bear in mind the scenario of AI-driven misconduct occuring and manipulation going undetected, malicious AI users exposing markets to vulnerability, resulting in numerous negative externalities and societal harm. Failure to effectively govern and regulate AI trading could potentially expose global capital markets to market failures and systemic instability Azzutti, et.al, 2022). That is why it is a significant oversight by the EU legislature that they did not provide clearer regulations in the AI Act regarding financial services.

4. *Mens rea*, financial crimes and AI?

In the theory of criminal law, three possible models of criminal liability are discussed in AI cases. According to the first model, AI represents a mere instrument of action behind which a human stands as the actual perpetrator or principal of the criminal act. Essentially, this involves perpetration through another person (so-called indirect perpetration), and the question of proving the guilt of the indirect perpetrator will not be disputed here, but it is possible that proving it may be difficult in terms of linking a specific individual to a specific

AI tool. The second model implies the responsibility of individuals behind AI tools according to the rules of negligence. This means that these individuals did not act intentionally (as in the first model) but did not exercise due care, resulting in certain consequences. In terms of guilt, it would be crucial to prove that the specific consequence was foreseeable, ie, that it represented the realization of a risk that was reasonably foreseeable in the given case. According to the third model, which is currently purely theoretical, AI would be capable of bearing its own autonomous guilt (Yeoh, 2019, p. 638). This would, of course, be applicable to cases where there is no guilt or it is not possible to prove the guilt of the person behind the AI entity. However, such a model is essentially nonsensical from the perspective of the purpose and role of criminal law, considering that the system of criminal sanctions is entirely tailored to humans, so AI, even if we were to declare it guilty, could not be punished (Abbott, 2020, p. 134). Therefore, we align ourselves with those who argue that existing criminal law is not an appropriate means to establish the accountability of the AI agent itself. A comparison with the concept of corporate criminal liability cannot be drawn here because that concept was designed to prevent individuals from hiding behind corporations. On the contrary, an AI system is intended to become entirely autonomous and independent of humans, so in that sense, it cannot be treated in the same way as a corporation which remains entirely under human control (Lina, 2018, p. 677). Lastly, *mens rea* is formulated in a manner that suits human offenders and encompasses not only intelligence but also intuition, a sense of ethics, and culpability.

Comparing different systems in the realm of *mens rea* is a very challenging task, given the fundamental differences in the forms of culpability. These differences are particularly pronounced between the European continental and Anglo-American systems. Below, we will delve into the analysis of the state of European continental law, UK law, and US law.

3.1. European continental law

Observing continental systems, we conclude that economic criminal offenses primarily require intent, often in the form of direct intent (*dolus directus*). Indirect intent (*dolus eventualis*) is also possible to a limited extent, which is more intriguing from the perspective of the theme of this text, hence we will devote some more attention to it.

In the context of financial crime, *dolus eventualis* may be relevant in cases where the perpetrator is aware that their actions could lead to unlawful financial gain or harm, but they consciously decide to proceed regardless. This mental state involves the perpetrator foreseeing the possibility of the illegal outcome as a likely consequence of their actions, and yet they choose to accept this risk. For example, in a case of financial fraud where an individual knowingly provides false information on financial documents to secure a loan, they may be considered to have *dolus eventualis* if they are aware that their actions could lead to financial loss for the lender but proceed regardless. German and Austrian criminal law hold this position (Tiedemann et al, 2012, p. 227). Although indirect intent is theoretically possible, in practice, it is very difficult to prove in financial crime cases and therefore relatively rare.

However, when it comes to negligence, liability in continental legal systems is generally significantly narrowed. Negligence involves a reckless disregard for the consequences of one's actions or a failure to exercise even slight care or diligence. In some legal systems, certain financial crimes may be defined in a way that encompasses acts of gross negligence, especially if the negligence leads to significant financial harm or facilitates criminal activities such as fraud or embezzlement. For example, Art 314-1 of the French Penal Code criminalizes fraud, which can include acts committed with intent to deceive or defraud others, as well as acts committed through negligence when the negligence is such that it facilitated the commission of the fraud (Novoselec, 2009, pp. 116 – 117). Similarly, Art 432-15 of the French Penal Code addresses embezzlement by public officials, which can be committed through intentional acts or acts of gross negligence leading to the misappropriation of public funds.

