International Journal of Law and Society

E-ISSN: 3046-9562
P-ISSN: 3046-9619

Research Article

Jurisdictional Enforcement Of Cyber Crime Against Lottery Scam

Jesslyn Elisandra Harefa[1*], Rahmayanti[2], Eri Siswanto[3], Faruq Rozy[4], Ireny Natalia Putri Sihite[5]

1 Universitas Pembangunan Panca Budi,Indonesia
e-mail: jesslynharefa19@gmail.com
2 Universitas Pembangunan Panca Budi,Indonesia
e-mail: rahmayanti@dosen.pancabudi.ac.id
3 Universitas Pembangunan Panca Budi,Indonesia
e-mail: erisiswanto@yahoo.com
4. Universitas Pembangunan Panca Budi,Indonesia
e-mail: faruqrozy48@gmail.com
5. Universitas Pembangunan Panca Budi,Indonesia
e-mail: renyputris@gmail.com

*** Corresponding Author** : Jesslyn Elisandra Harefa

Abstract: Cyber crime is increasingly prevalent with various modes, one of which is fraud under the guise of lottery prizes. This crime not only causes financial losses but also complicates law enforcement officials in terms of jurisdiction, especially if the perpetrators and victims are located in different regions, even across countries. This research aims to analyze how jurisdiction is enforced in dealing with cyber-based fraud crimes and examine the effectiveness of national legal instruments against the digital fraud mode. The research method used is a normative juridical approach with secondary data analyzed descriptively-analytically. The results show that jurisdictional enforcement in this case still faces technical and legal challenges, especially in the aspect of inter-state coordination and the limitations of domestic legal instruments in reaching cross-border perpetrators. Strengthening international cooperation and updating national regulations are needed to anticipate the dynamics of cybercrime.

Keywords: Cyber Crime; Fraud; Jurisdiction; Law Enforcement; Lucky Draw

1. Introduction

The development of information and communication technology has had a major impact on human life, including in social, economic and legal aspects. However, this technological advancement has also created new challenges in the form of cybercrime, which is increasingly complex and difficult to overcome. One mode that is often used in cybercrime is fraud under the guise of lucky draws, which is usually carried out through social media, instant messaging applications, or fake websites. The perpetrators use a manipulative approach by capitalizing on people's curiosity and expectations of prizes, which ultimately ensnares victims to hand over personal data or even money (Suryani, 2022).

Lottery scams are a form of online fraud that can have a devastating economic and psychological impact. Data from the Ministry of Communication and Information shows that public reports of online fraud, including lottery scams, have increased significantly since 2020 to date. In addition to financial losses, victims often experience mental distress because they feel embarrassed and helpless after being scammed by unknown and difficult-to-trace perpetrators (Ramadhani, 2021). This shows that digital crime is not only an economic crime, but also a social crime that erodes people's sense of security in the digital space.

The main problem in handling cyber crimes like this is the issue of jurisdiction. In conventional criminal law, jurisdiction refers to the geographical location where the criminal offense occurred. However, in cross-border cyberspace, perpetrators can be located in other countries, use foreign servers, and disguise their identities, making it difficult for law enforcement to reach and prosecute them (Yulianto, 2021). The territorial nature of the national legal system is less effective in dealing with crimes that do not recognize borders

Received: May 17, 2025

Revised: May 31, 2025

Accepted: June 25, 2025

Online Available: June 27, 2025

Curr. Ver.: June 27, 2025

such as digital fraud. This has led to the need for a more flexible jurisdictional approach and stronger international cooperation.

In Indonesia, law enforcement against cyber fraud under the guise of lotteries still relies on regulations such as Law Number 11/2008 on Electronic Information and Transactions (ITE) and its amendments, as well as the Criminal Code (KUHP). However, these regulations have not fully addressed the jurisdictional challenges in cross-border cybercrime. This weakness in law enforcement is often exploited by perpetrators who operate from abroad and feel safe from the reach of Indonesian law (Prasetyo, 2023). In some cases, perpetrators even use fake identities and location disguise software to avoid detection.

