



Journal of Business Crime

e-ISSN: 3090-4412
Vol 02 (1) 2026 p. 1-9

© Miguel Abel, 2026

Corresponding author:
Miguel Abel
Email : miguel.abel@usc.es

*Received 27 January 2026;
Accepted 3 March 2026;
Published 4 March 2026.*

This is an Open Access article distributed under the terms of the [Creative Commons Attribution 4.0 International license](https://creativecommons.org/licenses/by/4.0/), which permits unrestricted reuse, distribution, and reproduction in any medium, provided the original work is properly cited.



Conflict of interest statement:
Author(s) reported no conflict of interest

DOI: [http://doi.org/10.70764/gdpu-jbc.2026.2\(1\)-01](http://doi.org/10.70764/gdpu-jbc.2026.2(1)-01)

ARTIFICIAL INTELLIGENCE AND MONEY LAUNDERING IN THE APPLICATION OF INTERNATIONAL CRIMINAL LAW

Miguel Abel¹

¹ University of Santiago de Compostela, Spain

ABSTRACT

Objective: This study examines the legal and theoretical issues related to using Artificial Intelligence (AI) for preventing and enforcing money laundering under international and European law. It highlights the conflict between technological advancements and the safeguarding of fundamental rights, especially regarding the EU's 2024 anti-money laundering regulatory package and the AI Act. This work was financially supported by the PID2024-160160OB-I00 project of the Spanish State Research Agency (Ministry of Science, Innovation and Universities), Operational Program FEDER "A way of making Europe"

Research Design & Methods: This research examines how different EU regulations and directives on Artificial Intelligence align with each other. It analyzes key concepts such as the Europeanization of criminal law, the principles of legality and proportionality, and the balance between security and liberty. The study uses secondary data from EU legal documents and academic literature.

Findings: This research shows that AI can help detect and combat money laundering, but it also poses risks such as opaque algorithms, bias, and privacy violations. The EU 2024 regulatory framework seeks to make the use of AI more humane and trustworthy, but differences in criminal law across countries and the lack of a unified European Criminal Code make enforcement difficult. Concerns remain about the proportionality and legality of sanctions among Member States.

Implications: The study highlights the need for continuous legal changes, close human supervision, and a distinct separation of administrative and criminal law for using AI in anti-money laundering systems. It also emphasizes strengthening the alignment of criminal law across Europe for better legal clarity and fairness.

Contribution & Value Added: This paper looks at how international and European criminal law is developing in the digital world. It links AI governance with anti-money laundering policies. The paper critically assesses the EU 2024 regulatory framework and offers suggestions for balancing technological innovation with the protection of fundamental rights in the criminal legal system.

Keywords: International Criminal Law, Artificial Intelligence, Money Laundering.

JEL codes: K14, K42, O33

Article type: research paper

INTRODUCTION

In today's era of rapid digital transformation, Artificial Intelligence (AI) has emerged as a multi-functional cornerstone of the global economy. From high-frequency trading to personalized banking, AI's ability to process massive data sets in real time has redefined financial efficiency (Ali et al., 2025). However, this technological leap is a 'double-edged sword' (FATF, 2021). While offering unprecedented capabilities for economic growth, AI simultaneously provides sophisticated tools for criminal networks to obscure the origins of illicit funds with a speed and complexity that traditional oversight mechanisms struggle to match (Boukherouaa et al., 2021; Trozze et al., 2022). The global financial system is vulnerable to money laundering using AI technologies, such as automated smurfing, deepfake identity theft, and the use of generative AI to circumvent KYC protocols (Benavides et al., 2026). This poses a threat to the integrity of international financial markets. Criminals exploit the "black box" nature of AI, making it difficult for law enforcement to detect money laundering (Philipponnat, 2025). The international community now faces a dilemma about how to encourage technological innovation without giving opportunities to organized crime.

On May 31, 2024, the European Union approved a new anti-money laundering directive, 1640 (European Parliament and Council of the European Union, 2024a), and two other regulations, 1620 (European Parliament and

Council of the European Union, 2024b), which establishes the European Anti-Money Laundering Authority, and 1624 (European Parliament and Council of the European Union, 2024c), which provides directly applicable rules on preventing money laundering by the financial system. The European Union also adopted Regulation 1689 on artificial intelligence (AI) on June 13, 2024 (European Parliament and Council of the European Union, 2024d). The three regulations European Union 1620/2024, 1624/2024 and 1689/2024, and the Directive 1640/2024 represent a huge challenge for the application of international criminal law due to the emergence of AI, with a dizzying and frightening development, to which an infallible halo is given that does not correspond to reality, with an ambivalent effect, which makes life easier but creates new risks that must be addressed within the security-freedom framework, because although AI tools can revolutionize the fight against money laundering, it is necessary to maintain a balance between effectiveness and safeguarding fundamental rights.

