https://doi.org/10.55843/SG265128o

Su Generis,
5(1), June, 2026
e-ISSN: 2955-1900
visionjournal.edu.mk/suigeneris

International Vision University Press
© 2026
vision.edu.mk

Detection of Cybercrime Proceeds in Banking Money Transfers: A Comparative Analysis from the Perspective of Turkish, EU and U.S. Law

OĞURLU Cüneyt Şamil [1]

Abstract

This article examines the detection of cybercrime proceeds in banking money transfers from a comparative legal perspective, focusing on Turkish, European Union and United States law. It argues that cybercrime proceeds no longer move through simple linear banking channels but are increasingly routed through crypto-asset anonymisation services, OTC intermediaries, money mule networks and multi-layered transfer chains. In this context, traditional rule-based compliance systems are insufficient, making anomaly detection, risk scoring and machine-learning-based monitoring an expected institutional capacity for banks. The article first explains the structural link between cybercrime proceeds and banking transfers through ransomware, business email compromise and SWIFT manipulation cases. It then analyses the technical and legal status of statistical detection tools, including clustering, network analysis, ARIMA, Isolation Forest, Random Forest, XGBoost and LightGBM. The central legal question is whether algorithmic outputs should be treated as evidence, presumptions, risk indicators or mere grounds for initiating investigations. The article compares Turkish centralised administrative compliance, the EU's multilayered rights-sensitive regulatory model and the U.S. risk-based and innovation-oriented approach. It further evaluates the implications of algorithmic detection for legality, equality of arms, the right of defence, explainability, the presumption of innocence and property rights. The article concludes that the most defensible model is a hybrid framework combining Turkish institutional clarity, EU transparency and human oversight safeguards, and U.S. model risk management. Algorithmic detection should therefore be accountable, auditable, contestable, human-reviewed and compatible with cross-border cooperation within modern digital criminal procedure and financial regulatory governance systems today.

Keywords: Cybercrime Proceeds, Banking Money Tranfers, Turkish Law, EU Law, U.S. Law

Recieved: 19 May 2026
Accepted: 24 June 2026

2955-1900 © 2026 by Authors
Published by International Vision University Press
This is an open access article under the **CC BY** license

UDK:
[343.9:004.738.5]:34.05(560:4-6ЕУ:73)

[1] Dr., Istanbul Chamber of Commerce, Istanbul, Türkiye. cuneyt.ogurlu@ito.org.tr, 0009-0003-3708-755X

1. Introduction

The global expansion of digital banking infrastructures has fundamentally transformed not only the manner in which cybercrimes are committed, but also the ways in which proceeds derived from such crimes are integrated into the financial system. Cybercrime proceeds no longer move in a linear manner through a single account. Instead, crypto-assets obtained from ransomware attacks may be anonymised through mixer and tumbler services, converted into cash through OTC intermediaries, and then inserted into multi-layered chains of bank transfers.[1] Similarly, in business email compromise attacks, corporate wire-transfer instructions are directly manipulated; in phishing-based account takeover cases, funds are rapidly dispersed through money mule networks; and in investment fraud schemes, victims are induced through social engineering to make transfers voluntarily.[2]

This multidimensional attack surface demonstrates that banks' traditional rule-based filtering mechanisms are no longer sufficient on their own. Accordingly, anomaly detection has evolved from a static compliance activity based on fixed rules into a multidimensional, adaptive and continuously updated risk management architecture. This transformation has also shifted the centre of the legal debate concerning the monitoring of banking money transfers. Today, the main issue is not whether banks may use detection tools, but rather on what legal authority such tools are based, under which safeguards they operate, within what limits they are used, and according to what logic of oversight they are implemented.

---

[1] Chainalysis, *The 2024 Crypto Crime Report* (2024) 42–45 https://www.chainalysis.com/reports/2024-crypto-crime-report/ accessed 7 April 2026; Financial Action Task Force, *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* (2021) 28–30 https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets-2021.html accessed 7 April 2026; Europol, *Internet Organised Crime Threat Assessment (IOCTA)* (2023) 55 https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2023 accessed 7 April 2026.