The specific legal definitions and requirements for establishing gross negligence as a basis for financial crime will vary depending on the laws of the jurisdiction involved. Only a very small number of financial criminal offenses can be committed through negligence. This is mostly the case with the crime of money laundering, where certain systems (eg, German or Croatian) incriminate negligence concerning the fact that money and other assets were acquired through criminal activity. Regarding other elements, intent is also sought for this criminal offense (Novoselec, 2009, p. 196).

A particular issue is the fact that in some continental legal systems there is no criminal liability for legal entities, as is the case, for example, in German law. Literature rightfully warns that this will have an adverse effect on establishing criminal liability for producers, programmers, and distributors in situations involving AI agents (Gless et al, 2016, p. 429). On the other hand, European countries that recognize criminal liability for legal entities generally accept the concept of attaching such liability to the culpability of the responsible natural person (human) managing such legal entity. Some empirical studies show that precisely because of this model, the number of criminal proceedings against legal entities in practice in such countries is very small, and it is often not possible to determine the culpability of the relevant person or who that person even is. Furthermore, in practice, it is common for a legal entity to cease to exist (due to bankruptcy or liquidation) during criminal proceedings, resulting in a mere suspension of proceedings against it. For these reasons, it can be generally concluded that the existing criminal legal framework in continental Europe largely does not correspond to the challenges of AI-driven financial crime. All of the above points to the undeniable fact that it will not be possible to classify actions resulting in significant financial damage due to AI/ML tool malfunctioning under existing criminal offenses because *dolus directus* or *dolus eventualis* will be absent, while there generally will not be room for the application of negligence. Therefore, it can be concluded that European continental law, which firmly adheres to strict doctrinal positions of legality and culpability principles, will not have an adequate criminal law response to situations described in the previous chapter. In such a case, it is possible that individuals behind AI/ML tools may escape unpunished.

3.2. UK law

In the UK, for financial crimes such as fraud, the standard for *mens rea* is typically that the individual must have acted dishonestly with the intention of making a gain for themselves or causing a loss to another party. This principle is outlined in the Fraud Act 2006, which covers a wide range of fraudulent activities (Withey, 2007, p. 220). Specifically, Section 2 of the Fraud Act 2006 outlines the offense of fraud by false representation, where the individual is required to have acted dishonestly with the intent to make a gain or cause a loss. Under the Fraud Act 2006 in the UK, the standard for *mens rea* (mental state or intent) varies depending on the specific offense. The Fraud Act introduces three main offenses: fraud by false representation (Section 2), fraud by failure to disclose information when there is a legal duty to do so (Section 3), and fraud by abuse of position (Section 4). In summary, the key elements of *mens rea* under the Fraud Act 2006 involve acting dishonestly with the specific intent to gain for oneself or another, cause loss to another, or expose another to a risk of loss, depending on the particular offense outlined in the Act.

In the context of financial crimes in the UK, recklessness may be considered as an alternative *mens rea* when establishing criminal liability (Ruggiero, 2020, p. 245). Recklessness typically involves a conscious disregard for a risk that is unjustifiable in the circumstances, and it may apply in situations where the defendant is aware of a risk but proceeds with their actions regardless. For example, the Fraud Act 2006, section 2(2) specifies that a person's conduct may be considered dishonest if they act recklessly, ie, if they are aware that there is a risk that their conduct may cause loss to another, but they still go ahead with it. This means that even if the defendant did not specifically intend to cause harm or make a gain, they may still be found guilty of fraud if they acted recklessly and their actions resulted in a loss to another party (Ruggiero, 2020, p. 245).

Similarly, in other financial crimes such as insider trading or money laundering, recklessness may also be considered as a basis for establishing criminal liability if the defendant was aware of a risk but disregarded it in their actions. It is important to note that the application of recklessness in establishing criminal liability can vary depending on the specific offense and the circumstances of the case, and it is ultimately up to the courts to determine whether the threshold for recklessness has been met based on the evidence presented. The UK law is particularly interesting because it contains a very specific criminal offense known as "reckless misconduct by a senior bank staff member". This typically involves the individual knowingly taking risks or acting in a manner that disregards the potential consequences, despite being aware of the risks involved. This behavior could include making decisions that endanger the financial stability or integrity of the bank, such as approving risky loans or investments without proper due diligence. Reckless misconduct can lead to serious financial harm or loss for the bank, its clients, and the wider economy (Wilson and Wilson, 2013, p. 1).

