The Impact and Role of Information Technology in Money Laundering

1. Fardin Pormayeh: Department of Criminal Law and Criminology, Cha.C., Islamic Azad University, Chalus, Iran
2. Ali Mansour Lakurj*: Department of Criminal Law and Criminology, Cha.C., Islamic Azad University, Chalus, Iran

*Correspondence: ali1358@iau.ac.ir

Abstract

Today, the remarkable transformation in the global monetary and banking system, resulting from the information and communication technology (ICT) revolution, has had profound effects on the social and economic lives of individuals. At the same time, it has posed new challenges to the current anti-money laundering regulations. Access to electronic banking and internet networks has created a suitable safe haven for money laundering activities. In contemporary times, the discourse on organized crimes—both national and transnational—has entered a new phase, where efforts are increasingly directed at preventing the emergence of criminal organizations and confronting them decisively through various means. Autonomous approaches, namely preventing the entry of illicit revenues into national and international financial systems, have long been on the agenda of national and international policymakers. Unfortunately, this has led to the emergence of a new criminal trend known as money laundering, compelling responsible authorities to address it proactively. However, the radical transformation of the global monetary and banking system, brought about by the advent of electronic money and banking, has challenged the existing anti-money laundering regulations, making comprehensive revisions of such measures necessary. This research seeks to answer the question: What impact does electronic banking have on the money laundering process? Based on the hypothesis that electronic banking facilitates the commission of money laundering offenses and introduces new methods for committing such crimes, the study examines e-commerce and banking, along with the characteristics of each. It proposes techniques for electronic money laundering, explores both common and novel methods, and compares traditional money laundering processes with modern ones. In this context, the recommendations of the Financial Action Task Force (FATF) regarding the fight against electronic money laundering are also presented. The conclusion drawn is that information and communication technology, when provided in an insecure environment, can expand and develop money laundering, as well as facilitate and diversify its methods. Therefore, this issue must be taken into serious consideration in the formulation of economic, financial, and criminal policies.

Keywords: Electronic banking, E-commerce, Money laundering, Electronic money laundering, Information and communication technology.

Received: 15 August 2024
Revised: 19 September 2024
Accepted: 20 October 2024
Published: 27 October 2024

Citation: Pormayeh, F., & Mansour Lakurj, A. (2024). The Impact and Role of Information Technology in Money Laundering. *Legal Studies in Digital Age*, 3(4), 184-194.

1. Introduction

Information and communication technology (ICT) represents a clear and dramatic transformation of the second millennium CE, having profound impacts across all social and economic domains and rapidly transforming the world into an information society. The rapid proliferation of communication and information tools has brought with it countless positive and negative effects. One of the positive effects of this technology is the creation of an appropriate platform for conducting commercial and economic exchanges. This emerging phenomenon, formed within the framework of ICT, is referred to as *electronic commerce*, which, when implemented in a secure and suitable environment, can be even more effective than traditional commerce. E-commerce refers to all forms of commercial transactions conducted through online digital storefronts.

Among these transformations, the *banking industry*, utilizing ICT, has undergone substantial changes, including increased speed, accuracy, ease of use, and enhanced security in financial and commercial exchanges. This has resulted in a wide range of electronic services becoming available to banking customers. These services include electronic and internet payments, banking via landline and mobile phones, point-of-sale terminals, ATMs, and more. Nevertheless, despite its extensive capabilities and complexities, ICT remains highly vulnerable to threats. This is because ICT, in addition to facilitating the commission of traditional crimes, offers new and sophisticated opportunities for criminals in the *cyberspace*, resulting in the emergence of a new category of offenses known as *cybercrimes*.

Access to the internet and online networks, by creating a secure environment for offenders, facilitates the commission of certain crimes in virtual environments, such as *money laundering*. Money laundering is the process of concealing the origin and source of criminal proceeds and assets in a way that renders tracing the origin of the funds either impossible or extremely difficult. In other words, money laundering involves an attempt by an offender to obscure the true origin of revenues obtained from illicit activity. If the offender succeeds, the money loses its illicit identity and appears legitimate.