[2] Federal Bureau of Investigation, *FBI Announces International Business Email Compromise Takedown* (11 June 2018) 1–3 https://www.fbi.gov/news/press-releases/fbi-announces-international-business-email-compromise-takedown accessed 7 April 2026; United States Department of Justice, *74 Arrested in Coordinated International Enforcement Operation Targeting Business Email Compromise Schemes* (11 June 2018) 1–4 https://www.justice.gov/opa/pr/74-arrested-coordinated-international-enforcement-operation-targeting-business-email accessed 7 April 2026; Europol, *Money Muling: European Money Mule Action Awareness Report* (2020) 5–8 https://www.europol.europa.eu/publications-events/main-reports/european-money-mule-action-emma-awareness-report accessed 7 April 2026; Financial Crimes Enforcement Network, *Alert on Prevalent Virtual Currency Investment Scam Commonly Known as "Pig Butchering"* (FIN-2023-Alert005, 8 September 2023) 1–8 https://www.fincen.gov/resources/advisories/fincen-alert-prevalent-virtual-currency-investment-scam-commonly-known accessed 7 April 2026.

2. The Structural Link Between Cybercrime Proceeds and Banking Transfers

The relationship between cybercrime proceeds and bank transfers is not incidental; rather, it is structural and cyclical. Proceeds obtained from cybercrimes often require the channels of the financial system in order to acquire economic value and become usable by offenders. Therefore, the laundering of criminal proceeds is not merely a secondary financial activity that takes place after the offence. It is one of the core stages that enables the continuity of the cybercrime economy.

This relationship can also be clearly observed through concrete cases. The ransom demand made by the REvil group in the 2021 Kaseya VSA attack, and the fact that numerous businesses were affected by this attack, demonstrate how ransomware proceeds become connected with crypto-assets and financial transfer channels[3]. The Bangladesh Bank case, in which USD 81 million was transferred through the manipulation of SWIFT messages, strikingly reveals the connection between cyberattacks, payment messaging systems and bank transfers[4]. In addition, the FBI IC3 2022 report, which recorded 21,832 complaints and USD 2.7 billion in losses relating solely to business email compromise attacks, quantitatively illustrates the impact of this type of crime on the financial system[5].

The common feature of these cases is that criminal proceeds ultimately come into contact with banking or payment system channels. Accordingly, statistical detection methods are not merely technical compliance tools. From the perspective of criminal procedure, they are critical instruments that enable an evidentiary connection to be established between the source of criminal proceeds and their final destination. In this respect, algorithmic detection systems perform both a preventive and an investigative function in the fight against financial crimes.

3. The Technical and Legal Nature of Statistical Detection Methods

The legal nature of statistical detection methods is one of the central conceptual issues in the monitoring of banking money transfers. Techniques such as cost-sensitive classification, inductive data aggregation, time-based pattern analysis and anomaly detection are increasingly used to identify fraud and money laundering

[3] Cybersecurity and Infrastructure Security Agency and Federal Bureau of Investigation, *Kaseya VSA Supply-Chain Ransomware Attack* (4 July 2021) 1–3 https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-187a accessed 7 April 2026; United States Department of Justice, *Ukrainian Arrested and Charged with Ransomware Attack on Kaseya* (8 November 2021) 1–2 https://www.justice.gov/opa/pr/ukrainian-arrested-and-charged-ransomware-attack-kaseya accessed 7 April 2026.

[4] Kaspersky Lab, *Lazarus under the Hood* (2017) 3–12 https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180227/Lazarus_Under_The_Hood_PDF_final.pdf accessed 7 April 2026; United States Department of Justice, *Criminal Complaint: United States of America v Park Jin Hyok* (No 18-MJ-1479, 8 June 2018) 1–179 https://www.justice.gov/opa/press-release/file/1092091/download accessed 7 April 2026.

[5] Federal Bureau of Investigation Internet Crime Complaint Center, *2022 Internet Crime Report* (March 2023) 12 https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf accessed 7 April 2026.

patterns[6]. In the detection of structuring, clustering analysis; in network analysis, betweenness centrality; in time-series anomaly detection, ARIMA and Isolation Forest; and in machine-learning-based classification, models such as Random Forest, XGBoost and LightGBM have become practically indispensable tools for identifying suspicious patterns in banking money transfers[7].