Thus, article 76.5 of Regulation 1624/2024 of 31 May on the prevention of money laundering allows decisions involving AI systems, but article 75 g) only allows the sharing of information generated by AI if it has been subject to appropriate human supervision, in accordance with the Union's demands for "human-centered and trustworthy" AI (whereas 1 of Regulation 1689/2024 of 13 June on AI). Furthermore, despite the current existence of European anti-money laundering regulations, and the survival of the Union depends on their success, the crime of money laundering is not punished equally in the criminal codes of each European country, and the Community does not have European criminal law to protect its own interests. Although the Union increasingly directly applies rules, such as Regulation 1624/2024, which complains of fragmented approaches and inconsistent application (whereas 2).

Finally, the fight against money laundering requires, according to Regulation 1624/2024, "rapid and continuous adaptations of the legal framework" in the face of the constant evolution of technology and the means available to criminals (whereas 83) and requires preserving "social and financial inclusion" (whereas 78). In this sense, the Regulation highlights the positive aspects of new products but also warns that "it is important to be vigilant regarding the risks associated with the supply of innovative products or services" (whereas 7), which will be addressed in this paper.

Despite these strong regulations, the EU's financial stability depends on their successful implementation. A major obstacle remains: money laundering crimes are not punished equally across the criminal laws of individual European member states. The Community currently lacks a unified European criminal law to protect its own interests, leading to what Regulation 1624/2024 describes as a fragmented approach and inconsistent application.

Furthermore, combating money laundering requires rapid and continuous adaptation of the legal framework to counter the evolution of criminal methods while maintaining social and financial inclusion. Although the Regulation acknowledges the positive potential of innovative products, it warns of the need to remain vigilant about the risks of these services. This paper will examine these tensions, focusing on legal gaps and challenges in aligning AI governance with international criminal law standards. It contributes to the theoretical development of international and European criminal law in the digital age by integrating the discourse on AI governance with anti-money laundering criminal policy. This paper provides a critical normative assessment of the 2024 EU regulatory framework and offers recommendations for balancing technological innovation with the protection of fundamental rights in a coherent and harmonious criminal justice system

LITERATURE REVIEW

The Paradox of Digitalization and the Ambivalence of Artificial Intelligence

Digitalization in the financial sector has created a new scenario that is ambivalent in nature. On the one hand, this technology improves interaction and efficiency, but on the other hand, it creates new barriers and distances within the legal system (Pérez, 2024; Abel, 2024). AI is often viewed as a universal solution (panacea), but literature shows that this technology is fallible (can be wrong) due to programming flaws and lack of algorithm control (Caro-Coria, 2022; Miranda, 2022b). The use of AI in law is often shrouded in an "infallibility halo" that does not correspond to reality, given that its statistics and methodologies are easily manipulated and prone to systemic bias.

The Conflict Between Security and Freedom in Law Enforcement

The integration of AI in combating money laundering must be managed within the framework of the conflict between security and freedom (Muñoa, 2023). Although AI has the potential to revolutionize investigative efficiency, experts emphasize the importance of maintaining a balance between operational effectiveness and the protection of fundamental rights (Morón, 2024). The secrecy of algorithms has been criticized for its lack of transparency and reproducibility, even compared to "ancient alchemy" where the results of decisions appear without any known logical process (Demetrio, 2022).

New Technology, Anonymity, and Criminal Risk

The emergence of blockchain technology and cryptoassets poses a major challenge for law enforcement due to its anonymity features (Miranda & Aires, 2022). The use of mixing services (mixers/tumblers) has become a key tool for criminals to launder Bitcoin and other digital assets (Miranda, 2024b). Recent regulations (such as EU Regulation 2023/1113 and MiCA) specifically highlight the high risk of this anonymity-enabling technology as a serious threat to financial integrity (Miranda & Aires, 2022).

Collaborative Compliance Model

Modern compliance theory no longer views AI as the absolute determinant of a person's guilt or innocence, but rather as a collaborative model between humans and machines (Miranda, 2022b). AI in compliance programs must provide added value through proactive and preventive roles, rather than merely reacting to risks that have already occurred (Caro-Coria, 2022). However, this development should not lead to the creation of a "surveillance society" that violates privacy rights (Navarro, 2022).

The Challenge of Harmonizing International and European Criminal Law

In the field of international criminal law, there is no autonomous doctrinal body with sufficiently strong general principles. Currently, what is happening is the Europeanization of national criminal law (González, 2025). This harmonization is often imperfect due to the absence of a European Criminal Code: The Community does not have a uniform European Criminal Code, so penalties for money laundering vary from country to country (Ferré, 2021); Proportionality Issues: Some directives (such as 2018/843) have been criticized for violating the principle of proportionality through invasive processing of personal information on small-value transactions (Lorenzo, 2025); Democratic deficit: The structure of the community's legislative process still needs improvement to address the democratic deficit and ensure strict legality principles (Fernández, 2021).

