

TA'ZHIR LAW AS AN ALTERNATIVE SANCTION TO CYBERCRIME LAW (CASE STUDY OF CYBERCRIME LAW IN INDONESIA)



Muhamad Al Amin¹, Hendri Zola Efendi², Ferik Demiral³

*Correspondence :

Email :

alamanbm1930@gmail.com

Authors Affiliation:

¹²³State Islamic University Sjeh
M. Djamil Djambek Bukittinggi,
Indonesia

Article History :

Submission :

Revised :

Accepted :

Published

Keyword : *Ta'zhir, Sanction,
Cyber Crime*

Kata Kunci : *Ta'zhir, Sanksi,
Kejahatan Siber*

Abstract

Cyber crime is a new crime phenomenon that emerges along with the rapid development of technology, cyber crime is a form of crime that is not bound by a particular place and country. Cyber crime is also a sign that the law must be present to provide legal certainty for every citizen. Islamic criminal law does not clearly regulate cybercrime, so the determination of sanctions and penalties can only be done with ta'zhir punishment known in Islamic criminal law. Legislation of cybercrime law certainly cannot be separated from the concept of ta'zhir that has existed before. This research is conducted to see how ta'zhir can be used as an alternative in providing sanctions in the legislation of electronic information and transaction laws. The research conducted by the author finds the fact that ta'zhir punishment can be used as an alternative in providing sanctions for cyber criminals with several advantages offered, namely the flexibility and adaptive nature of ta'zhir punishment with changing situations, as well as making sanctions that have been legislated in the law with two changes as a deterrent effect and also as a form of teaching to the perpetrator and as a preventive for others not to commit acts of cyber crime. Ta'zhir punishment is also considered to be in line with the demands of the law, which is to bring justice and benefit to all people.

Abstrak

Kejahatan siber merupakan fenomena kejahatan baru yang muncul seiring dengan perkembangan teknologi yang semakin cepat, kejahatan siber merupakan bentuk kejahatan yang tidak terikat dengan tempat dan negara tertentu. Kejahatan siber juga menjadi tanda bahwa hukum harus hadir untuk memberikan kepastian hukum bagi setiap warga negara. Hukum pidana Islam tidak mengatur secara gamblang kejahatan siber ini, sehingga penentuan sanksi dan hukuman hanya bisa dilakukan dengan hukuman ta'zhir yang dikenal dalam hukum pidana Islam. Legislasi hukum kejahatan siber tentu tidak dapat dilepaskan dengan konsep ta'zhir yang telah ada lebih dahulu. Penelitian ini dilakukan untuk melihat bagaimana ta'zhir dapat dijadikan sebagai alternatif dalam pemberian sanksi dalam pelegislasian undang-undang informasi dan transaksi elektronik. penelitian yang penulis lakukan mendapati fakta bahwa hukuman ta'zhir dapat dijadikan sebagai alternatif dalam pemberian sanksi bagi pelaku kejahatan siber dengan beberapa keunggulan yang ditawarkan yaitu fleksibilitas dan sifat adaptif hukuman ta'zhir dengan perubahan situasi, serta mejadikan sanksi yang telah dilegislati dalam undang-undang dengan dua kali perubahan sebagai efek jera dan juga sebagai bentuk pengajaran kepada pelaku dan sebagai preventif bagi orang lain untuk tidak melakukan tindakan berupa kejahatan siber. Hukuman ta'zhir juga dianggap sejalan dengan tuntutan hukum yaitu mendatangkan keadilan dan kemaslahatan bagi semua orang

INTRDUCTION



Cybercrime is one of the impacts arising from massive technological advances in recent decades, one of these negative impacts can be traced to the development of criminal acts both in the real world and in the cyber world. The expansion of the types of crimes also requires the law to be present and take action and provide strict sanctions for cyber criminals. Clear legal certainty will certainly greatly impact everyone involved in cyber-based activities to be able to carry out their activities with a sense of security because they have a strong legal basis, as well as a warning for everyone to be wise and careful in carrying out every cyber-based activity and become a control suggestion not to commit various cyber-related criminal acts.¹

The massive and relatively fast cyber development also requires the government to be adaptive to the changes that occur, this adaptive attitude is shown by the government by issuing clear regulations in Law Number. 11 of 2008 concerning information and electronic transactions which was later revised with the birth of Law Number. 19 of 2016 concerning the first amendment to Law Number. 11 of 2008, relatively fast changes also guarantee the existence of legal certainty that is increasingly established, especially in the Cyber space, this legal certainty is also complemented by accommodating issues related to information and electronic transactions in Law Number. 1 of 2024 concerning the second amendment of Law Number. 11 of 2008.²

The rapid changes related to the issue of information and electronic transactions if examined through the perspective of Islamic criminal law, it can be traced that cyber crimes that have emerged recently are not specifically regulated in Islamic criminal law. The author sees that the rapid changes related to the legislation of the ITE Law in Indonesia can be seen from the perspective of *ta'zhir* punishment, by analyzing the ITE Law descriptively-normatively to see how the determination and application of the ITE Law is in line with the concept of Islamic criminal law with the principle that the law provides certainty and a sense of justice for every party involved, so on this basis *ta'zir* law is present as one of the alternative solutions to accommodate progress in the criminal field, especially crimes that arise due to technological advances such as cyber crimes.