The first stage in the money laundering process is referred to as *placement*, which involves introducing illicit funds into the financial system with the aim of integrating them into legitimate channels. This can be accomplished through cash deposits into formal or informal financial institutions and the purchase of valuable goods. The second stage, known as *layering*, involves converting the proceeds of crime into different forms to obscure or disguise their source and ownership. This is typically achieved through actions such as fund transfers, real estate purchases, and transferring assets abroad. The final stage of the money laundering process is called *integration*, where the laundered money is reintroduced into the national financial system by the end-user, with the intention of preventing official bodies from investigating its origin.

E-commerce and banking can only serve as suitable platforms for money laundering when presented in an insecure and unregulated manner. Thus, the central concern of the present study—that e-commerce and electronic banking provide a platform for money laundering—is strictly limited to insecure digital commerce and banking environments.

2. Concepts

This section explores the core concepts discussed in the article.

2.1. The Concept of Money Laundering

According to the Criminal Police Organization, money laundering is defined as any act or attempted act intended to conceal or alter the appearance and identity of illicit proceeds in such a way that they appear to originate from lawful sources (Saki, 2008). Rowan Bosworth and Graham Saltmarsh, authors of the book *Money Laundering*, define it as: "Money laundering is the process of concealing the proceeds of crime using deceptive tools to disguise the origin of illicit funds" (Bosworth-Davis, 1994).

The *Directive of the European Community*, adopted in March 1990, defines money laundering as follows:

"The conversion or transfer of property, knowing that such property is derived from criminal activity, for the purpose of concealing or disguising the illegal origin of the property or assisting any person involved in the commission of such an offense to evade the legal consequences of their action" (Bidabad, 2013).

The definition was expanded by the *Council of Europe Convention*, held in Strasbourg in August 1990, to include:

"The acquisition, possession, or use of property derived from criminal sources, and any involvement, management, conspiracy to commit, facilitate, or attempt to commit money laundering" (Bagherzadeh, 2009).

According to the Central Bank's anti-money laundering regulations, money laundering includes:

1. Acquisition, retention, or use of funds directly or indirectly obtained through the commission of a crime.
2. Assisting another person or persons in converting or transferring such funds.

Money laundering is a type of financial transaction in which the nature, source, or destination of the funds is concealed or obscured. In fact, it is considered one of the most prominent mechanisms of the underground economy. In the past, the concept of money laundering applied only to financial transactions connected to *organized crimes* such as drug trafficking or mafia operations. Today, however, the term "money laundering" has a broader application, encompassing all financial transactions involving assets derived from illegal activities such as tax evasion or fraudulent auditing. With the growing complexity of financial crimes, the need for intelligent solutions to combat financial crime and terrorism has become more critical than ever.

2.2. Characteristics of the Crime of Money Laundering

Money laundering is a complex, continuous, long-term, and group-based process that is typically carried out on a large scale. It often crosses geopolitical borders, turning "dirty money" derived from criminal activity into legitimate and legal assets, thereby making it difficult to trace its criminal origin. Since financial gain is the principal motive for criminal behavior, preventing the acquisition of illicit revenue is essential to purifying the economy and encouraging lawful income generation. Notable characteristics of money laundering include:

1. **Money laundering is a secondary crime.** To commit this crime, another offense such as drug trafficking, kidnapping, or organ trade must precede it. Its secondary nature has led to lower public sensitivity to it (Asadi, 2007).
2. **Money laundering is an organized crime.** Its structured nature introduces additional challenges to the prosecution of offenders. While a lone thief or murderer may be apprehended by law enforcement, money laundering involves organized entities, including various operational levels from petty drug dealers to skilled intermediaries and educated professionals. As a result, arresting one individual does not halt the operation, complicating law enforcement efforts (Asadi, 2007).
3. **Money laundering is a transnational crime.** It is not restricted to a specific geographical area or within the borders of a single country. The organized structure of this crime enables it to cross borders, reinforcing the concept of a "global village" for its perpetrators. This underscores the importance of international cooperation and the role of international organizations in coordinating efforts to combat it.
4. **Money laundering is a white-collar crime.** Criminal organizations employ experts such as accountants, lawyers, and bank staff to carry out the final stages of money laundering. The crime leverages reputable institutions like banks, legal firms, and auditing agencies to give a lawful appearance to illicit proceeds.
5. **It constitutes a new legal category.** Money laundering does not fall under any prior criminal classification. It represents a distinct legal offense that necessitates a new legal framework for prosecution.
6. **It excludes petty offenses.** Some may assume that small-scale crimes like selling stolen goods fall under money laundering. However, the concept is much broader and does not include such activities. The organizational nature of money laundering further distinguishes it from minor crimes.
7. **It is a continuous offense.** Unlike simple crimes, money laundering is an ongoing and sustained process that unfolds over time. Without following the full cycle, the offense cannot be legally characterized as money laundering (Mir Mohammad Sadeghi, 1998).
8. **It has multidimensional aspects.** In addition to its legal dimension, money laundering also encompasses economic, political, and ethical implications.

3. Electronic Money Laundering

Money laundering is one of the most significant forms of organized financial crime within the domain of electronic commerce. It is facilitated by modern technologies and developments in telecommunications systems, under the cover of

electronic banking, which is a key manifestation of e-commerce. This occurs because the liquidity obtained from criminal activity is always at risk of being confiscated if the criminal operation is successfully prosecuted and subject to legal penalties. Achieving immunity from such consequences requires laundering these proceeds and concealing their illicit origin. In other words, criminals have no choice but to integrate their illicit revenues into the legitimate economy and hide their unlawful origins.

One of the primary methods of laundering such proceeds is through the use of computer information networks and information technology, conducting money laundering operations under the guise of electronic commerce. This is a highly significant and noteworthy issue that, unfortunately, has not been addressed in the Electronic Commerce Law. It is imperative that this new phenomenon be recognized and that effective strategies for its prevention be developed. This section explores the stages and methods of electronic money laundering and compares them with traditional money laundering.

3.1. Stages of Electronic Money Laundering

With the expansion of internet usage in 1996 and the rapid growth of electronic finance, money launderers and terrorist groups gained the capability to launder money in the digital sphere. This type of laundering is only possible through the use of information and communication technology and its operation across computer, telecommunications, satellite, and other information networks. This dependency on digital infrastructure is considered the most essential characteristic of this crime. Today, computers and the internet have eliminated the need for paper documentation, which was previously a method for tracing the origin of illicit proceeds and apprehending offenders. Using computer networks, money can now be transferred across borders in a fraction of a second.

Electronic funds transfer, also known as wire transfer, allows organized criminals to exploit electronic banking to move dirty money and criminal proceeds into various accounts, just like money from legitimate business activities, without any substantial risk. In essence, ICT has created a virtual free-trade financial zone that can operate without legal requirements and financial auditing. This free flow of capital is a technological achievement enabling the circulation of funds in the global market—both legally and illegally (Rahbar & Fazlollah, 2008).

In electronic money laundering, various factors—such as the lack of physical presence of account holders at banks, the invisibility of large financial transactions, and most importantly, the thousands-fold speed of money movement compared to the traditional banking system—render detection exceedingly difficult. Consequently, the possibility of uncovering the crime and initiating criminal prosecution is drastically reduced. Furthermore, due to the ease and speed of fund transfers between accounts and banks, tracking money becomes highly technical and challenging. Offenders, by bypassing banking network security measures, hacking into bank vaults, or stealing from customer accounts using acquired usernames and passwords, can carry out micro-transactions using criminal methods. They often transfer units below the legal threshold for transaction reporting within a given timeframe as defined by anti-money laundering laws. These small amounts are deposited into intermediary accounts and eventually into final destination accounts. In this method, by expanding the crime scene and involving numerous intermediary bank accounts, the offender minimizes the traceability of fund transfers and obscures the true recipient of the money.

