PERADABAN JOURNAL OF LAW AND SOCIETY

Article

Law Enforcement Against Scampage at Polda Jatim: Perspectives of Positive Law and Islamic Criminal Law

Naila Nur Izzah

Universitas Islam Negeri (UIN) Sunan Ampel, Surabaya, Indonesia
email : nailaizh@gmail.com

Abstract

This article focuses on two main questions: (1) How is law enforcement against scampage crimes conducted during investigations by Polda Jatim from the perspective of positive law, and (2) How is law enforcement against scampage crimes from the perspective of Islamic criminal law. The research method used is empirical, with primary data obtained from interviews at Polda Jatim and secondary data from regulations, journals, and related articles. Data collection was conducted through interviews and documentation, then analyzed qualitatively with a deductive approach. The research findings indicate that law enforcement by the Cyber Unit of Ditreskrimsus Polda Jatim follows proper procedures. Preventive measures are carried out through cyber patrols, while repressive measures use Article 35 in conjunction with Article 51 Paragraph (1) of Law No. 19 of 2016 concerning Amendments to Law No. 11 of 2008 on Information and Electronic Transactions (ITE). From the perspective of Islamic criminal law, the applied sanctions resemble *jarimah ta'zir*, allowing judges to impose educational and corrective punishments.

Keywords

Law enforcement, scampage crimes, Islamic Criminal Law, Positive Law

PERADABAN JOURNAL OF LAW AND SOCIETY
Vol. 3, Issue 1, June 2024

E-ISSN: 2830-1757

Page : 63-76

DOI : https://doi.org/10.59001/pjls.v3i1.172

INTRODUCTION

Activities through electronic media or cyberspace have provided numerous benefits to contemporary society. The Internet is part of cyberspace and is considered a new reality in daily life (Wahid & Labib, 2005). The advancement of Information Technology has facilitated the dissemination of information but has also brought about negative impacts

(Rumlus et al., 2020). New threats such as cyber warfare, terrorism, pornography, illegal trade, phishing, and misuse of personal data have emerged due to the rapid development of the internet (Nursita, 2019).

Misuse in cyberspace, known as cybercrime, has broader impacts than conventional crimes due to its borderless nature (Sinaga, 2022). Transnational cybercrime requires international coordination and cooperation for effective mitigation (Saudi, 2018). One form of cybercrime is scampage, where perpetrators mimic legitimate websites to deceive individuals into divulging personal information unlawfully (Okpa et al., 2020). Scampage offenses in Indonesia are governed by Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 regarding Electronic Information and Transactions (ITE), particularly Article 35 jo. Article 51 paragraph (1).

From the perspective of Islamic criminal law, scampage is categorized as *jarimah ta'zir*, with its punishment determined by *Ulil Amri* or a judge (Syarbaini, 2019). A prominent scampage case in Indonesia occurred on March 1, 2021, where the Directorate of Criminal Investigation of East Java Police discovered two Indonesian nationals involved in creating a fake website to defraud the US government by fraudulently claiming Pandemic Unemployment Assistance (PUA) funds (Tri, 2021). This case resulted in a loss of USD 60,000 to the US government.

Addressing transnational scampage crimes requires international law enforcement cooperation to uphold justice, utility, and legal certainty. A primary challenge in combating cybercrime is the low awareness among victims to report incidents (Friend et al., 2020). Therefore, the role of experts and law enforcement is crucial in detecting and preventing cybercrime.

The purpose of this study is to provide a clear overview of law enforcement regarding scampage crimes at the East Java Regional Police (Polda Jatim). This research aims to understand and analyze how law enforcement processes against scampage crimes are conducted from a positive legal perspective. Additionally, the study seeks to uncover how Islamic criminal law addresses similar cases.

In the Indonesian context, understanding cybercrime from an Islamic perspective is a pressing necessity given two main considerations: first, the significant impact of rapid technological advancements, and second, the large Muslim population in the country. Studies indicate that Islamic education and ethical values play a crucial role in shaping individual character and fundamental social values, which are essential in addressing the complex challenges posed by cybercrime (Suparjo & Hidayah, 2023). The integration of Sharia principles into digital technologies, such as online payments, highlights the need to maintain harmony between technological innovations and religious values, making them relevant to Islamic teachings (Hamsin et al., 2023).