However, even UK law does not recognize negligent forms of economic criminal offenses. The previously described recklessness largely overlaps in substance with continental indirect intent, so the same objection already stated applies here. These cases imply the perpetrator's awareness of the possibility of consequences occurring. In the absence of a negligent form, challenges will also arise in UK law if such awareness was lacking because the human being using a certain tool relied on its proper functioning, meaning they acted in good faith and not recklessly.

It appears though that the legal framework for corporate criminal liability in the UK is significantly more flexible than in continental Europe, which could better address the situations involving the use of AI that we are discussing here. Specifically, the UK introduced the Corporate Manslaughter and Corporate Homicide Act, which took effect in 2008. This law came about after discussions that started in 1994 about how the legal system should handle situations where a company's actions lead to someone's death, whether it is due to accidents at work or problems with products. Before this law, it was difficult to hold companies accountable for deaths caused by their actions. Usually, individuals within the company had to be identified as responsible. But with this new law, companies themselves can be held directly responsible for deaths caused by the way they manage their activities, especially if this involves a serious breach of their duty of care towards people affected by their actions. Under this law, it's not just the top managment level who can be held responsible. Anyone in a significant role within the company, who has a say in how things are done, could also be held accountable. This means the law now focuses more on how the company operates as a whole, rather than just on individual actions. However, even though this law was meant to make companies more responsible for their actions, it has not been used much by the authorities, partly because has been difficult to interpret. Another important law introduced later, in 2010, is the Bribery Act. This law makes companies responsible for preventing bribery by people associated with them. If someone connected to the company bribes someone else to get an advantage for the company, and the company cannot prove it had proper procedures in place to stop this, then the company can be held responsible (Lederman, 2016, p. 71).

3.3. US law

The United States is one of the countries with the most extensive experience regarding artificial intelligence technology in the context of criminal law (Novokmet et al, 2022, p. 1). In the US legal system, the standard of proof for *mens rea* (mental state or intent) in financial crimes, as in all criminal cases, is beyond a reasonable doubt. This means that the prosecution must prove, to the satisfaction of the jury or judge, that the defendant had a culpable mental state beyond any reasonable doubt. Similar as in prevous the two previously observed legal systems, in US law, when it comes to financial crimes, *mens rea* requires that the perpetrator knew of the possibility of consequences occurring. In practice, most cases of this nature result in the conviction of individuals who were aware of the consequences and intended to produce them (which is comparable to direct intent in continental Europe). The following examples illustrate this perspective.

In the case of *United States v Skilling*, the defendant, Jeffrey Skilling, was the former CEO of Enron Corporation, a company that collapsed in 2001 due to widespread accounting fraud and corporate misconduct. The prosecution argued that Skilling knowingly participated in various fraudulent activities within Enron, such as hiding the company's financial losses and inflating its earnings to deceive investors and stakeholders. The key issue regarding *mens rea* in this case was whether Skilling had the requisite intent or knowledge of the fraudulent activities occurring within the company. The court ultimately found Skilling guilty of multiple counts of securities fraud, conspiracy, and insider trading. The verdict suggested that the jury believed Skilling possessed the necessary *mens rea* to be held criminally liable for his actions. In other words, they concluded that he knowingly engaged in the fraudulent schemes that led to the collapse of Enron (United States v Skilling [2010] 130 S.Ct. 2896).

In the case of *United States v Rajaratnam*, the defendant Raj Rajaratnam was a hedge fund manager who was accused of insider trading, specifically obtaining and using non-public information to make profitable trades in the stock market. The prosecution argued that Rajaratnam knowingly engaged in illegal insider trading by receiving confidential information from corporate insiders and using it to execute trades that would benefit his hedge fund. The key issue regarding *mens rea* in this case was whether Rajaratnam had the requisite intent or knowledge of the illegal nature of his actions. The court ultimately found Rajaratnam guilty of multiple counts of securities fraud and conspiracy to commit securities fraud. The verdict suggested that the jury believed Rajaratnam possessed the necessary *mens rea* to be held criminally liable for his actions. In other words, they concluded that he knowingly engaged in insider trading, fully aware that his conduct was unlawful (United States v Rajaratnam [2011] 660 F.3d 118 (2d Cir)).