Nevertheless, the status of these algorithmic outputs under criminal law and criminal procedure has not yet been sufficiently clarified. Should an algorithmic alert be accepted as direct evidence? Or should it be regarded merely as a presumption, a risk indicator, or an initial suspicion meeting the threshold for opening an investigation? This distinction is not simply a matter of theoretical classification. The legitimacy of investigative measures, the applicability of protective measures and the scope of the right of defence depend directly on this legal characterisation.

For this reason, it must be clearly accepted that a statistical anomaly does not, by itself, constitute proof of a crime. However, under certain conditions, such an anomaly may constitute an indicator of reasonable suspicion requiring investigative authorities to act. Under Turkish criminal procedure, this assessment must be considered particularly in relation to the thresholds of suspicion required for the opening of an investigation and the preparation of an indictment[8]. Clarifying this conceptual distinction at the normative level is one of the priority needs of digital criminal procedure. As long as the legal status of algorithmic output remains uncertain, both the legitimacy of investigative actions based on such output and the accused's ability to develop an effective defence against it will remain contested.

4. Algorithmic Monitoring Regimes in Turkish, EU and U.S. Law

From a comparative perspective, a common tendency can be observed in Turkish, European Union and United States law: manual monitoring of large-volume money transfers is no longer practically sufficient. For this reason, anomaly detection, risk scoring and real-time alert mechanisms have become integral components of banking systems.

---

[6] Andrea Correa Bahnsen, Djamila Aouada, Aleksandar Stojanovic and Björn Ottersten, 'Feature Engineering Strategies for Credit Card Fraud Detection' (2016) 51 *Expert Systems with Applications* 134, 139–141 https://doi.org/10.1016/j.eswa.2015.12.030 accessed 7 April 2026.

[7] Anil K Jain, 'Data Clustering: 50 Years beyond K-means' (2010) 31(8) *Pattern Recognition Letters* 651; Linton C Freeman, 'Centrality in Social Networks: Conceptual Clarification' (1979) 1(3) *Social Networks* 215; George EP Box and Gwilym M Jenkins, *Time Series Analysis: Forecasting and Control* (5th edn, Wiley 2015) 47–80; Fei Tony Liu, Kai Ming Ting and Zhi-Hua Zhou, 'Isolation Forest' in *Eighth IEEE International Conference on Data Mining* (IEEE 2008) 413; Leo Breiman, 'Random Forests' (2001) 45(1) *Machine Learning* 5; Tianqi Chen and Carlos Guestrin, 'XGBoost: A Scalable Tree Boosting System' in *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining* (ACM 2016) 785; Guolin Ke and others, 'LightGBM: A Highly Efficient Gradient Boosting Decision Tree' (2017) 30 *Advances in Neural Information Processing Systems* 3146.

[8] CMK Article 160; CMK article 170; Nur Centel and Hamide Zafer, *Criminal Procedure Law* (Beta Publications 2023) 278–285.

In Turkish law, this process has been institutionalised through the suspicious transaction reporting obligation under Law No 5549 on the Prevention of Laundering Proceeds of Crime and MASAK regulations (*Financial Crimes Investigation Board (MASAK)*); the information systems security obligation under Banking Law No 5411; and the obligation of banks to manage operational and information technology risks under BDDK (Banking Regulation and Supervision Agency-BRSA) regulations[9]. In particular, the expectation that obliged entities conduct the necessary inquiries within the scope of their authority and capacity and continuously monitor transaction patterns in the detection of suspicious transactions is no longer an obligation that large-scale banks can fulfil solely through human labour. In practice, this situation directs banks to establish data analytics, behavioural profiling and automated alert systems.

In European Union law, PSD2 and the Technical Regulatory Standards numbered 2018/389 place transaction monitoring mechanisms on a normative basis within the framework of payment security and strong customer authentication. In addition, the AMLR and AMLA regulations adopted under the 2024 AML Package aim to strengthen institutional coordination in the monitoring of cross-border financial crimes[10]. In U.S. law, the Suspicious Activity Report obligation under the Bank Secrecy Act and the AMLA 2020 reform position the use of machine learning and advanced data analytics as a natural component of banking compliance systems[11].