Additional challenges arise from the Islamic legal perspective on phenomena like sexual harassment and the spread of fake news on social media, which are deemed serious under *Fiqh jinayah*, reinforcing the need for legal protection for victims and the implementation of stringent sanctions against offenders (Rizky et al., 2023). Overall, the urgency of understanding cybercrime

from an Islamic viewpoint in Indonesia impacts moral and ethical aspects and necessitates robust legal frameworks and comprehensive education for the community, particularly the younger generation vulnerable to online crime risks (Anggraeny et al., 2022).

Therefore, a deeper understanding of Islamic principles in the context of cybercrime can contribute to creating a safer digital environment aligned with religious values while ensuring that technological advancements do not compromise moral integrity and legal justice in Indonesia. This research aims to provide comprehensive insights and offer recommendations for improving the handling of scampage offenses in the future.

METHOD

The research conducted in this study falls under the category of empirical legal research, which analyzes the functioning of law within society (Muhaimin, 2020). It is carried out through field research, utilizing a qualitative approach. Field research involves direct interaction between the researcher and data sources, in this case, the police, particularly the Cyber Unit of the Directorate of Criminal Investigation (Ditreskrimsus) at the East Java Regional Police (Polda Jatim).

Qualitative analysis is conducted as the method and data collection technique, involving observations and participatory interviews. The focus is on the aspects of law enforcement conducted by the Cyber Unit of Ditreskrimsus Polda Jatim regarding scampage crimes committed by two Indonesian citizens against the government of the United States of America.

RESULTS AND DISCUSSION

Law Enforcement of Scampage Crimes: A Review of Positive Law and Islamic Criminal Law

In Dutch law, a strafbaar feit refers to an act regulated and prohibited by law, with criminal penalties as consequences for violations (Moeljatno, 2008). In the digital era, cybercrime phenomena like scampage or phishing have demonstrated their transnational characteristics, often involving elements from multiple countries in their transnational activities (Sinaga,2022).

Scampage involves online fraud where perpetrators create replicas of web pages to obtain victims' personal information through deception (Zahron & Ali, 2021). Merwe et al. (2005) define phishing as "fraudulent activity involving the creation of replicas of existing website pages to deceive users into divulging their personal information (Marwe et al., 2005)." Perpetrators, known as scammers, employ various techniques such as email spoofing and web-based messaging to steal sensitive information (Okpa, Ajah, & Igbe). Scammers typically contact victims via email or text messages, for instance, receiving an email purportedly from a bank asking the victim to update their personal data and bank account number. However, the login page is fake, and the perpetrator exploits this to steal the victim's information for personal gain (Zaharon, Farhana, & Ali, 2022).

In the context of Indonesian law, scampage crimes are regulated by Law Number 19 of 2016 concerning Electronic Information and Transactions (ITE). Article 28 point (1) of the ITE Law categorizes scampage as electronic fraud, with specified sanctions under applicable law (Gulo et al., 2020).

From an Islamic legal perspective, scampage crimes may be categorized as *jarimah ta'zir*, an act prohibited and subject to punishment based on considerations of justice (Muslich, 2024). The concept of *jarimah* emphasizes that in Islam, any action violating Sharia rules, even if not specifically stipulated in had or qissas diyat, remains prohibited and subject to sanctions.

Law enforcement in this context aims not only to impose punishment as deterrence but also to ensure behavioral change and uphold justice values in society (Rahardjo, 2009). Soekanto (1983) explains that law enforcement is a harmonization process between applied legal values and tangible actions to create peace and justice.

In Indonesia, law enforcement against scampage involves both preventive and repressive strategies. Preventive efforts occur before crimes happen, such as through public education about scampage threats and prevention methods (Arief, 1998). Meanwhile, repressive approaches occur post-crime, involving law enforcement agencies to prosecute perpetrators according to the law (Arief, 1998).

In law enforcement, three crucial elements must be considered: legal certainty, justice, and societal benefits (Mertokusumo, 1999). The success of law enforcement lies in balancing these elements to create a safe and just environment for all (Sudikno, 1999).