In the case of *United States v Madoff*, the prosecution argued that Madoff knowingly operated a Ponzi scheme, in which he used funds from new investors to pay returns to earlier investors while falsely representing the scheme as a legitimate investment opportunity. The key issue regarding *mens rea* in this case was whether Madoff had the requisite intent or knowledge of the fraudulent nature of his actions. The court ultimately found Madoff guilty for knowingly engaged in fraudulent conduct, fully aware of the consequences of his actions on the investors and financial markets (United States v Madoff [2009] 709 F. Supp. 2d 458 (S.D.N.Y.)).

In the case of *United States v Stanford*, the *mens rea*, or mental state, of the defendant, R. Allen Stanford, was a key aspect of the prosecution's case. Stanford, a financier, was accused of orchestrating a massive Ponzi scheme through his company, Stanford Financial Group, defrauding investors of billions of dollars. The prosecution argued that Stanford knowingly and intentionally engaged in fraudulent activities, including misrepresenting the investments offered by his company and using investor funds for personal gain rather than for their intended purposes. They contended that Stanford was fully aware of the fraudulent nature of his actions and deliberately deceived investors to maintain the illusion of a successful investment enterprise. The court found Stanford guilty of multiple counts of conspiracy, fraud, and obstruction of justice. The verdict suggested that Stanford possessed the requisite intent to commit the offenses and was aware of the wrongful nature of his conduct (United States v Stanford [2012] 850 F. Supp. 2d 547 (S.D. Tex.)).

From this analysis, it can be concluded that the US legal system predominantly emphasizes (direct) intent concerning knowledge and intention regarding consequences. Here, even indirect intent or recklessness is viewed as controversial and deviates from established case law. Consequently, the criticisms previously addressed to other legal systems are equally applicable, if not more so, to US law.

Corporate criminal liability in the United States has been evolving for over a century. This liability is based on the concept of vicarious liability. According to this concept, courts establish a corporation's liability for the mistakes of its employees on the basis that the corporation has delegated authority to individuals, thereby empowering them to act on its behalf. Consequently, all actions performed by individuals on behalf of the corporation actually create legal obligations for the corporation itself. Essentially, US courts apply this civil law (litigation) concept to criminal law, thus holding the corporation jointly responsible for the criminal acts of its employees (such as programmers and workers). It is not necessary for the employees themselves to be held responsible (Laufer and Strudler, 2000, p. 1296). This concept of corporate liability is much broader than in the criminal systems of continental Europe, making it more suitable for situations involving the actions of AI entities.

3.4. Conclusion

From the preceding discussions, it emerges that concerning *mens rea* in financial crime within comparative law, perhaps the only dominant aspect is intent. While it may be termed differently across various systems, all observed countries share the commonality of categorizing and prosecuting only those behaviors supported by *knowledge* of all facts, including recognizing the risk of financial harm occurring. Here it is necessary to note that the previously mentioned Market Abuse Directive envisages, as a minimum standard, the criminalization of intentional criminal acts in this domain, but it also fails to address the issue of negligence liability. The same is advocated in the Market Abuse Directive regarding the criminal liability of legal entities, so proof of intentional malicious actions by responsible bodies is also required in their case.

As an issue, or more precisely a legal gap, the lack of accountability for negligence will certainly arise. Specifically, if there is no accountability in a situation where a person utilizes AI in financial transactions without awareness of the potential risk of harm and still causes harm to users (customers), then it will not be possible to establish criminal liability. This circumstance could even be exploited to some extent. For these reasons, it is important to change the basis of the concept of financial crime in a way that criminalizes negligence in situations where there is a risk of greater financial harm.

We believe that such an expansion of accountability would be justified if there is a valid market interest in protecting the customer along with the interest of those using AI tools to increase profit. This is not an activity carried out in the interest of public or common goods (unlike, for example, healthcare and human health) but rather in the private interest of profit acquisition. Accordingly, in our opinion, it is justified to tighten the assumptions for assessing (greater) risk-taking.

Regarding the criminal liability of legal entities, it should be noted that this is a concept that is a necessary prerequisite for effective criminal protection in this area. Behind AI tools for trading and financial transactions, there will almost invariably be corporations, which may sometimes be very large and have complex management structures. Therefore, the absence of this form of criminal liability from the outset narrows the scope of criminal protection. In this context, those legal systems, such as the German one, that have not yet implemented such liability are most deficient. Generally speaking, in continental Europe, the situation in this segment is more complex because the criminal liability of a legal entity is usually linked to the criminal liability and guilt of the responsible natural person, which often poses difficulties in practice. Conversely, in the Anglo-American legal sphere, especially in the US, the concept of vicarious liability and a more flexible interpretation of guilt enable more effective criminal protection. Therefore, we believe that US law is currently most in line with the technological development of the financial market in this regard and can provide the most effective criminal protection.