However, significant structural differences exist among these three legal systems. The Turkish legal system establishes a more centralised and administration-oriented compliance regime. EU law, by contrast, continues to develop a more multilayered architecture that addresses security obligations together with data protection and fundamental rights safeguards. U.S. law adopts a risk-based and flexible structure that is more open to technological innovation, although it does not provide as comprehensive a data protection framework as the EU.

---

[9] Law on the Prevention of Laundering Proceeds of Crime, Law No. 5549, Official Gazette, No. 26323 (2006) art. 4; Financial Crimes Investigation Board, *MASAK General Communiqué on the Implementation of the Regulation on Measures Regarding the Prevention of Laundering Proceeds of Crime and Financing of Terrorism* (Sequence No 13, Official Gazette, No. 28925, 2014); Banking Law, Law No. 5411, Official Gazette, No. 25983 (2005) art. 68; Banking Regulation and Supervision Agency, *Regulation on Banks' Information Systems and Electronic Banking Services* (Official Gazette, No. 31069, 2020).

[10] 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 [2024] OJ L 2024/1624; 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 [2024] OJ L 2024/1620.

[11] Bank Secrecy Act, 31 U.S.C. §§ 5311–5332; Financial Crimes Enforcement Network, *Bank Secrecy Act/Anti-Money Laundering Examination Manual* (2024) https://bsaaml.ffiec.gov/manual accessed 7 April 2026; Anti-Money Laundering Act of 2020, Pub L No 116-283, 134 Stat 3388, §§ 6207–6209 (2021).

This difference is also reflected in the determination of the evidentiary value of algorithmic outputs. In the United States, the Daubert standard evaluates the admissibility of scientific evidence through criteria such as testability, peer review, error rate and general acceptance.[12] In Turkish law, by contrast, the judge's authority to freely evaluate evidence is broader, and there is no explicit and specific regulation concerning the evidentiary status of algorithmic outputs.[13][13] This uncertainty makes the systematic integration of algorithmic detection into criminal adjudication more difficult and creates an area that may lead to inconsistencies among courts in practice.

The EU acquis, on the other hand, treats the inclusion of algorithmic systems in judicial processes not merely as a matter of technical efficiency, but as a fundamental rights safeguard shaped around the principles of transparency, explainability and human oversight. In this respect, EU law seeks to construct a third path between the more flexible and market-oriented approach in the United States and the traditional free evaluation of evidence in Turkish law. This third path is based on an effort to standardise the evidentiary value of algorithmic detections at the intersection of technical reliability, data protection and fundamental rights safeguards.

5. Fundamental Rights, the Right of Defence and the Problem of Explainability

The integration of algorithmic detection methods into criminal procedure creates various tensions from the perspective of the rule of law. With respect to the principle of legality in crime and punishment, the use of algorithmic outputs to substantiate suspicion of crime requires the legal status of such outputs to be clearly determined. From the perspective of the right of defence and the principle of equality of arms, the black-box nature of an algorithm used against the accused, and the inability of the defence to examine its internal logic, may create serious problems in terms of the right to a fair trial[14].

A significant portion of algorithmic models learn non-linear relationships in high-dimensional feature spaces, and therefore their decision boundaries may become impossible for humans to interpret directly. This structurally limits the defence's capacity to effectively challenge the output used against the accused.[15] In addition, from the perspective of the presumption of innocence, basing precautionary measures such as

[12] *Daubert v Merrell Dow Pharmaceuticals Inc* 509 US 579, 593–594 (1993).
[13] CMK article 217; Bahri Öztürk and others, *Digital Criminal Procedure Law* (3rd edn, Seçkin Publishing 2024) 420–422; Centel and Zafer (n 8) 628–640.
[14] Bahri Öztürk and others, *Criminal Procedure Law: Theoretical and Applied* (18th edn, Seçkin Publishing 2024) 249–264; Stefan Trechsel, *Human Rights in Criminal Proceedings* (Oxford University Press 2005) 82–120.
[15] Alejandro B Arrieta and others, 'Explainable Artificial Intelligence (XAI): Concepts, Taxonomies, Opportunities and Challenges toward Responsible AI' (2020) 58 *Information Fusion* 82, 82–115.

account freezing solely on algorithmic output may result in a de facto shift in the burden of proof. Such a practice also carries the risk of disproportionate interference with the right to property.