In summary, electronic money laundering is the process of legitimizing illicit income derived from criminal activities using virtual space services, which are utilized to legalize the funds and use them as tools for transferring illegal proceeds.

The stages of electronic money laundering are as follows:

3.1.1. Electronic Placement

As previously stated, the first step in money laundering is the physical disposal of cash. Traditionally, this involves depositing the funds into a bank or financial institution or smuggling the cash abroad for deposit into foreign accounts, or using it to purchase high-value goods such as artwork, aircraft, precious metals, and gemstones, which can later be sold. However, electronic money laundering allows the launderer to use digital anonymity or the anonymity of e-money to transfer illicit proceeds through smart cards and e-currency, completing the placement phase without physical interaction.

These funds may be used to purchase foreign currency or high-value items for resale, thereby replacing dirty money with electronic money. With such conveniences, the money launderer no longer needs to smuggle cash or engage in face-to-face

transactions. They can easily transfer criminal revenues, obtained in digital form, across borders or use them to purchase luxury goods and foreign currencies. The primary advantage of this electronic method over traditional methods is the elimination of face-to-face transactions and the concealment of identity. In this method, it is impossible to verify whether the identity provided is accurate, and therefore, the electronic execution of this stage poses less risk than traditional methods. Some experts even believe that in electronic money laundering, this stage may be bypassed altogether (Jalali Farahani, 2005).

3.1.2. Electronic Layering

This stage requires complex layers of financial transactions to create distance between the illicit proceeds and their source and to mislead investigators. Traditionally, layering involves converting savings into monetary instruments and investing in real estate or legitimate businesses, particularly in the entertainment, tourism, or joint venture sectors—often registered abroad. For the money launderer, however, speed, distance from the source, and anonymity are always critical. All these features can be achieved through continuous financial services. In this phase, the offender attempts to separate the money from its original source. This can be done by transferring funds through multiple bank accounts for the appearance of legitimate goods purchases and resale, or through offshore companies located in diverse legal jurisdictions.

If individuals are allowed to open online accounts without submitting authentic identity documents, this stage becomes even easier (Habibzadeh, 2011).

3.1.3. Electronic Integration

The final step in money laundering is to make large sums of illegally obtained money appear legitimate. Traditionally, this could be done through various methods, including investing in offshore financial institutions to issue legitimate loans, using shell companies, creating or forging invoices for goods sold abroad, or fabricating sales receipts.

Clearly, these mechanisms entail high risks. However, in electronic money laundering, a simple method is for the offender to open a bank account under a shell company that ostensibly provides services such as internet service provision. The launderer is not even required to deliver actual services. Instead, the company serves as a cover to make it appear that the funds—having already undergone a second layering stage—are in exchange for legitimate services, even though their origin is criminal (Habibzadeh, 2011).

3.2. Methods of Electronic Money Laundering

Money laundering via electronic banking can be executed in two primary ways: directly and indirectly. In the direct method, the launderer engages with a financial institution directly by presenting an identity while concealing their true intent and purpose.

The direct method refers to the use of digital signature technology and internet-based interaction with financial institutions, allowing the launderer to open accounts without physical presence. By using forged identities and even falsified digital signatures, the launderer can carry out money laundering operations without attracting attention. This approach may involve concealment within corporate structures, misuse of legitimate businesses, employment of falsified documents and identities, exploitation of international jurisdictional complexities, and anonymity in cyberspace—none of which necessarily trigger the reporting of suspicious transactions (Habibzadeh, 2011).