Ethics and Constitutional Rights in Algorithms

The use of private algorithms by large technology companies poses challenges to the principles of presumption of innocence and equality of arms due to their opaque nature. The delegation of judicial power to machines is even viewed by some experts as a threat to human dignity and the potential extinction of human values in the judicial system (Miranda, 2022b).

METHODS

This study uses a normative legal research method with a qualitative approach that focuses on the analysis of legal texts and doctrines. The first approach is the statutory approach, which critically examines the synchronization between the 2024 European Union Anti-Money Laundering regulatory package (Regulations 1620/2024, 1624/2024, and Directive 1640/2024) with the AI Act (Regulation 1689/2024). This analysis aims to identify legal gaps and contradictions between the mandate of technological efficiency and the protection of fundamental rights. A conceptual approach is also used to analyze key doctrines such as the Europeanization of criminal law, the principle of legality, proportionality, and the security-freedom conflict. This study is based on secondary data, including European Union legal documents and relevant academic literature.

This study applies a conceptual approach by referring to literature and the opinions of leading international legal experts to analyze principles such as "Europeanization of criminal law" and "the principle of proportionality" in the context of digitalization. Through the technique of legal synchronization analysis, this study compares the application of criminal standards at the member state (national) level with the European Union's harmonization ambitions to evaluate the effectiveness of international criminal law enforcement against AI-based crimes. The data used is secondary data consisting of official European Union legal documents, court decisions, and relevant academic literature as listed in the reference list.

RESULT AND DISCUSSION

The ambivalent effect of AI

Digitalization has created a new landscape marked by inherent ambivalence (Pérez, 2024). On the one hand, digitalization has produced new forms of separation and structural barriers; on the other hand, digitalization has enabled various forms of interaction that were previously unimaginable. While digital technology significantly improves efficiency and convenience, it simultaneously introduces new risks that must be managed within the broader framework of the security-freedom tension (Abel, 2024). In the context of combating money laundering, artificial intelligence offers transformative potential; however, its implementation requires a careful balance between operational effectiveness and the protection of fundamental rights (Pavlidis, 2023).

According to Regulation 1624/2024, the fight against money laundering requires "rapid and continuous adaptations of the legal framework" in the face of the constant evolution of technology and the means available to

criminals and requires preserving "social and financial inclusion". In this sense, the Regulation highlights the positive aspects of new products but also warns that "it is important to be vigilant regarding the risks associated with the supply of innovative products or services".

Risks of AI

Artificial intelligence should not be understood as a universal "panacea" capable of solving all structural problems (Miranda, 2022c). On the contrary, artificial intelligence still has inherent weaknesses (Caro-Coria, 2022), mainly due to programming errors and the limitations of human supervision of algorithmic processes. Nevertheless, AI is often surrounded by an aura of unwarranted infallibility, because its output depends on statistical models and methodological frameworks that are susceptible to manipulation. In addition, AI systems require constant human intervention and recalibration, and their decision-making patterns can reproduce or even reinforce existing social biases and structures of oppression (Jaume, 2023). Concerns have also been raised about its limited reliability, lack of transparency, and lack of reproducibility (Demetrio, 2022). For these reasons, the opacity of algorithmic systems is metaphorically compared to ancient alchemy, as its conclusions are sometimes difficult to investigate or reconstruct logically (Martínez, 2022). In addition, the environmental and energy catastrophe caused by artificial intelligence was denounced, since, as an example, a conversation with ChatGPT consumes half a liter of water and tens of millions are made daily (European Parliament and Council of the European Union, 2023; Jaume, 2023; Wu and Tran, 2018).

Certainly the absence of credit risk, as there is normally a prepayment, discourages service providers from obtaining complete and accurate information about clients or the nature of commercial relationships (FATF, 2010), providers who usually use "weak technology" (Gómez, 2021); the quality of the data that generates false positives and negatives (Miranda, 2023) and the "voracity" of the markets to access "all types of data for the most varied uses" and its obtaining outside the interested parties contrary to the Right to Privacy has been denounced (Morón, 2024), with the problems of liability for damages caused by AI in models designed for people, physical or legal (Miranda & Aires, 2022) and the dangers of both algorithms ending judicial discretion (Miranda, 2020) and transforming prisons into institutions of control rather than socialization; and the delegation of judicial power to machines has even been described as a sacrifice or extinction of humanity and genocide (Nunes, 2021).

In addition, security gaps have been detected in artificial intelligence and blockchain tools have been associated with the use of cryptocurrencies for money laundering (Domingos, 2024), there are tumblers or multi-address mixers that guarantee anonymity (Gómez, 2021), in fact mixer services processed the majority of bitcoins laundered (Joffre-Calasich, 2022), Regulation (EU) 2023/1113, of May 31, on information on transfers with funds and cryptoassets, warns of the high risk regarding money laundering of technologies designed for anonymity, citing "cryptoasset mixers" and the Regulation (EU) 2023/1114, also of May 31, or MiCA Regulation, on cryptoasset markets, also added a section 6 to article 18 of Directive 2015/849 that obliges the European Banking Authority to pay special attention, by favoring anonymity, to mixing services.