This risk becomes concrete at the technical level through the precision-recall balance and the false positive rate. A high false positive rate may mean the unjustified restriction of the financial rights of innocent customers.[16] Therefore, the legality of algorithmic detection systems should not be reduced merely to their accuracy rate. For a legally defensible model, accuracy, explainability, recordability, review through human intervention and effective avenues of objection must be assessed together.

The EU Artificial Intelligence Act introduces transparency and human oversight obligations for high-risk artificial intelligence systems.[17] However, the fact that systems used for financial fraud detection are not always classified as high-risk does not mean that this area is entirely unregulated. On the contrary, such systems are considered within a broader accountability regime surrounded by PSD2, GDPR, DORA and AML/CFT regulations. In Turkish law, the right to object to decisions producing adverse consequences for an individual solely through automated systems under the KVKK (Law on the Protection of Personal Data-LPPD) constitutes an important starting point. Nevertheless, how this right will operate in the context of banking and the prevention of financial crimes has not yet been sufficiently concretised.

6. Algorithmic Outputs from the Perspective of Digital Criminal Procedure

The digitalisation of criminal procedure does not merely mean transferring existing processes into an electronic environment. This transformation requires reconsideration of the paradigm of evidence evaluation, the right of defence and the architecture of criminal procedure. The involvement of algorithmic outputs alongside traditional types of evidence such as statements, documents and inspection expands the conceptual boundaries of evidence law.

In this context, the legal status of the concept of "machine-generated suspicion" is of particular importance. Whether signals produced by banks' algorithmic filtering systems may be accepted as the basis for orders to seize computer data or as grounds for initiating an investigation is one of the central issues of digital criminal procedure.[18] The critical question here is whether algorithmic output alone can legitimise a protective measure. A more appropriate approach is to consider algorithmic output not on its own, but together with the assessment of a human decision-maker and independent supporting evidence. This

[16] Jesse Davis and Mark Goadrich, 'The Relationship between Precision-Recall and ROC Curves' in *Proceedings of the 23rd International Conference on Machine Learning* (ACM 2006) 233; Andrea Dal Pozzolo and others, 'Learned Lessons in Credit Card Fraud Detection from a Practitioner Perspective' (2014) 41(10) *Expert Systems with Applications* 4915.
[17] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence [2024] OJ L 2024/1689, arts 13–14.
[18] Öztürk and others, *Digital Criminal Procedure Law* (n 13) 561 ff.

approach is better suited to protecting both the need for effective investigation and fundamental rights safeguards.

7. International Cooperation and Cross-Border Access to Evidence

Combating cybercrimes involving banking money transfers is not an issue that can be resolved solely through national legislation. Since funds can be transferred to different countries within minutes, suspicions detected through algorithmic monitoring must be supported by rapid preservation of evidence, access to account information, freezing of assets and information sharing among financial intelligence units.

At this point, the expedited preservation and production order mechanisms of the Budapest Convention, as well as the direct cooperation with service providers and emergency tools provided under the Second Additional Protocol, are of particular importance.[19] FATF recommendations, in turn, form the basis of global AML/CFT standardisation with respect to the risk-based approach, the obligations of virtual asset service providers, suspicious transaction reporting and sanctions regimes.[20] In addition, the FinCEN 314(b) information sharing programme, the U.S. CLOUD Act and the EU e-Evidence Regulation provide complementary mechanisms for cross-border access to electronic evidence and the fight against financial crimes.[20]

Furthermore, the UN Cybercrime Convention adopted on 24 December 2024 offers a new multilateral framework with the potential to expand international cooperation mechanisms. In this framework, algorithmic detection should not be regarded as a closed security technology that produces results on its own. Rather, it can acquire real deterrent capacity when it operates together with effective judicial cooperation, rapid data preservation, cross-border access to evidence and financial intelligence sharing.

8. Comparative Assessment and Model Proposal

The strength of Turkish law in this field lies in institutional clarity and administrative centralisation. The relatively clear distribution of functions among MASAK, BDDK and the TCMB (Central Bank of the Republic of Türkiye-CBRT) may provide speed and uniformity in the implementation of obligations. However, the same centralised structure also requires the development of stronger procedural safeguards, explanation obligations and objection mechanisms against the effects of algorithmic decisions on individuals.