3.2.1. Continuous Banking

Electronic money laundering threatens online banking through three main avenues:

a. Account Opening Without Customer Identification via the Internet

International and domestic banking regulations require the reporting of suspicious transactions. However, launderers can easily evade these restrictions through the facilities provided by online banking. For instance, by opening accounts with companies that have online banking but operate under weak regulatory oversight, launderers can use electronic payment systems without scrutiny. The most significant advantage for launderers in electronic banking lies in identity verification—

online banking makes it difficult to authenticate customer identities, record and retain accurate information, or report suspicious activity. By removing face-to-face interactions between customer and institution, it becomes extremely difficult to determine who truly controls an account or to verify the legitimacy of transactions. The person using the account may not be the one who initially opened it.

b. Use of Encryption and Digital Signature Technologies

As previously mentioned, encryption and digital signature technologies are critical in electronic money systems and banking operations for secure execution and reliability. If electronic money is encrypted, its content becomes unreadable, and only the intended recipient—regardless of global location—can decode it using the appropriate software. This level of confidentiality and anonymity allows anyone to transfer funds globally without revealing transaction contents.

c. Use of Money Mules

At times, launderers use individuals known as money mules to facilitate laundering processes. These may be natural or legal persons with seemingly legitimate fronts who assist criminals in laundering money. Such individuals support not only this method but also other laundering techniques used by offenders.

3.2.2. Internet Gambling

Today, traditional casinos are regulated to prevent money laundering, and many countries have been compelled to adopt similar oversight measures. As a result of this regulation, online casinos have become attractive venues for money launderers.

The online gambling process typically involves a criminal opening an account on a gambling website and sending dirty money to the site's online account in exchange for virtual chips, then deliberately betting with those funds.

Both parties in the gambling session may be accomplices. For example, one participant receives $100,000 in chips, and the other receives only $1,000. They then play until the first party wins all $101,000 through collusion. When asked about the origin of the funds, the winner can simply claim it was gambling winnings. Payments are often processed through checks drawn from the casino's accounts. Sometimes, launderers may have the winning chips issued in the name of a third party, thus hiding the criminal origin of the funds while laundering significant amounts of dirty money.

3.2.3. Continuous Online Gaming

Another relatively new method of money laundering is known as *virtual laundering*. In this technique, criminals utilize multi-level online games hosted on internet platforms played by numerous participants. In some of these games, players can purchase virtual currency using real-world money. They pay an entry fee, compete, and earn additional virtual income as rewards.

Players can transfer funds to other players or use virtual currency to buy and sell goods or services. This allows conversion between traditional and virtual currencies and facilitates transfers to other accounts. Sometimes instead of virtual money, players are given debit cards that can be transferred between accounts or used to withdraw money from ATMs.

3.2.4. Prepaid Cards

These electronic payment instruments can function like credit cards and are commonly used for purchasing online services. For instance, a person who has obtained money through illegal means may purchase a large number of phone cards or internet cards, then resell them at market price or even at a discount. The income from these sales is deposited into their account, thereby laundering the dirty money.

Alternatively, someone holding illicit funds may purchase large volumes of internet services from a provider, print the access cards, and resell them to shopkeepers or newsstand vendors. The revenue is then deposited into their own account. If questioned about the origin of the money, they may claim it was earned through legitimate commercial activity. In reality, this facilitates money laundering and complicates the process of tracing the true source (Richards, 1999).

3.2.5. Continuous Online Auctions

Companies that conduct online auctions and operate e-commerce-enabled websites maintain bank accounts. The seller lists a product on the website, and once a buyer shows interest and sends payment to the company's account, the seller ships the product. If the buyer confirms that the received item matches the order, the company transfers the payment to the seller's account.

Money launderers can exploit this system by listing expensive products for sale on the website and then having a fake buyer (often an accomplice) purchase the item and confirm receipt. This allows the laundering of illicit funds under the guise of legitimate transactions, transferring dirty money from one launderer to another (Bagherzadeh, 2004).

3.2.6. Electronic Trading of Precious Metals

The possibility of trading and transacting precious metals and bullion electronically has been established through certain websites globally. Prior to initiating any transaction, the buyer or seller must register on the platform to receive an electronic account. To register, the user is typically required to electronically submit their first and last name, identifying information, email address, and physical address. However, it is often possible to use falsified identities and addresses. Some websites do not even require identity verification to issue an electronic account. This creates opportunities for identity fraud or concealment. Once registered and assigned an electronic account, users can buy and sell precious metals with other registered users on the platform.