Continental Europe will certainly have to reconsider its rigid understandings of the institute of guilt in the long term and devise more flexible solutions to keep pace with modern developments.

5. Closing remarks

During the preceding discussions in this chapter, the issue of criminal law and European law concerning the presence of AI in financial operations has been analyzed. Risks of fulfilling the characteristics of so-called economic, or financial, crimes have been pointed out, with a warning about a possible scenario in which it may not be possible to ascertain the responsible person, thus rendering appropriate judgment unattainable. This problem has been scrutinized from a comparative perspective, looking at fundamentally different systems, Anglo-American and European. However, this analysis has led to a similar fundamental conclusion: financial crime typically entails intent as a form of culpability and does not recognize forms of negligence. Establishing intent, particularly in cases involving the integration of fully autonomous software into financial processes, is exceedingly difficult. This issue is somewhat less pronounced in the US legal system, which is traditionally market-oriented and thus more flexible in that regard. On the other hand, European criminal laws are much more stringent in this respect, hence they do not currently offer an adequate protective model at this stage of development. An additional issue for certain European laws is the absence of criminal liability for legal entities. The EU legislature's failure to provide clearer regulations in the AI Act regarding financial services is a notable oversight, despite its efforts to keep up with advancements in technology and artificial intelligence. It is evident that while the AI Act primarily focuses on aligning with EU legislation in insurance and credit arrangements, it will also extend to other financial services utilizing artificial intelligence, such as autonomous trading agents. Nevertheless, there remains a need for the AI Act to offer more precise guidance on how sector-specific requirements for internal governance and risk management intersect with the obligations outlined in the legislation. As algorithmic trading technology advances in sophistication and complexity, the Market Abuse Regulation and Market Abuse Directive risk regulation are becoming outdated due to the continual and remarkable progress in Artificial Intelligence fields and no development in EU legislation in this regarad. Upon examining both adopted and pending EU legislation concerning the use of AI in the financial sector, it becomes apparent that the full implementation of these regulations will enhance contractual protection for users of autonomous trading agents. However, it falls short of ensuring criminal liability for producers and distributors.

Consequently, the conclusion is that financial crimes will need to undergo appropriate reform in terms of defining their characteristics and forms of culpability (intent and negligence) in the near future, to adapt to the new reality and provide effective criminal law protection to financial markets.

Bibliography

Abbott, R. (2020). *The reasonable robot: Artificial intelligence and the law*. Cambridge University Press.

Azzutti, A. (2022). AI trading and the limits of EU law enforcement in deterring market manipulation. *Computer Law & Security Review, 45*, 9 https://doi.org/10.1016/j.clsr.2022.105690.

Azzutti, A., Ringe, W.-G., & Stiehl, S. H. (2022). The regulation of AI trading from an AI life cycle perspective. European Banking Institute Working Paper Series, 130/2022. Retrieved January 30, 2025, from https://ssrn.com/abstract=4260423

Abraham, A., Chowdhury, M. U., & Petrovic-Lazarevic, S. Y. O. (2003). Australian forex market analysis using connectionist models. *Management*, 29, 18-22.

Bajaković, I. (2024). *Navigating the future of EU's digital finance and open financial strategic autonomy through strategic regulatory management. Balkan Social Science Review, 24*(24), 7–31.

Bagattini, G., Benetti, Z., & Guagliano, C. (2023). Artificial intelligence in EU securities markets. *European Securities and Markets Authority (ESMA) Report on Trends, Risks, and Vulnerabilities – Risk Analysis*. ESMA.