---

[19] Council of Europe, *Convention on Cybercrime* (European Treaty Series No 185, 23 November 2001); Council of Europe, *Explanatory Report to the Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence* (2022) paras 1–25.

[20] Financial Action Task Force, *International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation: The FATF Recommendations* (2023) 10–25.

The strength of EU law is its attempt to balance payment security, AML/CFT, data protection, digital operational resilience and cross-border access to evidence within the same regulatory ecosystem. Its weakness is that the combined application of these regulations creates a complex and costly compliance burden for banks. The strength of U.S. law is its innovation-friendly and operationally pragmatic understanding of risk management. By contrast, the fragmented nature of its rights-based general data protection perspective and the reliance of safeguards mostly on sectoral rules and supervisory guidance constitute important limitations.[21]

For this reason, the Turkish, EU and U.S. models represent three different logics of legitimacy: Türkiye proceeds through administrative obligation and centralised oversight; the EU through balancing multilayered regulation; and the United States through innovative risk management. In our view, the more appropriate model should be a hybrid framework combining the strengths of these three approaches. In such a model, the institutional clarity of Turkish law, the transparency and human intervention safeguards of EU law, and the model risk management and technological innovation capacity of U.S. law should be evaluated together.

9. Future Trends and Normative Needs

In the short term, with the full implementation of the EU's 2024 AML Package, the inclusion of virtual asset transfers under a supervisory regime similar to that applicable to bank transfers will accelerate the transformation of statistical detection methods into de facto normative obligations. In the medium term, the integration of explainable artificial intelligence standards into the law of evidence in criminal procedure appears inevitable. These standards must cover not only the technical performance of the model, but also the legal justifiability of the algorithmic decision.[22]

In the long term, the widespread adoption of central bank digital currencies may fundamentally change the way criminal proceeds transfers are monitored.[23] In systems where every transaction is recorded on a central

[21] Financial Crimes Enforcement Network, *Section 314(b) Fact Sheet* (2020) 1–4 https://www.fincen.gov/sites/default/files/shared/314b-Fact-Sheet.pdf accessed 7 April 2026; Clarifying Lawful Overseas Use of Data Act, Pub L No 115-141, 132 Stat 1213 (2018); Jennifer Daskal, 'Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0' (2018) 71 *Stanford Law Review Online* 9; Regulation (EU) 2023/1543 of the European Parliament and of the Council of 27 June 2023 on European Production Orders and European Preservation Orders for Electronic Evidence in Criminal Proceedings and for the Execution of Custodial Sentences Following Criminal Proceedings [2023] OJ L191/118.

[22] Arrieta and others (n 15) 82–115; Regulation (EU) 2024/1689 (n 17) arts 13–14.

[23] Bank for International Settlements, *Central Bank Digital Currencies: Foundational Principles and Core Features* (2020) 1–8 https://www.bis.org/publ/othp33.pdf accessed 7 April 2026; Central Bank of the Republic of Turkey, *Digital Turkish Lira First Phase Evaluation Report* (2023).

infrastructure, the function of statistical detection may change; however, the tension between surveillance and fundamental rights may deepen further. For Türkiye, the priority need is not merely the formal implementation of the Budapest Convention, but the effective operation of that Convention and, in particular, the Second Additional Protocol; the strengthening of explicit provisions on the digital evidence regime in the CMK (Turkish Criminal Procedure Code-TCPC); and the development of MASAK's analytical capacity together with fundamental rights safeguards.

10. Conclusion

The monitoring of bank transfers arising from cybercrime proceeds is no longer a secondary technical option, but has become part of the institutional capacity legally expected from financial institutions. Nevertheless, Turkish, EU and U.S. laws structure this capacity according to different logics of legitimacy. Turkish law proceeds through centralised compliance and administrative oversight; EU law through its multilayered balance between security and fundamental rights; and U.S. law through risk-based programmes, supervisory guidance and the encouragement of innovation.