From an Islamic legal perspective, the principle of justice in imposing sanctions is highly emphasized. *Ulil Amri* asserts that Islamic judges must render decisions based on impartial justice, in line with Islamic teachings that uphold social and individual values (Pancasilawati, 2013).

Case Description and Scampage Crime at East Java Regional Police (Polda Jatim)

The scampage crime that occurred within the jurisdiction of the East Java Regional Police was uncovered by the Cyber Unit of the Directorate of Criminal Investigation (Ditreskrimsus) Polda Jatim. Based on interviews conducted by the Author with the Informant, in February 2021, Officers conducted cyber patrols on the Facebook group SIG (Silent is Gold), whose members were involved in illegal access activities. During this operation, a post was found by a Facebook account under the name "Ozy Localhost," indicating an intention to purchase Twilio accounts for sending SMS spam/phishing to the United States, as well as a post by the defendant expressing interest in purchasing credit cards belonging to residents of Columbia.

Subsequently, the Cyber Unit conducted profiling of the owner and/or user of the Facebook account "Ozy Localhost," leading to the identification of SFR as the owner and/or user of the account. On March 9, 2021, SFR was

successfully apprehended. Based on SFR's statement, MZ was then apprehended by officers from Ditreskrimsus Polda Jatim on Wednesday, March 10, 2021.

The incident began in May 2020 when SFR met S, is person on the wanted list and an Indian citizen, through the SIG Facebook group (Silent Is Gold), whose members included hackers, spammers, and carders. They frequently discussed illegal access methods. S requested assistance from SFR in spreading scampage to obtain personal data of American citizens in exchange for USD 1 per personal data. However, SFR claimed an inability to create scampage but could assist in dissemination.

To create the scampage, S (DPO) contacted MZ, a member of the "Kolam Tuyul" Facebook group, which includes hackers, spammers, carders, and discussions on illegal access methods. S claimed the ability to manipulate the personal data of citizens in American states to access or steal government aid funds, intending to sell the data within their community. He promised to compensate MZ with a sum of money if he assisted in creating the scampage.

Since May 2020, the fake website created by MZ has been disseminated by SFR using SMS Blast techniques with messages such as: "alert from NyDMV: We are sorry to inform you due to our regulation-compliant update, you must update your contact information. For more info visit: ow.ly/3ko2423ko." Clicking on the link directs users to the scampage URL, tricking targets into believing it is an official government website.

The stolen personal data of American citizens was used by the suspects to claim pandemic unemployment assistance (PUA) funds intended for unemployed individuals affected by the COVID-19 pandemic in the United States. Each individual in the country was eligible to receive USD 2,000 in aid. As a result of the defendant's actions, the United States government incurred a loss of USD 60,000 over the course of one year. SFR gained approximately USD 30,000 (approximately IDR 420 million), while MZ earned IDR 60 million during the execution of their scheme (Jatimpos, 2021).

The distinguishing factor between the authentic and fraudulent websites created by the defendants lies in their domain names. The genuine government websites of the United States utilize the domain ".gov," whereas the fraudulent scampage websites operated by the defendants used various domains such as .link, .com, .info, and .net (Charisma, 2022). Below are 14 government websites whose scampage versions were successfully created by MZ and subsequently handed over to S :

- https://www.dmv.ca.gov/portal/website](https://www.dmv.ca.gov/portal/website) - California Department of Motor Vehicles, United States
- https://www.bmv.ohio.gov/website - Ohio Bureau of Motor Vehicles, United States
- https://www.dmv.ny.gov/website - New York Department of Motor Vehicles, United States