A user can register with different names and act as both buyer and seller. Some service providers continue to obscure identities during the transaction process—neither the buyer nor the seller knows the other's identity, and even their bank account numbers remain hidden. Consequently, the electronic market for precious metal exchanges potentially becomes a tool for money laundering.

3.3. Comparison of Traditional and Electronic Money Laundering (Stages and Outcomes)

The emergence and application of information and communication technology (ICT) in contemporary societies and its convergence with commerce and banking have fostered the development of money laundering. It has created a suitable virtual infrastructure for transforming traditional laundering into electronic laundering, which not only does not increase operational risk but also facilitates and accelerates the laundering process. Thus, electronic money and banking can be considered highly effective tools for money launderers, providing maximum profit at minimal cost. However, given the numerous benefits these technologies offer to society, they cannot be eliminated. The only viable approach is to pursue principled policies that prevent abuses—such as money laundering—while preserving the legitimate and developmental functions of these innovations.

Despite the identification of some laundering techniques, electronic money laundering continues to expand. Offenders will continue to develop more complex methods to operate in this space, often staying several steps ahead of anti-money laundering (AML) authorities. To effectively combat money laundering and its impact on society, governments must close this gap and pay greater attention to the role of new technologies in criminal activities.

As previously discussed, traditional money laundering typically involves three stages:

First: Introducing illicit proceeds into formal or informal financial networks, or purchasing high-value goods to convert criminal funds into legitimate financial instruments. This is usually conducted in the country where the criminal proceeds were originally generated.

Second: Obscuring audit trails by converting illicit proceeds into assets with ambiguous origins. One major method used in this stage is transferring funds to foreign bank accounts, often through offshore banks, regional commercial centers, or international banks with less stringent regulations.

Third: Reintegrating laundered income into the legitimate economy, giving the appearance of lawful revenue derived from legal activity. In this stage, funds are moved to economically stable countries for concealment and reinvestment (Tazhibi, 2005).

In electronic or modern money laundering, these stages are not necessarily required. Illicit funds can be circulated through electronic transactions and financial networks within a fraction of a second, leaving no traceable evidence of the origin or end-use of criminal proceeds.

In summary, a comparative analysis of traditional and electronic money laundering yields the following conclusions:

1. No need to follow all three traditional stages to launder illicit assets.
2. No requirement to commit auxiliary crimes such as forgery, murder, intimidation, or manipulation of financial institution employees.
3. Maximized profit with minimum time and cost.
4. Threats to users' privacy and opportunities for exploitation.
5. Possibility of identity concealment and failure to verify customer identity, allowing account users to differ from account openers.
6. Potential transgression of national borders and difficulty in determining the location and perpetrator of the laundering, affecting the criminal jurisdiction of states.

4. Effects of Money Laundering

This section presents the implications and adverse consequences of money laundering for society.

4.1. Societal Effects of Money Laundering

Large-scale money laundering has destructive and detrimental effects on national economies and the global community, including: the proliferation of underground criminal activity; disruption in tax collection and encouragement of tax evasion; distortion of financial markets; inflation; social deviation; institutional corruption; and damage to national integrity. Additional consequences include: unfair economic competition, weakening of the private and cooperative sectors, disruption of capital markets, illegal capital flight, bankruptcy of private firms, weakening of international trade foundations, heightened risks in privatization, accumulation of wealth by criminals and illegal operators, and declining productivity in the real economy.

Money laundering threatens a country’s economic and social health, contributes to institutional corruption, and undermines productive and public-benefit investments. It expands the informal economy and disrupts balance in housing, stock, currency, and other markets. The domestic impact of money laundering on the national economy is often far more severe than foreign influences. Structural reforms are essential to eliminate or at least reduce this adverse phenomenon (Mousavi Moghadam, 2007).