Bonnefon, J.-F., Shariff, A., & Rahwan, I. (2016). The social dilemma of autonomous vehicles. *Science*, 352, 1573–1576. https://doi.org/10.1126/science.aaf2654

Borch, C. (2022). Machine learning, knowledge risk, and principal-agent problems in automated trading. *Technology in Society,* 68, 1–10. https://doi.org/10.1016/j.techsoc.2021.101852

Borch, C. (2016). High-frequency trading, algorithmic finance and the Flash Crash: reflections on eventalization. *Economy and Society*, 45(3–4), 350–378. https://doi.org/10.1080/03085147.2016.1263034

Caldwell, M., Andrews, J. T. A., Tanay, T., & Griffin, L. D. (2020). AI-enabled future crime. *Crime Science*, 9(14), 1–14. https://doi.org/10.1186/s40163-020-00123-8

Cao, L. (2020). AI in finance: A review. http://dx.doi.org/10.2139/ssrn.3647625

Cliff, D., & Rollins, M. (2013). Methods matter: A trading agent with no intelligence routinely outperforms AI-based traders. IEEE Symposium on Computational Intelligence for Engineering Solutions, 392. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9308172

Dennett, D. C. (1994). The myth of original intentionality. In E. Dietrich (Ed.), *Thinking computers and virtual persons: Essays on the intentionality of machines* (pp. 91 - 107). Academic Press.

Easley, D., López de Prado, M., & O'Hara, M. (2012). The volume clock: Insights into the high-frequency paradigm. *The Journal of Portfolio Management*, 38(1), 1-23. https://dx.doi.org/10.2139/ssrn.2034858European Commission.

(2020). White paper on artificial intelligence – A European approach to excellence and trust (COM 2020 65 final).

European Commission, 'Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence' (AI Liability Directive), COM (2022) 496 final.

European Parliament & Council of the European Union. (2002, September 23). *Directive 2002/65/EC of the European Parliament and of the Council of 23 September 2002 concerning the distance marketing of consumer financial services and amending Council Directive 90/619/EEC and Directives 97/7/EC and 98/27/EC (Distance Marketing of Consumer Financial Services Directive). Official Journal of the European Communities, L 271, 16–24.*

European Parliament & Council of the European Union. (2008, April 23). *Directive 2008/48/EC of the European Parliament and of the Council of 23 April 2008 on credit agreements for consumers and repealing Council Directive 87/102/EEC. Official Journal of the European Union*, L 133, 66–92

European Parliament & Council of the European Union. (2009, November 25). *Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009 on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II) (recast). Official Journal of the European Union*, L 335, 1–155.

European Parliament & Council of the European Union. (2013, June 26). *Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC. Official Journal of the European Union*, L 176, 338–436.

European Parliament & Council of the European Union. (2014, April 16). *Directive 2014/57/EU of the European Parliament and of the Council of 16 April 2014 on criminal sanctions for market abuse (Market Abuse Directive). Official Journal of the European Union*, L 173, 179–189.

European Parliament & Council of the European Union. (2014, February 4). *Directive 2014/17/EU of the European Parliament and of the Council of 4 February 2014 on credit agreements for consumers relating to residential immovable property and amending Directives 2008/48/EC and 2013/36/EU and Regulation (EU) No 1093/2010. Official Journal of the European Union*, L 60, 34–85.

European Parliament & Council of the European Union. (2016, January 20). *Directive (EU) 2016/97 of the European Parliament and of the Council of 20 January 2016 on insurance distribution (recast). Official Journal of the European Union*, L 26, 19–59.

European Parliament & Council of the European Union. (2023, November 22). *Directive (EU) 2023/2673 of the European Parliament and of the Council of 22 November 2023 amending Directive 2011/83/EU as* *regards financial services contracts concluded at a distance and repealing Directive 2002/65/EC. Official Journal of the European Union*, L 2023, 2673–2687

European Parliament & Council of the European Union. (2013, June 26). *Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012. Official Journal of the European Union*, L 176, 1–337.

European Parliament & Council of the European Union. (2014, April 16). *Regulation (EU) No 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse (market abuse regulation) and repealing Directive 2003/6/EC of the European Parliament and of the Council and Commission Directives 2003/124/EC, 2003/125/EC and 2004/72/EC (Market Abuse Regulation). Official Journal of the European Union*, L 173, 1–61

European Parliament & Council of the European Union. (2024, June 13). *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). Official Journal of the European Union*, L 1689,

Floridi, L. (2021). The European legislation on AI: A brief analysis of its philosophical approach. *Philosophy & Technology, 34*, 215-222. https://doi.org/10.1007/s13347-021-00460-9

Gless, S., Silverman, E., & Weigend, T. (2016). If robots cause harm, who is to blame? Self-driving cars and criminal liability. *New Criminal Law Review*, 19(3), 412–436. https://dx.doi.org/10.2139/ssrn.2724592

Gode, D. K., & Sunder, S. (1993). Allocative efficiency of markets with zero-intelligence traders: Market as a partial substitute for individual rationality. *Journal of Political Economy*, 101(1), 119-137.