- https://www.oregon.gov/odot/dmv/pages/index.aspx - Oregon Department of Motor Vehicles, United States
- https://www.dmv.ri.gov/website - Rhode Island Department of Motor Vehicles, United States
- https://doa.alaska.gov/dmv/ - Alaska Department of Motor Vehicles, United States
- https://drive.ky.gov/Pages/default.aspx - Kentucky Department of Transportation, United States
- https://ides.illinois.com/ - Illinois Department of Employment Security, United States
- https://www.flhsmv.gov/ - Florida Department of Highway Safety and Motor Vehicles, United States
- https://revenue.alabama.gov/ - Alabama Department of Revenue, United States
- https://mdot.maryland.gov/pages/home.aspx - Maryland Department of Transportation, United States
- https://azdot.gov/ - Arizona Department of Transportation, United States
- https://wisconsinindot.gov/Pages/home.aspx - Wisconsin Department of Transportation, United States
- https://www.in.gov/bmv/ - Indiana Department of Transportation, United States

Barda Nawawi Arief highlighted that law enforcement efforts consist of two main approaches: preventive and repressive measures. Repressive law enforcement actions are undertaken when a criminal act has already occurred. At the operational level, repressive law enforcement is supported through various separate organizational entities within the framework of law enforcement, namely the Police, Public Prosecutor's Office, Lawyers, and Judiciary (Arief, 1998).

Regarding the policies pursued by the Cyber Crime Directorate of the Criminal Investigation Unit (Ditreskrimsus) of East Java Regional Police, in this case, it involves repressive or penal measures using Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law). These efforts are initiated based on reports or complaints received from the aggrieved parties.

A Police Report is a written report prepared by the Indonesian National Police officers regarding an incident suspected of constituting a criminal offense, whether discovered independently or through notification by someone due to rights or obligations under statutory regulations. According to Article

5 of the Chief of the Indonesian National Police Regulation Number 14 of 2012 concerning Criminal Investigation Management, Police Reports consist of two models: First, Police Report Model A is prepared by police officers who directly experience, witness or discover the incident. Second, Police Report Model B is prepared by police officers based on complaints received from the public.

The case of scampage criminal offenses within the jurisdiction of East Java Regional Police, it falls under Police Report Model A because the incident was uncovered by the Cyber Crime Unit of Ditreskrimsus in March 2021, where the report was made by police officers who directly experienced, witnessed, or discovered the incident.

The next stage involves investigation. Investigation, as defined in Article 1 number 5 of the Indonesian Criminal Procedure Code (KUHAP), is a series of actions to search for and find an incident suspected of constituting a criminal offense to determine whether an investigation should proceed. According to Article 1 number 4 of KUHAP, an Investigator is a designated Indonesian National Police officer with authority. The investigation into the report is conducted by investigators to determine whether an act constitutes a criminal offense, and if so, the law enforcement process can proceed to subsequent stages.

Based on an interview with IPDA Niken Charisma from the Cyber Crime Unit of East Java Regional Police, the investigative team conducted examinations on SFR on March 1, 2021, presenting an assignment order and investigation warrant. During this examination, evidence was found indicating that SFR disseminated scampage to obtain or transfer other personal data. Subsequently, on March 2, 2021, MZ was examined with the same procedural documentation, revealing that MZ was the creator of the scampage that SFR distributed.

Based on this investigation and initial evidence collected by the investigators, it was determined that these actions constituted a criminal offense due to meeting both subjective and objective elements. From a subjective standpoint, intent or dolus was established as the actions were deliberate, unauthorized, or unlawful. Objectively, the offense was established as it violated the law, causing harm to the victims and the Government of the United States.

In investigating this case, it was found that the illegal actions involving technology within cyberspace constituted as a criminal act. Therefore, the next stage involved criminal investigation, authorized by an investigation order. According to Article 1 number 2 of the Indonesian Criminal Procedure Code (KUHAP), an investigation comprises a series of actions by investigators as stipulated by law to gather evidence that clarifies the criminal offense and identifies the suspect. An investigator, as defined in Article 1 number 1 of KUHAP, is a designated officer of the Indonesian National Police or certain civil servants authorized by law to conduct investigations.

Following the investigation, the investigators proceeded with suspect designation. To designate someone as a suspect, preliminary evidence is required. As per Article 1 number 14 of KUHAP, a suspect is someone who, based on preliminary evidence, is reasonably suspected of committing a

criminal act supported by at least two pieces of evidence.

During the steps conducted by the Cyber Unit, if there is evidence of the alleged criminal offense as previously charged and the perpetrator can be identified as a suspect, efforts will be made to compile the case for submission to the Prosecutor's Office. If no criminal offense is found in the incident, law enforcement efforts will be discontinued.