4.2. Adverse Economic Impacts of Money Laundering

1. The increase in money laundering and associated crimes leads to reduced monetary demand and a measurable decline in annual gross domestic product (GDP). Moreover, the growth of underground economic activities—which are not captured in GDP statistics—distorts economic policymaking.
2. Money laundering promotes the spread of criminal activity, weakens investment in productive sectors, and undermines economic foundations. It also distorts income distribution, diverting funds from large savings to smaller, high-risk ventures or from transparent investments to low-quality assets, thereby hindering economic growth (Rahbar & Fazlollah, 2008).
3. Money laundering contaminates legal transactions, eroding trust in markets and financial dealings due to high-profile embezzlement and fraud.
4. Another negative consequence is the illegal flight of capital. Illicit funds are often moved to developed Western countries for laundering and investment.
5. Weakening of the private sector: Money launderers mix criminal proceeds with legitimate funds through front companies. These entities, having access to considerable illegal capital, can offer products or services below market prices, making competition impossible for legitimate businesses. This forces legitimate enterprises out of the market and weakens the lawful private sector (Jazayeri, 2009).

6. Erosion of financial market integrity: Financial institutions reliant on criminal proceeds face greater difficulties managing assets, meeting obligations, and maintaining operational stability.
7. Reduction of government control over economic policy: In some developing nations, illegal revenues may distort national budgets and reduce state control over economic policy. In fact, large accumulations of laundered assets can exert pressure on entire markets or even small economies (Tazhibi, 2005).

5. Conclusion

The emergence of electronic banking and new methods of electronic fund transfer has facilitated the commission of money laundering offenses and introduced innovative ways to perpetrate this crime. Today, money launderers can easily transfer their illicit proceeds to other countries and cleanse the revenues from various crimes by exploiting the capabilities provided by electronic banking and cyberspace.

Countries with advanced information technology infrastructures but limited capacity to combat ICT-based and cybercrimes have become safe havens for organized crimes, including money laundering. Considering that organized criminal groups can recruit diverse experts and technologists in the field of information technology, we should expect increasingly innovative and advanced methods for committing organized crimes in the future. Many of these criminal organizations also adopt one another's methods for illicit enrichment, leading to the normalization and proliferation of such techniques, including the laundering of criminal proceeds. At the same time, obtaining intelligence about the criminal activities of these groups remains highly challenging. This is primarily because, first, most ICT-related services are provided by the private sector, whose main objective is commercial profit and client protection rather than combating transnational crimes. Second, the protection of civil liberties and individual rights is a legal priority in many countries, which restricts or complicates efforts to gather data related to money laundering and to monitor activities facilitated by information technology.

At present, there is widespread consensus across legal systems that the rapid growth of technology has led to an increased use of information systems and computer networks in the commission of economic crimes. The harmful impacts of money laundering on the economy—including the destruction of financial markets, weakening of the private sector, economic instability, damage to international reputations, and other adverse political and social consequences—combined with its transnational nature and potential to spread into the territories of other countries, necessitate the criminalization of money laundering both domestically and internationally. It also underscores the need for interstate collaboration to prevent, prosecute, and investigate crimes committed using advanced technologies, especially electronic money laundering.

In Iran's economy, due to the lack of awareness regarding the consequences and harms of money laundering—particularly electronic money laundering—no significant measures have yet been taken. The only notable step has been the enactment of the Anti-Money Laundering Law, which still suffers from significant shortcomings and requires substantial revision, enforcement mechanisms, and regulatory oversight to be effectively implemented.

To combat money laundering in Iran's legal system, the following actions must be taken:

1. One fundamental approach is to prevent predicate offenses that generate illicit income, thereby limiting the necessity for money laundering. According to Principle 156 of the Constitution of the Islamic Republic of Iran, the judiciary is responsible for crime prevention. Thus, it is appropriate for the judiciary to establish institutions and engage experts to conduct comprehensive studies identifying the causes of crime and strategies for prevention, as well as to manage executive actions aimed at reducing crime rates. This, of course, does not negate the responsibility of other branches of government. Given that various economic, social, political, and cultural factors contribute to criminal behavior, relevant ministries and agencies must participate in policymaking, and legislation must clearly define the duties of each institution regarding crime prevention.
2. Reforming and restructuring the economy is essential to reduce criminal incentives. All major policy decisions affecting society must be analyzed through a criminological lens.
3. A specific law tailored to combat money laundering should be drafted, aligned with international and regional conventions, to address current legal gaps and implementation issues in the existing anti-money laundering framework.