Joint Committee of the European Supervisory Authorities. (2018, March 15). *Joint Committee final report on big data* (JC/2018/04).

Jung, J., & Lee, J. (2017). Contemporary financial crime. *Journal of Public Administration and Governance*, 7(2), 88 – 97, http://dx.doi.org/10.5296/jpag.v7i2.11219

Kandel, E., & Marx, L. M. (1997). Nasdaq market structure and spread patterns. *Journal of Financial Economics*, 45(1), 61–89. https://doi.org/10.1016/S0304-405X(96)00894-X

King, T. C., Aggarwal, N., Taddeo, M., & Floridi, L. (2020). Artificial intelligence crime: An interdisciplinary analysis of foreseeable threats and solutions. *Science and Engineering Ethics*, 26(1), 89–120. https://doi.org/10.1007/s11948-020-00224-9

Kirilenko, A. A., & Lo, A. W. (2013). Moore's law vs. Murphy's law: Algorithmic trading and its discontents. *Journal of Economic Perspectives*, 27(2), 51–72. https://doi.org/10.2139/ssrn.2235963

Lederman, E. (2016). Corporate criminal liability: The second generation. *Stetson Law Review*, 46, 71–87.

Łączkowski, H. (2024, February 1). Work on the AI Act: The financial sector's perspective on artificial intelligence regulations. TKP. Retrieved January 30, 2025, https://www.traple.pl/en/work-on-the-ai-act-the-financial-sectors-perspective-on-artificial-intelligence-regulations/

Laufer, W. S., & Strudler, A. (2000). Corporate intentionality, desert, and variants of vicarious liability. *American Criminal Law Review*, 37, 1285–1312.

Lina, D. (2018). Could AI agents be held criminally liable? Artificial intelligence and the challenges for criminal law. *South Carolina Law Review*, 69(3), 677–696.

Mazzini, G., & Bagni, F. (2023a). Considerations on the regulation of AI systems in the financial sector by the AI Act. *Frontiers in Artificial Intelligence*, 6. doi: 10.3389/frai.2023.1277544

Mazzini, G., & Scalzo, S. (2023b). The proposal for the Artificial Intelligence Act: Considerations around some key concepts. In C. Camardi (Ed.), *La via europea per l'Intelligenza artificiale* (The European approach to Artificial Intelligence) . Cedam.

Melvin, M., & Norrbin, S. C. (2017). *International money and finance* (9th ed.). Elsevier Academic Press.

Novokmet, A., Tomičić, Z., & Vinković, Z. (2022). Pretrial risk assessment instruments in the US criminal justice system—What lessons can be learned for the European Union. International Journal of Law and Information Technology, 30(1), 1–22. doi: https://doi.org/10.1093/ijlit/eaac006

Novoselec, P. (2009). *Uvod u gospodarsko kazneno pravo* (Introduction to Economic Criminal Law). Pravni fakultet Sveučilišta u Zagrebu.

Pamuk, M., Schumann, M., & Nickerson, R. C. (2024). What do the regulators mean? A taxonomy of regulatory principles for the use of AI in financial services. *Machine Learning and Knowledge Extraction*, 6(1), 143-155. https://doi.org/10.3390/make6010008

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)

Ruggiero, V. (2020). Hypotheses on the causes of financial crime. *Journal of Financial Crim*e, 27(1), 245–257. https://doi.org/10.1108/JFC-02-2019-0021

Sciarrone Alibrandi, A., 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, 2023(138). Available at SSRN http://dx.doi.org/10.2139/ssrn.4414559

Tiedemann, K., Valerius, B., Vogel, J., Schünemann, B., & Möhrenschlager, M. (Eds.). (2012). Band 14 §§ 263-266b, *Strafgesetzbuch* (Criminal Code) Leipziger Kommentar (12th ed.). De Gruyter.

Wellman, M. P., & Rajan, U. (2017). Ethical issues for autonomous trading agents. *Minds and Machines,* 27(4), 609-617. https://doi.org/10.1007/s11023-017-9440

Yong, J., & Prenio, J. (2021). *Humans keeping AI in check – Emerging regulatory expectations in the financial sector* (FSI Insights on Policy Implementation No. 35). Financial Stability Institute, Bank for International Settlements. https://www.bis.org/fsi/publ/insights35.pdf