The crime of scampage not only occurs domestically within one country but also involves multiple countries, commonly known as Transnational Cybercrime, where the victims include the government of the United States. Therefore, both countries collaborate to exchange information in the interest of law enforcement in tackling this transnational crime.

Regarding preventive law enforcement efforts by the Cyber Unit of the Criminal Investigation Directorate of East Java Regional Police against scampage crimes, measures include blocking scampage sites to secure the public from falling victim to this criminal modus operandi. Officers also conduct cyber patrols to ensure prompt handling of similar cases without waiting for victim reports.

Challenges faced by investigators of the Criminal Investigation Directorate of East Java Regional Police in uncovering cybercrime cases involving website forgery or scampage include internal factors such as investigator capabilities and forensic facilities related to the case. Additionally, the lack of reports poses a significant hurdle; in this case, victims may not be aware that their rights are being infringed upon by others, thereby not reporting the cybercrime. Besides internal factors, external obstacles include the illegal nature of the technology used in cyberspace, constituting transnational crimes against the government of the United States.

The efforts of investigators to overcome obstacles during the investigation process include conducting cyber patrols aimed at monitoring cyber activities. Thus, upon identifying suspicious activities, investigations can promptly commence without waiting for victim reports. Given the low reporting rates in cybercrime, the role of experts is crucial in detecting and preventing cybercrime, particularly law enforcement agencies well-versed in various forms of cybercrime, including scampage. However, due to the involvement of multiple countries in scampage crimes, the Cyber Unit of East Java Regional Police's second effort to address these obstacles involves collaborating with the United States government, specifically the Federal Bureau of Investigation (FBI). This mutual effort benefits both parties, as the victims of the actions by two Indonesian citizens, SFR and MZ, are the government and citizens of the United States. In this case, the East Java Regional Police's Criminal Investigation Directorate directly received an FBI Letter of Appreciation (LOA) for successfully uncovering fake websites resembling those of the United States.

Analysis of Law Enforcement on Scampage Criminal Acts at East Java Regional Police

Based on the explanation regarding the concept of law enforcement in positive law and Islamic criminal law, along with field findings on scampage criminal cases at East Java Regional Police, the analysis or proof process regarding the elements contained in Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law) has been reached.

During the cyber patrol, the Cyber Crime Unit of East Java Regional Police's Criminal Investigation Department (Ditreskrimsus) discovered suspicious activities related to the dissemination of scampage or fake websites resembling official websites of the United States government, using the SMS Blast technique as follows: "alert from NyDMV: We are sorry to inform you due to our regulation compliant update, you must update your contact information. For more info visit: ow.ly/3ko2423ko". Clicking on the link directs users to a scampage URL, leading them to believe the site is official. The website forgery was carried out by two Indonesian citizens, SFR and MZ, at the request of S (an Indian citizen wanted by the Indian government and US citizens). Their goal was to liquidate the US government's Pandemic Unemployment Assistance funds and aid to unemployed US citizens due to the COVID-19 pandemic. This scampage crime caused the US government a loss of USD 60.000 over a period of one year. SFR gained approximately USD 30,000 (around IDR 420 million), and MZ gained IDR 60 million during their actions.

The actions of two Indonesian citizens, MZ and SFR, consciously involved creating a counterfeit website mimicking a United States government site, disseminating this fake site using the SMS Blast technique to illicitly obtain their victims' personal identity information for profit. This criminal case constitutes transnational scampage due to its involvement across multiple countries. Therefore, addressing it requires forms of coordination and cooperation between nations.

Such acts fall under criminal offenses or delicts, which, if proven to violate their elements, may result in imprisonment. In the case of scampage crimes, specific legislation governs the forgery of websites conducted through electronic media. Perpetrators in such cases are prosecuted under Article 35 in conjunction with Article 51(1) of Law Number 19 of 2016 concerning ITE (Electronic Information and Transactions).

Law enforcement in Indonesia operates through two main approaches: preventive and repressive. Prevention involves actions taken before a crime occurs to deter its commission, while repression involves responding to and processing criminal violations after they have occurred, according to applicable legal norms.