4. Integration of the banking and stock market systems with the tax system can facilitate more effective implementation of the Anti-Money Laundering Law. The judiciary, the Ministry of Economic Affairs and Finance, and other relevant bodies should collaborate to establish appropriate mechanisms and enforceable safeguards for the law.
5. Currency and monetary system oversight, along with the deployment of supervisory mechanisms to prevent laundering by public officials, the establishment of necessary institutions, and the modernization of the tax administration system, are strategies that reduce the economic motivations for laundering within a country.
6. Another recommendation is the use of data mining techniques. Data mining is the extraction of predictive and hidden information from large datasets and is a powerful new technology with significant potential to help organizations focus on critical insights. Data mining tools predict future behaviors and trends, allowing institutions to make decisions based on analysis and forecasting. These tools can answer questions that previously took too long to resolve. Today, data mining is used in both banking and non-banking financial sectors, as well as auditing institutions, to detect suspicious financial behavior, including money laundering.
7. Finally, it is important to recognize that one of the most effective tools against electronic money laundering is global cooperation, as electronic money knows no borders. Therefore, joining international monetary and financial treaties and leveraging their mechanisms can strengthen a country's immunity to money laundering. More important than the mere existence of laws is the establishment of regional and international cooperation frameworks to create supervisory and regulatory umbrellas for combating illicit finance. Countries that understand they cannot tackle money laundering in isolation—and that such crime has a transnational and cross-border nature—must seek to reduce its damaging effects by joining regional agreements or acceding to international conventions.

Authors' Contributions

Authors contributed equally to this article.

Declaration

In order to correct and improve the academic writing of our paper, we have used the language model ChatGPT.

Ethical Considerations

All procedures performed in this study were under the ethical standards.

Acknowledgments

Authors thank all individuals who helped us do this study.

Conflict of Interest

The authors report no conflict of interest.

Funding/Financial Support

According to the authors, this article has no financial support.

References

Asadi, S. H. (2007). *Transnational Organized Crimes*. Mizan Publishing, Tehran.

Bagherzadeh, A. (2004). *Economic Crimes and Money Laundering in the Draft United Nations Convention Against Corruption and Other International Documents*. Majd Publications, Tehran.

Bagherzadeh, A. (2009). *Money Laundering in Iranian and English Law and International DocumentsPB - Mizan Publishing, Tehran*.

Bidabad, B. (2013). *Detailed Plan for the Money Laundering Detection System*. Research and Planning Department.

Bosworth-Davis, R. (1994). *Money Laundering: A Practical Guide to New Legislation*. kluwer law publication.

Habibzadeh, M. J. (2011). The Role of Electronic Banking in Money Laundering and Methods to Combat It. *Comparative Research Quarterly*, *15*(1).

Jalali Farahani, A. H. (2005). Electronic Money Laundering. *Quarterly Journal of Jurisprudence and Law*(4).
Jazayeri, M. (2009). *Money Laundering and Financial Institutions*. Higher Institute of Banking Education of Iran, Tehran.
Mir Mohammad Sadeghi, H. (1998). *International Criminal Law*. Mizan Publishing, Tehran.
Mousavi Moghadam, M. (2007). *Money Laundering*. Ninava Publications, Qom.
Rahbar, F., & Fazlollah, M. (2008). *Money Laundering and Methods to Combat It*. Tehran University Press and Publishing Institute, Tehran.
Richards, J. (1999). *Transnational Criminal Organizations,Cybrecrime, and Money Laundering*. CRC Press. https://doi.org/10.4324/9780367801991
Saki, M. R. (2008). *Introduction to Money Laundering Crime*. Judicial Training and Research Deputy, Javdaneh Publications, Tehran.
Tazhibi, F. (2005). *Money Laundering and the Banking System*. Zaeem Publications, Tehran.