Given this reality, it is important for governments and law enforcement officials to develop a more adaptive jurisdictional enforcement approach to the development of digital crime. This includes bilateral and multilateral cooperation, the use of sophisticated cyber-tracking technology, and the updating of legal regulations that are more specific and responsive to the evolving modes of digital crime (Wahyuni, 2023). Thus, law enforcement against fraud under the guise of lucky draws is not only the responsibility of national law, but also part of the global agenda in creating a safe and fair digital space for society.

2. Theoretical Study

Cybercrime

Cybercrime is a form of crime that utilizes information and communication technology as the main means of committing unlawful acts, either by attacking systems, data, or individuals in cyberspace. According to Law No. 11/2008 on Electronic Information and Transactions (ITE), as updated by Law No. 19/2016, cybercrimes include the dissemination of false information, defamation, illegal access, system disruption, and fraud committed through electronic media. In practice, these crimes are very dynamic and difficult to trace because perpetrators often use anonymous devices, virtual private networks (VPNs), and spread digital traces in a fragmented manner across multiple jurisdictions. The uniqueness of cyber crime lies in its non-physical characteristics, can be carried out remotely, does not recognize national borders, and uses methods that continue to evolve along with technological advances. Cyber-based fraud under the pretext of lucky draws is a concrete example of this crime, where perpetrators deliberately spread false information to trick victims and gain illegal financial benefits. Such crimes pose great challenges due to the difficulty of identifying perpetrators hidden behind virtual identities, as well as limited human resources and technology in conducting investigations. Therefore, cyber crimes require a specialized, integrated and responsive legal approach to changes in modus operandi and involve cross-agency and cross-state collaboration to ensure justice and protection of the digital society (Suryani, 2022; Ramadhani, 2021).

Jurisdiction in Criminal Law

Jurisdiction in criminal law is a fundamental concept that determines the authority of a state to create, apply, and enforce criminal law against individuals or acts that occur within or in relation to the state with its territory. In general, jurisdiction in criminal law is divided into several principles, namely territorial principle, active national principle, passive national principle, protection principle, and universal principle. The territorial principle provides authority for the state to prosecute criminal acts that occur within its territory; the active national principle provides jurisdiction over its citizens who commit crimes abroad; the passive national principle applies when citizens become victims abroad; while the protection and universal principles are used in the context of crimes that endanger the interests of the state or the international community. In the context of cybercrime, the concept of jurisdiction faces great challenges because the perpetrators, victims, and data used can be located in different countries, so that geographical boundaries become blurred and difficult to apply conventionally. The Indonesian ITE Law in Article 2 tries to overcome this by expanding jurisdiction extraterritorially, stating that the ITE Law applies to everyone who performs legal acts both inside and outside the jurisdiction of Indonesia, as long as the act has legal consequences in the territory of Indonesia. However, the implementation of this jurisdiction in practice is highly dependent on the state's ability to establish international cooperation, both bilaterally and multilaterally, including through mutual legal assistance (MLA), extradition agreements, and coordination through organizations such as INTERPOL.

Without this cooperation, jurisdictional enforcement will be hampered by differences in legal systems, the reluctance of the perpetrator's home country to extradite its citizens, and technical obstacles in the identification of perpetrators. Thus, the study of jurisdiction in criminal law must continue to be expanded and updated in order to be able to answer the challenges of transnational crime, especially in the context of a very complex and rapidly changing cyber world (Yulianto, 2021; Prasetyo, 2023).