The Cyber Crime Unit of East Java Regional Police's Criminal Investigation Department (Ditreskrimsus) enforces a law against scampage through several methods: blocking, investigation, cyber patrols, and prosecution. The primary

goal of law enforcement is to maintain order in society and ensure legal certainty in cases of violations. Upholding the law aims to achieve Legal Certainty (Rechtssicherheit), Justice (Gerechtigkeit), and Utility (Zweckmassigkeit). These objectives can be effectively realized through collaborative efforts between law enforcement agencies and affected parties. Cooperation involves prompt response to law enforcement summons, providing truthful information, and readiness to assist further as needed.

Islamic Criminal Law Analysis on Law Enforcement of Scampage Crimes at East Java Regional Police

Fraud in Islamic criminal law (*fiqh jinayah*) is conceptually similar to fraud as discussed in the Indonesian Criminal Code (KUHP), encompassing any deceptive act aimed at gaining undue advantage, including lying, false oaths, and tampering with measurements. These fraudulent activities are considered jinayah (acts prohibited by Islamic law) due to their potential to harm others (Gunawan, 2022).

In enforcing *ta'zir* punishments, the government adheres to the principle of "preserving public interest and protecting every member of society from harm," ensuring that *ta'zir* enforcement aligns with Sharia principles. Scholars categorize *ta'zir* offenses into two types:

1. *Ta'zir* offenses related to the rights of Allah, involving actions detrimental to public welfare such as causing corruption on earth, robbery, theft, rebellion, adultery, and disobedience to *Ulil al-Amri*.
2. *Ta'zir* offenses affecting individual rights, and threatening the welfare of individuals, such as debt evasion and defamation (Munajat, 2004).

Characteristic features of *ta'zir* punishments include:

1. Indeterminate and unrestricted penalties, implying punishments not explicitly stipulated by Sharia with flexible limits.
2. Determination of punishments lies within the authority of the ruler (*Ulil al-Amri*) (Marsaid, 2020).

Someone who commits *jarimah* jinayah or a criminal act can be punished if its elements are fulfilled. These elements are divided into two categories: general elements applicable to all offenses and specific elements applicable to each offense, differing between offenses.

The general elements include:

1. *Al-rukn al-syar'iy* (formal element): The presence of authoritative Islamic texts explicitly prohibiting fraud and detailing punishments for perpetrators of fraud.
2. *Al-rukn al-maddy* (material element): The actual act or deed demonstrating the commission of fraud, supported by strong evidence.
3. *Al-rukn al-adaby* (moral element): The perpetrator of fraud must be mukallaf, meaning they are mature individuals capable of being held accountable for their actions (Gunawan, 2022).

These elements are present in instances of *jarimah* or *jinayah*, as failure to fulfill any of these elements precludes categorizing the event as a *jarimah* or *jinayah*. Scampage cybercrimes in this study satisfy both general and specific elements, thus allowing for *ta'zir* punishment.

Based on the chronology previously outlined, the sanction for perpetrators of scampage cybercrimes under positive law is governed by Article 35 in conjunction with Article 51(1) of Law Number 19 of 2016 concerning Electronic Information and Transactions (ITE Law). This entails a maximum prison sentence of 12 years and/or a fine of up to IDR 12,000,000,000 (twelve billion Indonesian Rupiah). While fraud itself is not explicitly described in the texts or legal evidence of the Quran and Hadith, analyzing the elements contained in the Fraud Article above confirms its inclusion as conduct against the law, automatically contradicting societal norms.

Islam permits *ra'yu*, or methods of establishing punishment not derived from explicit textual evidence in the Quran and Hadith, while adhering to general principles and sources of Islamic law. Qiyas serves as a means to determine such punishments through juristic reasoning conducted by scholars (Ulama).

The sanctions imposed in *ta'zir* punishments vary from the lightest to the most severe, including imprisonment, confinement, exile, admonition, warning, and even capital punishment, among others. Meanwhile, under general fraud provisions, sanctions typically involve imprisonment and fines, aligning with Islamic law. The key difference lies in the purpose of imposing sanctions: in Islamic law, sanctions aim to provide greater assurance as they are not explicitly defined but rather left to the discretion of the judge to determine. It allows judges to weigh the severity of the punishment based on the offender's actions and the consequences caused.