In short, to condemn the dangers that artificial intelligence and new technologies represent with respect to money laundering, it has been said that the name of the search engine chosen on the Internet allows us to open "the gates of Dante Alighieri's hell", so before clicking the button should remember what was written on the lintel of the door to hell: "lasciate ogni speranza, voy che entrate" (Dante, 1870; Salazar, 2024).

Advantages of AI

However, artificial intelligence and the development of technologies, including the Internet, have implied unquestionable advantages (Mata-Barranco, 2020), cryptographic security, the traceability of the blockchain, the development of user profiles (Gómez, 2021), patterns of money laundering and suspicion (Miranda, 2023), the obtaining of evidence by the prosecution through Transaction tracking through blockchain and artificial intelligence even facilitates, through online resources, identity verification or other duties of diligence for the prevention of money laundering (The Money Laundering Officer's Practical Handbook, 2011), such as in Fintech companies through big data systems and computer applications or Regtech, technologies that facilitate compliance with regulatory requirements. The Chainalysis Reactor investigation software is used judicially as expert evidence by identifying transaction users and analyzing movement flows, searching for bitcoin addresses to detect tax crimes (Joffre-Calasich, 2022), with which the encrypted protocols "serve investigation and repression organizations to track illicit operations and identify those responsible" (Ferré, 2024), and Regulation 2023/1113, of May 31, on information on fund transfers and crypto assets, refers to the "use of analytical tools based on distributed registry technology, to detect the origin or destination of cryptoassets" and with a vision of the future obliges the Commission to present, until June 30, 2027, a report on technological solutions for compliance with the obligations imposed on cryptoasset service providers with the latest advances and the use of distributed ledger analytical tools to identify transfers as well as trends in the use of self-hosted addresses to make transfers without third-party intervention and their risks for money laundering.

AI and compliance

It is not about artificial intelligence based on big data deciding innocence or guilt, since justice is not programmable and requires human intervention, but about a collaborative model between people and machines that process a large amount of information to make predictions (Miranda, 2022a), with the ability to filter and analyze almost unlimited data (Caro-Coria, 2022). Nor is it just that compliance programs exempt or mitigate the criminal liability of legal entities and that they have an evidentiary function, but that artificial intelligence and new technologies incorporated into compliance programs must provide added value to management business and play a more proactive or preventive role, warning of risks, than reactive, reacting against dangers that have already materialized, but without reaching a "surveillance society" (Miranda, 2024a; Navarro, 2022).

Ethical considerations

On the other hand, artificial intelligence is in the hands of large technology companies more powerful than many states, which by using "secret and industrial property" can end up violating "the most basic constitutional principles and rights, such as non-discrimination or freedom of information" and the proof by private algorithms challenges the presumption of innocence and the contradiction or equality of arms, due to its opacity (Caro-Coria, 2022; Miranda, 2022c). The replacement of the judge by the AI also violates the constitutional principle of human dignity (Greco, 2020). Obviously, "innovation and development are permanent sources of tension for the Law", forcing it to "redefine categories or even generate new ones" (Navarro, 2022). Therefore, the risks of artificial intelligence must be offset by "reliable" AI regulation that protects, among many other things, from algorithmic bias (Caro-Coria, 2022; Pérez, 2024).

In this sense, the Presidency of the Council and the negotiators of the European Parliament reached an agreement in December 2023 on the Artificial Intelligence Regulation to ensure that its use in Europe is safe and respects both fundamental rights and the values of the Union (Consejo-Europeo, 2023). After two marathon sessions, of 22 and 14 hours, a framework was agreed upon so that technological innovation is guided by ethical and legal principles, with a risk-based approach that requires stricter standards for cases of greater danger, evaluations of impact on fundamental rights prior to the implementation of high-risk artificial intelligence systems and prohibitions on uses of artificial intelligence that entail unacceptable risks, such as cognitive behavioral manipulation, indiscriminate tracking of facial images and some cases of police surveillance predictive, although exceptionally police emergency procedures are allowed to use artificial intelligence tools without assessment or remote biometric identification in certain crimes and real threats, such as terrorism or more serious crimes (Consejo-Europeo, 2023). The Regulation also affects generative artificial intelligence models, such as ChatGPT, with rules to guarantee transparency and risk management, as well as copyright, which has already generated lawsuits against the companies that created ChatGPT and other popular platforms artificial intelligence (Grynbaum and Mac, 2023).

Thus, Regulation 1624/2024 on the prevention of money laundering allows decisions involving AI systems, but only allows the sharing of information generated by AI if it has been subject to appropriate human supervision (European Parliament and Council of the European Union, 2024c), in accordance with the Union's demands for "human-centered and trustworthy" (European Parliament and Council of the European Union, 2024d).