Modes of Fraud in the Guise of Lottery

The lottery scam is a form of fraud-based crime that utilizes people's excitement, curiosity, and lack of digital literacy as an entry point for misleading information and subtle extortion. Generally, this mode is carried out through short messages (SMS), instant messaging applications such as WhatsApp or Telegram, social media, and emails containing information as if the victim has won a prize from a certain company or institution. In the message, the perpetrator includes instructions to call a certain number or access a link, which will then direct the victim to a request to send personal data, account numbers, or even pay a certain amount of money as a condition of prize disbursement. This modus operandi has evolved to become increasingly convincing, complete with fake winner's certificates, official agency logos and fake testimonials from "previous winners". Some perpetrators even use bots and voice engineering to amplify their deception. In a legal context, this mode is classified as electronic fraud as stipulated in Article 28 paragraph (1) of the ITE Law, which prohibits the dissemination of false and misleading information that harms consumers in electronic transactions. Unfortunately, there are still many victims who are reluctant to report because they are embarrassed, do not know the reporting mechanism, or feel that they will not get justice. Therefore, countermeasures against this mode must not only be carried out through a legal approach, but also through a public education approach, strengthening digital literacy, and tighter supervision of the digital communication channels used by the perpetrators (Wahyuni, 2023; Hamdani, 2020).

3. Research Methodology

The research method used in this writing is the normative juridical method, which is an approach that relies on the study of laws and regulations, legal literature, doctrine, and relevant court decisions, in order to analyze legal issues related to the enforcement of jurisdiction over cyber crimes, especially fraud enforcement of jurisdiction over cyber crimes, especially fraud under the guise of lucky draws. This research is descriptive-analytical, with the aim of describing systematically and in depth how Indonesian positive law regulates jurisdiction in cybercrime and assessing the effectiveness of its application in practice. The data used is secondary data obtained through literature study, including primary legal materials such as laws, implementing regulations, and court decisions; secondary legal materials such as law journals, textbooks, and scientific articles; and tertiary legal materials such as legal dictionaries and legal encyclopedias. This normative approach was chosen because the focus of the study is on applicable legal norms and their interpretation in the context of the dynamics of digital crime, allowing researchers to provide legal arguments in a logical and structured manner. In addition, researchers also used a conceptual approach to understand the principles of jurisdiction in international and national criminal law, as well as a comparative approach in examining jurisdictional practices in other countries as relevant comparisons. All data collected is then analyzed qualitatively to produce conclusions that are in accordance with the formulation of the problem that has been set.

Results And Discussion

Jurisdictional Enforcement in Cyber Crime Under the Guise of Lucky Draws

Jurisdictional enforcement in the context of cybercrime, especially fraud under the guise of lucky draws, faces serious challenges in its implementation in Indonesia. Based on the provisions of Article 2 of Law Number 11 Year 2008 on Electronic Information and Transactions (ITE), Indonesia adheres to the principle of expansion of jurisdiction which allows the application of law against perpetrators who are outside the territory of Indonesia if the consequences of their actions are felt in Indonesia. In the case of digital fraud committed through electronic media, Indonesian jurisdiction is theoretically enforceable even though the perpetrator is not physically located in Indonesian jurisdiction. However, in practice, law enforcement mechanisms are still limited by technical constraints, limited access to electronic data across countries, and the low effectiveness of cooperation between countries in the context of mutual legal assistance (MLA) and extradition. This condition shows that the normative expansion of jurisdiction has not been in line with implementation in the field, especially if the perpetrator is located in a country that does not have an extradition treaty with Indonesia.

In several case studies, as reported by the Indonesian National Police in 2022, there were many public reports related to digital lottery scams that led to large losses but could not be processed further because the perpetrators used foreign numbers and could not be traced with ordinary IP addresses. One example is a scam that uses fake domains resembling official agencies, directs victims to fill out personal data forms, and asks for money for "prize management." Law enforcement efforts are often hampered because perpetrators use digital disguise techniques such as VPNs, anonymous servers, and disposable social media accounts that make their digital footprints disappear quickly. The existence of overlapping legal jurisdictions, as well as the lack of data coordination systems between countries, means that perpetrators of these crimes feel safe from prosecution. In fact, in some cases, perpetrators take advantage of time gaps to move the proceeds of crime to various international digital platforms before authorities have a chance to track them down.