The punishment administered is in the form of *ta'zir*, intended to educate offenders to prevent recidivism and deter others from following their example. In this context, the principle of imposing *ta'zir* punishments rests entirely with the government (*Ulil Amri*), meaning judges or the government have the authority to decide on penalties.

Based on the above explanation, positive law stipulates sanctions such as imprisonment and fines under Article 35 in conjunction with Article 51(1) of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 on Electronic Information and Transactions (ITE Law). Therefore, these positive law sanctions indirectly reflect similarities with the category of *ta'zir* punishments mentioned in the Quran, although the specific acts violated do not have explicit sanctions defined. The various forms of *ta'zir* sanctions outlined above, ranging from light to severe, including imprisonment and fines, are thus considered consistent with *ta'zir*, to be determined by the judge's discretion in adjudicating the case.

CONCLUTION

Law enforcement against scampage crimes by the Cyber Unit of Criminal Investigation Bureau (Ditreskrimsus) East Java Regional Police has successfully achieved legal certainty, justice, and utility. These efforts consist of two main approaches: firstly, preventive measures through cyber patrols to preempt similar cases before formal reports from victims; secondly, punitive actions utilizing Article 35 in conjunction with Article 51(1) of the Information and Electronic Transactions Law to legally pursue offenders.

This law enforcement also reflects principles of Islamic criminal law, where sanctions imposed on scampage offenders resemble *ta'zir* punishments. These penalties aim at both educational and corrective purposes, with judges granted full authority to determine sentences according to case-specific needs.

To enhance law enforcement effectiveness, synergy between the police and the community is crucial in raising awareness about the dangers of scampage. Active community participation in reporting scampage crimes in their surroundings is pivotal. Moreover, given the transnational nature of cybercrimes, international cooperation and inter-country coordination are essential for effectively combating this phenomenon.

REFERENCES

Anggraeny, I., Monique, C., Wardoyo, Y. P., & Slamet, A. B. (2022). The Urgency of Establishing Guidelines for Handling Cybercrime Cases in the Indonesian National Police Department. *KnE Social Sciences*, 349–359. https://doi.org/10.18502/kss.v7i15.12107

Arief, Barda Nawawi. (1998). *Beberapa Aspek Kebijakan Penegakan Hukum dan Pengembangan Hukum Pidana*. Bandung: Citra Aditya Bakti.

Arief, Barda Nawawi.(1998). *Beberapa Aspek Kebijakan Penegakan Hukum dan Pengembangan Hukum Pidana*.Citra Aditya Bakti.

Friend, Catherine, Lorraine Bowman Grieve, Jennifer Kavanagh, dan Marek Palace. (2022). Fighting Cybercrime: A Review of the Irish Experience. *International Journal of Cyber Criminology* 14 (2). https://cybercrimejournal.com

Gulo, Ardi Saputra, Sahuri Lasmadi, dan Khabib Nawawi.(2020). Cyber Crime dalam Bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik. *PAMPAS: Journal of Criminal Law* 1(2). https://online-journal.unja.ac.id

Gunawan, Hendra. (2018). Tindak Pidana Penipuan dalam Perspektif Fikih Jinayah." *Jurnal El-Qanuny* 4(2). http://jurnal.iain-padangsidimpuan.ac.id

Hamsin, M. K., Halim, A., & Anggriawan, R. (2023). Addressing Cybercrime in the Sharia Digital Wallet Industry: A Legal Perspective in the Indonesian Context. *E3S Web of Conferences*, *440*, 04016. https://doi.org/10.1051/e3sconf/202344004016

Jatimpos. (2021, April 15). *Polda Jatim Bongkar Pembuat dan Pengedar Scampage atau Website Palsu Cairkan Dana PUA Warga AS*. https://www.jatimpos.co/kriminal/5103-polda-jatim-bongkar-pembuat-dan-pengedar-scampage-atau-website-palsu-cairkan-dana-pua-warga-as

Marsaid.(2020). *Al-Fiqh Al-Jinayah (Hukum Pidana Islam)*. Cetakan I. Palembang: Rafah Press.