Application of international criminal law

The future in the application of international criminal law is uncertain. In this area, there is not "an autonomous doctrinal body sufficiently endowed with general principles" (González, 2025), and initiatives arose for the construction of a European criminal law in a broad sense that have not yet become positive law (Lorenzo, 2021), such as the Corpus Iuris, a doctrinal text commissioned by the European Parliament and the Commission from a group of experts led by Professors Tiedemann and Delmas-Marty (Ferré, 2021), or the so-called eurocrimes. Therefore, there is no "something similar to a European Criminal Code" (Foffani, 2021), although there are criminal harmonization directives with minimum standards on the definition of crimes and sanctions as well as intense judicial cooperation (Foffani, 2021). It is a "Europeanization of national criminal law", and not an "authentic" or "properly European criminal law", a Europeanized national law in which the importance of harmonization through directives without direct effectiveness but which must be transposed in each country is indisputable (Fernández, 2021; González, 2025; Lorenzo, 2021). Despite this "clear legal basis", since the Lisbon Treaty of 2008, the political basis for the construction of a European criminal law is uncertain, at a time when several countries and political parties question the idea of Europe (Foffani, 2021), and also there are "strong resistances" and legal difficulties "to unify criteria at the international level", such as in matters of criminal liability of legal entities (Abel, 2021; Ferré, 2021; González, 2025).

However, money laundering, due to globalization (Abel, 2002), has been "the center of gravity of an intense network of initiatives" in the international area, and continues to be among "the great challenges of criminal policy" in the world (Foffani, 2021). The fight against money laundering has generated a necessary internationalization of criminal law due to the common objectives that exceed the sovereignty of each country and the facilities that "legislative and judicial uniformity" represents, although this globalization has also been highly

criticized by those who "They oppose a world government of the economy and defend the reaffirmation of the identity of the peoples" (Fernández, 2021).

Money laundering belongs to the "hard core" of eurocrimes and constitutes, from the beginning and in the last 35 years, "a paradigmatic example of a European criminal policy that aspires to become authentic European criminal law" (Foffani, 2021), that is why, it has been rightly described as "the type of crime most intensely determined by the community harmonization process" (Fernández, 2021), since seven directives and four regulations in less than three and a half decades on the same crime establish a record that is difficult to surpass, although, surprisingly, the Union was slow to adopt one real criminal harmonization, since the first five directives refer to administrative prevention measures, despite its great criminal political impact that motivated the criminalizing wave of money laundering throughout Europe, and only Directive 2018/1673 is a true instrument of penal harmonization (Abel, 2025; Foffani, 2021).

If progress is to be made in the construction of European criminal law, it is essential to delimit precisely criminal law from administrative sanctioning law (González, 2025), and respect the principle of legality, both in its democratic aspect, according to which the "structure of the Community legislative process must be perfected (Lorenzo, 2021) to overcome the traditional democratic deficit (Abel, 2002), and in its basic foundations of liberal criminal law, through directives without overlapping actions that "duly delimit the criminal sphere, without indeterminacy zones or elastic clauses, avoiding, in short, ambiguities and trying to achieve an obligatory degree of concretion" (Lorenzo, 2021; Vidales-Rodríguez, 2025). Only in this way could the task of national legislators be facilitated and harmonization be reconciled with the validity of the principle of legality.

Also it is essential in the construction of European criminal law to respect the principle of proportionality, punishing only suitable conduct that affects the vital interests for community coexistence, necessary or indispensable to protect the legal interest and proportional *stricto sensu* or without limitations of rights superior to those protected (Lorenzo, 2025).

Consequently, it should be criticized that Directive 2018/843, in addition to violating proportionality with invasive processing of personal information in prepaid cards with operations of 50 euros (Gómez, 2020), has forgotten both providers of virtual assets, crypto assets or tokens, which are not virtual currencies (Lorenzo, 2020), such as "virtual to virtual" (Gómez, 2021), exchanges, and that Directive 2018/1673, on criminal aspects (Abel, 2020), leans towards "solutions subject to abundant doctrinal criticism" (Lorenzo, 2020), such as the violation of the principle of proportionality punishing money laundering for many minor offenses (Vidales-Rodríguez, 2025), and the aggravation of money laundering in response to various previous crimes (Abel, 2025), even though it uses "optional transposition clauses" (Lorenzo, 2020), which can determine "that the internal regulations "allow themselves to be guided" and develop a criminal policy that is highly debatable or directly misguided".

Furthermore, despite the current existence of European anti-money laundering regulations, and the survival of the Union depends on their success, the crime of money laundering is not punished equally in the criminal codes of each European country, and the Community does not have European criminal law to protect its own interests. Although the Union increasingly directly applies rules, such as Regulation 1624/2024, which complains of fragmented approaches and inconsistent application.