Jurisdictional enforcement cannot rely solely on a narrow territorial approach, but must be based on international legal collaboration, improved digital tracking technology, and active involvement of digital service providers to assist in the identification of perpetrators. Strengthening the role of institutions such as the Authority Financial Services (OJK), Kominfo, and BSSN in handling complaints and accelerating the collection of digital evidence are key. In addition, the Indonesian government needs to continue to encourage the ratification of international agreements such as the Budapest Convention on Cybercrime in order to effectively seek cross-border cooperation in cracking down on cybercrime perpetrators. Without strengthening the jurisdiction and cross-border legal coordination network, law enforcement efforts against digital fraud with lucky draw mode will continue to face dead ends that harm the public and weaken public confidence in the law.

Effectiveness of National Legal Instruments in Dealing with Cyber Fraud in the Guise of Lucky Draws

National legal instruments such as the Criminal Code and ITE Law have provided a legal basis to take action against cyber fraud perpetrators, but in practice there are still many weaknesses found in handling fraud cases under the guise of lucky draws. Article 28 paragraph

(1) of the ITE Law does prohibit the dissemination of false and misleading information, but it does not specifically regulate fraud modes such as fictitious lotteries that occur in the community. Law enforcement officers often have difficulty in proving the complete criminal elements because the perpetrators use temporary accounts and disguise their identities. In addition, coordination between institutions such as the police, Kominfo, and digital platforms is still not optimal. People's lack of digital literacy also worsens the situation, as victims often do not report or only realize that they have been deceived after losses have occurred. Therefore, the effectiveness of legal instruments will be optimized if accompanied by regulatory updates that are specific to digital crime modes, increased capacity.

Conclusion

Jurisdictional enforcement of cyber crimes, particularly lottery scams, still faces complex challenges in terms of legal, technical and cooperation between countries. Although normatively Indonesia has expanded jurisdiction through Article 2 of the ITE Law, implementation in the field has not been fully effective due to limited tracking technology, lack of international cooperation, and weak regulations that specifically regulate this mode of crime. National legal instruments such as the Criminal Code and ITE Law have also not been fully responsive to the ever-changing and increasingly sophisticated development of digital crimes. Therefore, the law enforcement approach to cybercrime requires updating regulations, strengthening the capacity of law enforcement officials, as well as improving cross-agency and cross-state coordination.

Advice

The government needs to update and strengthen national regulations, particularly by adding provisions that explicitly regulate mode-based digital fraud such as fake lotteries so that law enforcement has a stronger basis for prosecution. In addition, it is important to increase the capacity of cyber investigators through training and utilization of digital forensic technology, and expand international legal cooperation, both through extradition agreements and cross-border crime data exchange. On the other hand, public education on digital literacy and how to recognize fraud modes must be massively promoted to prevent more victims. Prevention, prosecution, and protection efforts must run simultaneously so that Indonesia's digital space becomes safer and protected from cybercrime.

Referensi

[1]. Hamdani, F. (2020). Cyber fraud and legal challenges in the digital era. Journal of Criminal Law, 11(2), 77–90.
[2]. Law of the Republic of Indonesia Number 11 of 2008 concerning Electronic Information and Transactions. (2008).
[3]. Law of the Republic of Indonesia Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions. (2016).
[4]. Prasetyo, A. (2023). The development of cybercrime regulation in Indonesia. Journal of National Legislation, 11(2), 89–101.
[5]. Ramadhani, T. (2021). Cyber crime and law enforcement in Indonesia. Journal of Cyber Security, 3(1), 22–36.
[6]. Suryani, M. (2022). The effectiveness of the ITE Law in dealing with cybercrime. Journal of Legal Science, 14(1), 33–48.
[7]. Wahyuni, L. (2023). Analysis of online lottery crime mode in digital space. Journal of Technology and Law, 6(3), 44–56.
[8]. Wicaksono, R. (2022). The principle of jurisdiction in cyber crime. Journal of International Law, 8(1), 15–27.
[9]. Widodo, I. (2023). International collaboration in tackling cyber crime. Journal of Global Security, 6(1), 29–43.
[10]. Yulianto, D. (2021). Law enforcement against cybercrime in the perspective of international jurisdiction. Journal of Law and Technology, 5(2), 120–133.