Mertokusumo,Sudikno.(1999). *Mengenal hukum.*Liberty.

Merwe, Alta van der, Marianne Loock, dan Marek Davrowski. (2005) *Characteristics and responsibilities involved in a Phishing attack*. *WISICT'05: Proceedings of the 4th international symposium on information and communication technologies*. Trinity College Dublin. https://dl.acm.org/doi/10.5555/1071752.1071800

Moeljatno.(2008). *Asas-Asas Hukum Pidana*. Jakarta: PT Rineka Cipta.

Mohd Zaharon, Nur Farhana, dan Mazurina Mohd Ali. (2021).Phishing as Cyber Fraud: The Implications and Governance. *Hongkong Journal of Social Science* 57.http://hkjoss.com

Muhaimin.(2020). *Metode Penelitian Hukum*. Mataram: Mataram University Press.

Munajat, Makhrus. (2004). *Dekonstruksi Hukum Pidana Islam*. Yogyakarta: Logung Pustaka.

Niken Charisa .(2022). Wawancara, Surabaya, 14 Februari 2022, Pukul 12.24 WIB.

Nursita, Rizki Dian. (2019). Cyberspace: Perdebatan, Problematika, serta Pendekatan Baru dalam Tata Kelola Global. *Dauliyah* 4(1). https://ejournal.unida.gontor.ac.id

Okpa, John Thompson, Benjamin Okorie Ajah, dan Joseph Egidi Igbe.(2020). Rising Trend of Phishing Attacks on Corporate Organisations in Cross River State, Nigeria. *International Journal of Cyber Criminology* 14(2). https://cybercrimejournal.com

Pancasilawati, Abnan.(2013). Penegakan Hukum Dalam Syari'at Islam. *Journal IAIN Samarinda* https://journal.uinsi.ac.id

Rahardjo, Satjipto.(2009). *Penegakan Hukum: Suatu Tinjauan Sosiologis*. Yogyakarta: Genta Publishing.

Rizky, F. A., Mualimin, J., & Nurhasanah, S. (2023). Digital Marketing, Cybercrime, and Islamic Business Ethics A Case Study in Indonesia. *AB-JOIEC: Al-Bahjah Journal of Islamic Economics*, *1*(2), Article 2. https://doi.org/10.61553/abjoiec.v1i2.68

Rumlus, Muhamad Hasan, dan Hanif Hartadi. (2020). Kebijakan Penanggulangan Pencurian Data Pribadi dalam Media Elektronik. *Jurnal HAM* 11(2). https://ejournal.balitbangham.go.id

Saudi, Ahmad.(2018). Kejahatan Siber Transnasional dan Strategi Pertahanan Siber Indonesia. *Jurnal Demokrasi & Otonomi Daerah* 16(3). https://jdod.ejournal.unri.ac.id

Sinaga, M. I. J. (2022). Penetapan Tersangka dalam Penyidikan Tindak Pidana Transnational Cybercrime Menurut Sistem Hukum di Indonesia. *Syntax Literate ; Jurnal Ilmiah Indonesia*, *7*(3), 1229–1253. https://doi.org/10.36418/syntax-literate.v7i3.6430

Soekanto, Soerjono (1983). *Faktor-Faktor yang Mempengaruhi Penegakan Hukum*. Jakarta: Rajawali Pers.

Suparjo, S., & Hidayah, L. N. (2023). Islamic Religious Education in Indonesia: Understanding the Urgency and Paradigm Shift from a Societal Perspective. *International Journal of Multidisciplinary Research and Analysis*, *06*(06). https://doi.org/10.47191/ijmra/v6-i6-08

Syarbaini, A. (2019). Teori *Ta'zir* dalam Hukum Pidana Islam. *Ius Civile: Refleksi Penegakan Hukum Dan Keadilan*, *2*(2), Article 2. https://doi.org/10.35308/jic.v2i2.967

Wahid, Abdul, dan Mohammad Labib.(2005). *Kejahatan Mayantara (cyber crime)*. Bandung: Refika Aditama.