CONCLUSION

The three regulations European Union 1620/2024, 1624/2024 and 1689/2024, and the Directive 1640/2024 represent a huge challenge for the application of international criminal law due to the emergence of AI, with a dizzying and frightening development, to which an infallible halo is given that does not correspond to reality, with an ambivalent effect, which makes life easier but creates new risks that must be addressed within the security-freedom framework, because although AI tools can revolutionize the fight against money laundering, it is necessary to maintain a balance between effectiveness and safeguarding fundamental rights through a "human-centered and trustworthy" AI. Furthermore, despite the current existence of European anti-money laundering regulations, and the survival of the Union depends on their success, the crime of money laundering is not punished equally in the criminal codes of each European country, and the Community does not have European criminal law to protect its own interests. Although the Union increasingly directly applies rules, such as Regulation 1624/2024, which complains of fragmented approaches and inconsistent application (whereas 2). The future in the application of international criminal law is uncertain and initiatives arose for the construction of a European criminal law in a broad sense that have not yet become positive law. If progress is to be made in the construction of European criminal law, it is essential to delimit precisely criminal law from administrative sanctioning law and respect the principle of legality and proportionality.

REFERENCES

Abel, M. (2002). El blanqueo de dinero en la normativa internacional: especial referencia a los aspectos penales. *Universidad de Santiago de Compostela*.

- Abel, M. (2020). Money laundering, criminal responsibility of legal persons and 2018 directives. *Journal of Applied Business & Economics*, 22(2020), 205–222.
- Abel, M. (2021). Algunas discordancias legislativas sobre la responsabilidad criminal de las personas jurídicas en el Código penal español. *Revista General de Derecho Penal*, 35, 1–62.
- Abel, M. (2024). Money laundering, artificial intelligence, criminal responsibility of legal persons and corporate crime. *Consilium Iuridicum*, 1. <https://doi.org/10.52097/ci.8989>
- Abel, M. (2025). Las reformas penales sobre el blanqueo de dinero introducidas en España por la Ley orgánica 6/2021. In Abel Souto, M./Lorenzo Salgado, J.M./Sánchez Stewart, N., *X congreso internacional sobre prevención y represión del blanqueo de dinero*.
- Ali, O., Murray, P. A., Al-Ahmad, A., Jeon, I., & Dwivedi, Y. K. (2025). Comprehending the theoretical knowledge and practice around AI-enabled innovations in the finance sector. *Journal of Innovation & Knowledge*, 10(5), 100762. <https://doi.org/10.1016/j.jik.2025.100762>
- Benavides, J. E. D., Navarro, J. A. L., & Hernández, A. P. G. (2026). Deepfakes in Onboarding, KYC, and Financial Fraud: Authenticity Standards and Liability Framework for Digital Banks and FinTech. *Journal of FinTech and Sustainable Finance*, 2, 1–9. <https://doi.org/10.31875/2755-8398.2026.02.01>
- Boukherouaa, E. B., Shabsigh, G., AlAjmi, K., Deodoro, J., Farias, A., Iskender, E. S., Mirestean, A. T., & Ravikumar, R. (2021). Powering the digital economy: Opportunities and risks of artificial intelligence in finance. *International Monetary Fund*.
- Caro-Coria, D. C. (2022). Compliance, neurociencias e inteligencia artificial. In Demetrio (E. (2022)). *Tirant lo Blanch*.
- Consejo-Europeo. (2023). Reglamento de inteligencia artificial: el Consejo y el Parlamento alcanzan un acuerdo sobre las primeras normas del mundo en materia de inteligencia artificial (p. 1). <http://www.consilium.europa.eu/es/press/press-releases/2023/12/09>
- Dante, D. C. (1870). Translated by Cayetano Rosell, illustrated by Gustavo Doré, Montaner y Simón editors (p. 13). *Montaner y Simón*.
- Demetrio, E. (2022). El Derecho penal ante el desafío neurotecnológico y algorítmico: reflexiones preliminares. In *Derecho penal y comportamiento humano. Avances desde la neurociencia y la inteligencia artificial* (pp. 17–33). Tirant lo Blanch.
- Domingos, I. M. (2024). Las nuevas tecnologías y el impacto del blanqueo de dinero procedente de la corrupción organizada en la democracia. In *IX Congreso sobre prevención y represión del blanqueo de dinero*. Tirant lo Blanch. <https://dialnet.unirioja.es/servlet/articulo?codigo=10125162>
- European Parliament and Council of the European Union. (2023). Regulation (EU) 2023/1114 of 31 May 2023 on markets in crypto-assets (MiCA) and amending Regulations (EU) No 1093/2010, (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937.
- European Parliament and Council of the European Union. (2024a). Directive (EU) 2024/1640 of the European Parliament and of the Council of 31 May 2024 on the mechanisms to be put in place by Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing. Official Journal of the European Union.
- European Parliament and Council of the European Union. (2024b). Regulation (EU) 2024/1620 of the European Parliament and of the Council of 31 May 2024 establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No. 1095/2010.
- European Parliament and Council of the European Union. (2024c). Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.
- European Parliament and Council of the European Union. (2024d). 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).
- FATF. (2010). Money laundering using new payment methods. *Financial Action Task Force*. <https://www.fatf-gafi.org/en/publications/MethodsandTrends/Moneylaunderingusingnewpaymentmethods.html>
- FATF. (2021). Opportunities and Challenges of New Technologies for AML/CFT. *The Financial Action Task Force*.