This study argues that the most appropriate model is a hybrid structure that brings together the strengths of these three approaches. Such a structure should combine the institutional clarity of Turkish law, the transparency and human oversight safeguards of EU law, and the model risk management and technological innovation capacity of U.S. law within the same framework. Otherwise, two extreme risks may arise: either a formal compliance regime that remains ineffective in combating cybercrimes, or a disproportionate financial surveillance order that erodes fundamental rights in the name of security.

From the perspective of modern criminal law and banking law, the main objective should not be to expand algorithmic detection without limits. Rather, the main objective should be to place such detection within a legal architecture that is accountable, auditable, contestable, open to human intervention and suitable for cross-border cooperation.

References

Anti-Money Laundering Act of 2020. (2021). *134*, 116-283.

Arrieta AB and others, 'Explainable Artificial Intelligence (XAI): Concepts, Taxonomies, Opportunities and Challenges toward Responsible AI' (2020) 58 *Information Fusion* 82.

Box GEP and Jenkins GM, Time Series Analysis: Forecasting and Control . (2015). Wiley.

(2021). *c.* United States Department of Justice.

Chainalysis. (2024). The 2024 Crypto Crime Report.

Clarifying Lawful Overseas Use of Data Act. (2018). (132), 115-141.

Correa Bahnsen A, A. D. (2016). Feature Engineering Strategies for Credit Card Fraud Detection. (51), 134.

Council of Europe. (2001, November 23). Convention on Cybercrime. *(European Treaty Series*, 185.

Council of Europe. (2022). Explanatory Report to the Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence.

(2018). *Criminal Complaint: United States of America v Park Jin Hyok No 18-MJ-1479.* United States Department of Justice.

Cybersecurity and Infrastructure Security Agency and Federal Bureau of Investigation. (2021, July 4). *Kaseya VSA Supply-Chain Ransomware Attack.*

Daubert v Merrell Dow Pharmaceuticals Inc 509 US 579. (1993).

Dal Pozzolo A and others, 'Learned Lessons in Credit Card Fraud Detection from a Practitioner Perspective' (2014) 41(10) *Expert Systems with Applications* 4915.

Türkiye Cumhuriyet Merkez Bankası, *Dijital Türk Lirası Birinci Faz Değerlendirme Raporu* (2023).

Europol. (2020). Retrieved from Money Muling: European Money Mule Action Awareness Report.

Europol. (2023). Retrieved from Internet Organised Crime Threat Assessment (IOCTA).

Gazette, O. (2005). Retrieved from Bankacılık Kanunu,Kanun No 5411.

Gazette, O. (2020). Retrieved from Bankacılık Düzenleme ve Denetleme Kurumu, Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik.

H, C. N. (2023). Ceza Muhakemesi Hukuku . *Beta Yayınları*.

J, D. (2018). Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0. *Stanford Law Review Online 9*, 71.

Kaspersky Lab. (2017). Lazarus under the Hood .

Liu FT, T. K. (2008). Isolation Forest' in Eighth IEEE International Conference on Data Mining. (p. 413). IEEE.

M, D. J. (2006). The Relationship between Precision-Recall and ROC Curves' in Proceedings of the 23rd International Conference on Machine Learning . *ACM* , 233.

Mali Suçları Araştırma Kurulu. (2014). *Suç Gelirlerinin Aklanmasının ve Terörün Finansmanının Önlenmesine Dair Tedbirler Hakkında Yönetmelik Uygulanmasına İlişkin MASAK Genel Tebliği Sıra No 13.* Retrieved from Official Gazette.

Network, F. C. (2020). Retrieved from Section 314(b) .

Network, F. C. (2024). Retrieved from Bank Secrecy Act/Anti-Money Laundering Examination Manual .

Network, F. C. (223, September 8). Retrieved from Alert on Prevalent Virtual Currency Investment Scam Commonly Known as "Pig Butchering.

Ke G and others, 'LightGBM: A Highly Efficient Gradient Boosting Decision Tree' (2017) 30 *Advances in Neural Information Processing Systems* 3146.

Öztürk B and others, *Ceza Muhakemesi Hukuku: Nazari ve Uygulamalı* (18th edn, Seçkin Yayıncılık 2024).

Öztürk B and others, *Dijital Ceza Muhakemesi Hukuku* (3rd edn, Seçkin Yayıncılık 2024).

(2006). *Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanun, Kanun No 5549.* Official Gazette.