<https://www.fatf-gafi.org/publications/fatfrecommendations/documents/opportunities-challenges-new-technologies-aml-cft.html>

- Fernández, J. G. (2021). Evolución del Derecho penal económico europeo. In *Abel, M., Lorenzo, J. M. L., & Sánchez, N. (2021). VIII Congreso internacional sobre prevención y represión del blanqueo de dinero* (pp. 767–780). Tirant lo Blanch.
- Ferré, J. C. (2021). El Corpus Iuris de normas penales para la tutela de los intereses financieros de la Unión Europea. Desde el proyecto europeo hasta la actualidad. In *Abel, M., Lorenzo, J. M. L., & Sánchez, N. (2021). VIII Congreso internacional sobre prevención y represión del blanqueo de dinero* (pp. 781–804). Tirant lo Blanch.
- Ferré, J. C. (2024). Los hechos previos del blanqueo, con especial consideración en la ciberdelincuencia y los delitos antecedentes en la Directiva 2018/1673. In *Abel, M., Lorenzo, J. M. L., & Sánchez, N. (2024). IX Congreso sobre prevención y represión del blanqueo de dinero* (p. 253). Tirant lo Blanch.
- Foffani, L. (2021). Exigencias fundamentales para la construcción de un Derecho penal europeo. In *VIII congreso internacional sobre prevención y represión del blanqueo de dinero* (p. 806). Tirant lo Blanch.
- Gómez, D. J. (2020). El uso de las tarjetas de prepago para el blanqueo y la financiación terrorista y la directiva 843/2018. In *Abel, M., Lorenzo, J. M. L., & Sánchez, N. (2020). VII Congreso sobre prevención y represión del blanqueo de dinero* (pp. 295–330). Tirant lo Blanch.
- Gómez, D. J. (2021). El uso de las monedas virtuales y el dinero electrónico en el delito de blanqueo y la directiva 843/2018. In *Abel, M., Lorenzo, J. M. L., & Sánchez, N. (2021). VIII Congreso internacional sobre prevención y represión del blanqueo de dinero* (pp. 651–686). Tirant lo Blanch.
- González, J. L. (2025). De nuevo sobre la construcción de un Derecho penal económico europeo. In *Abel, M., Lorenzo, J. M. L., & Sánchez, N. (2025). X Congreso internacional sobre prevención y represión del blanqueo de dinero* (pp. 675–676). Tirant lo Blanch.
- Greco, N. (2020). A impossibilidade jurídica de juízes robôs. <http://www.institutoeduardocorreia.com.br/videos>
- Grynbaum, M. M., & Mac, R. (2023). The New York Times demanda a OpenAI y Microsoft por el uso de obras con derechos de autor en la IA. *The New York Times*.
- Jaume, L. (2023). Ha impulsado la pandemia la digitalización. In *M. Santalla Pulido (Ed.), Estamos preparados para el mundo que viene? La sociedad poscovid* (pp. 75–80). La Voz de Galicia.
- Joffre-Calasich, F. (2022). Cripto Criminalidad. Nft´S, Dex´S, Cross Chain Bridges, Nuevos Datos E Innovaciones En La Tecnología Blockchain De Uso Criminal. In *Ilícitos Económicos Y Evidencia Digital* (p. 190 and 195).
- Lorenzo, J. M. (2020). El blanqueo de dinero procedente de los delitos descritos en los artículos 368 a 372 del CP y las nuevas tendencias de financiación del terrorismo advertidas por las Directivas de 2018. In *Abel Souto, M./Lorenzo Salgado, J.M./Sánchez Stewart, N. (Coords.), VII congreso sobre prevención y represión del blanqueo de dinero*. Tirant lo Blanch.
- Lorenzo, J. . (2021). Consideraciones sobre el dogma legalista como principio básico en la construcción de un Derecho penal europeo. In *Abel Souto, M./Lorenzo Salgado, J.M./Sánchez Stewart, N., VIII congreso internacional sobre prevención y represión del blanqueo de dinero* (p. 813). Tirant lo Blanch.
- Lorenzo, J. M. (2025). Estructura del principio de proporcionalidad penal y su aplicación en la Unión Europea. In *Abel, M., Lorenzo, J. M. L., & Sánchez, N. (2025). X Congreso internacional sobre prevención y represión del blanqueo de dinero* (pp. 519–552). Tirant lo Blanch.
- Martínez, L. (2022). Ciencia o alquimia? Algoritmos y transparencia en la valoración del riesgo de reincidencia. In *Demetrio (E. (2022), pp. 489–506*). Tirant lo Blanch.
- Mata-Barranco, N. J. De La. (2020). Ilícitos vinculados al ámbito informático. In *Cuesta Arzamendi, J.L. De La (Dir.), Derecho penal informático, Civitas/Thomson Reuters/Aranzadi*. Cizur Menor.
- Miranda, A. (2020). A determinação da medida concreta da pena privativa de liberdade—entre a dogmática e a algoritmização. *Católica Talks—Responsabilidade*.
- Miranda, A. (2022a). Compliance inteligente e prevenção e luta contra o branqueamento. In *Miranda Rodrigues, A. (Coord.), A inteligência artificial no Direito penal, II* (pp. 212, 215 and 219–221).
- Miranda, A. (2022b). Inteligência Artificial no Direito Penal. In *Miranda Rodrigues, A. (Coord.), A inteligência artificial no Direito penal, II*.
- Miranda, A. (2022c). Inteligência artificial no Direito penal - a Justiça preditiva entre a americanização e a europeização. In *Miranda Rodrigues, A. (Coord.), A inteligência artificial no Direito penal, I*.
- Miranda, A. (2023). Compliance Cooperativo Inteligente na Prevenção e Luta contra o Branqueamento. *Revista Do*

- Ministério Público, 176, 9–40.
- Miranda, A. (2024a). Compliance criminal digital - a aliança ambígua entre a prevenção e a repressão da criminalidade empresarial. In *Miranda Rodrigues, A. (Coord.), A inteligência artificial no Direito penal, III* (p. 108).
- Miranda, A. (2024b). *Inteligência Artificial no Direito Penal-Vol. III*.
- Miranda, A., & Aires, S. (2022). Algoritmos em contexto empresarial: vantagens e desafios à luz do Direito penal. In *Miranda, A. (Coord.), A inteligência artificial no Direito penal, II* (pp. 11–39).
- Morón, I. (2024). La utilidad de las nuevas tecnologías en la prevención del blanqueo de dinero. In *Abel, M., Lorenzo, J. M. L., & Sánchez, N. (2024). IX Congreso sobre prevención y represión del blanqueo de dinero* (p. 604). Tirant lo Blanch.
- Muñoz, T. (2024). Blanqueo de dinero y mundo digital. In *Abel, M., Lorenzo, J. M. L., & Sánchez, N. (2024). IX Congreso sobre prevención y represión del blanqueo de dinero* (pp. 553–556). Tirant lo Blanch.
- Navarro, F. (2022). Blockchain, smart contract y compliance: anotaciones para el Derecho penal y procesal de la persona jurídica. In *Demetrio (E. (2022))*.
- Nunes, T. M. (2021). The legal impossibility of the robot referee. <https://www.migalhas.com.br/coluna/arbitragem-legal/356434/a-impossibilidade-juridica-do-arbitro-robo>
- Pavlidis, G. (2023). Deploying artificial intelligence for anti-money laundering and asset recovery: the dawn of a new era. *Journal of Money Laundering Control*, 26(7), 155–166. <https://doi.org/10.1108/JMLC-03-2023-0050>
- Pérez, S. (2024). Responsabilidad penal empresarial por uso de sistemas de inteligencia artificial. In *González, M.R., & Poelemans, M. (Coords.)*. Estudios sobre los efectos de la aplicación de la inteligencia artificial en el sistema jurídico. Bosch.
- Philipponnat, T. (2025). Artificial intelligence in finance: how to trust a black box? (R. Nosker (Ed.)).
- Salazar, J. C. (2024). Blanqueo de dinero y medios digitales. In *Abel, M., Lorenzo, J. M. L., & Sánchez, N. (2024). IX Congreso sobre prevención y represión del blanqueo de dinero* (p. 558). Tirant lo Blanch.
- The money laundering officer's practical handbook (pp. 37–39 and 54). (2011). Compliance training products limited.
- Trozze, A., Kamps, J., Akartuna, E. A., Hetzel, F. J., Kleinberg, B., Davies, T., & Johnson, S. D. (2022). Cryptocurrencies and future financial crime. *Crime Science*, 11(1), 1. <https://doi.org/10.1186/s40163-021-00163-8>
- Vidales-Rodríguez, C. (2025). Los principios de legalidad y proporcionalidad en la Directiva 2018/1673, del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativa a la lucha contra el blanqueo de capitales mediante el Derecho penal. In *Abel Souto, M./Lorenzo Salgado, J.M./Sánchez Stewart, N., X congreso internacional sobre prevención y represión del blanqueo de dinero*. Tirant lo Blanch.
- Wu, J., & Tran, N. K. (2018). Application of Blockchain Technology in Sustainable Energy Systems: An Overview. *Sustainability*, 10(9), 3067. <https://doi.org/10.3390/su10093067>