METHODS

The research conducted by the author is qualitative research by collecting various data that are primary, secondary and tertiary. The research approach that the author takes is a library research or literature approach by collecting various available literature to then be analyzed as an effort to see how *ta'zhir* law can be an alternative solution in sanctioning cyber-related crimes, how changing conditions and rapid technological advances still make *ta'zhir* punishment as an alternative with the various advantages it offers, in order to draw conclusions that are comprehensive and thorough.

RESULT AND DISCUSSION

Ta'zhir Law

Islamic criminal law stipulates three types of punishment (*uqubat*) as an implication of the occurrence of criminal offense (*jinayah*). Some forms of *punishment* in Islamic criminal law are, *first*, *hudud*, whose form and implementation are regulated by *Shari 'ah* and become the absolute right and inviolable. *Second*, *Qishas* and *diyat*, which are the rights of the servant due to criminal acts that harm others and become the rights of the servant. *Third*, *ta'zhir* which regulates all things that have not been regulated or determined by the *nash* regarding the form and type of punishment. The form of *ta'zhir* also varies, but the determination is left to the Government or the authorities.³

¹ Herry Saputra Siti Kurnia Rahayu, Siti Ruqoyah, Sanniyah Berliana, Sekar Budi Pratiwi, "Cybercrime Dan Dampaknya Pada Teknologi E-Commerce," JISAMAR, n.d., 632–37, <https://doi.org/10.52362/jisamar.v5i3.478>.

² Nita Maharani Harahap, "Resiko Kejahatan Teknologi Dan Informasi Cyber Crime Dan Analisis Inovasi Pencegahan Resiko Cyber Crime Di Indonesia" 3 (n.d.): 52–59.

³ Rokhmadi, *Hukum Pidana Islam* (Semarang: Karya Abadi Jaya, 2015). 27

Ta'zhir punishment is linguistically taken from the word *azara* which means preventing, maintaining, educating, helping and strengthening. Specifically, *ta'zhir* is defined by Al-mawardi with a type of punishment that is educational for sinful acts (*sin*) whose punishment has not been determined by *shara'*. In understanding the term *Ta'zhir*, Al-mawardi concluded that the meaning of *ta'zhir* is most suitable for use to define this term with the meaning of educating, it can also be understood that *ta'zhir* as a form of education that prevents the perpetrator not to repeat the act. This opinion is in line with the opinion put forward by Wahbah Zuhaili and Abdul Qadir Audah that the educational aspect is the main aspect to be achieved by the implementation of this *ta'zhir* punishment. The definition of *ta'zhir* put forward by Al-mawardi is also an illustration that related laws that are not regulated by *nash* both the Qur'an and Sunnah must be held in line with the will of *shari'a* that wants the benefit and the preservation of the principles of *maqashid shari'ah* for every human being. *Ta'zhir* punishment must be carried out by a strong authority and is considered capable of carrying it out, so in this case *ulil amri* plays its role and function as a party capable of carrying out *ta'zhir* punishment to realize the overall benefit for all people.⁴

The legality of the existence of *ta'zhir* punishment also comes from the hints of *nash* in the Qur'an as found in Surah An-nisa verse 16 which implies that it is permissible for the husband to punish his wife for the misconduct committed by his wife, as well as other hints such as those found in Surah An-nisa verse 34 which implies that it is permissible for the husband to beat his wife with the aim of providing good teaching to the wife. This indicates that the husband has the authority to punish his wife for her misconduct. Another clearer indication is mentioned in Surah An-Nisa verse 59, that the obligation to obey *ulil amri* is a command from *Shari'* itself. So the obligation to obey *ulil amri* implies that humans are bound by the laws and regulations set by *ulil amri*, especially on various issues that are not regulated in the Qur'an and Sunnah, so this kind of law is the authority of *ulil amri* as the owner of the authority in establishing laws that are binding and force everyone to obey and obey. The presence of *ulil amri* becomes a necessity so that the laws stipulated have a strong binding force for the people governed by the laws that have been made and determined.⁵

In looking at these types of *ta'zhir*, the scholars divide *ta'zir* into two forms:⁶

1. *At-ta'zir ala Al-ma'asi*, To sin is to do something that is forbidden by *sharee'ah* and not to do something that is prescribed by *sharee'ah*. The stipulation of *ta'zhir* is imposed on the types of sin for which neither *hadd* nor *expiation* is prescribed, whether the sin involves the rights of Allah or the rights of the slave. For example, immoral acts are not only related to divine rights but also to individual rights. Another example is the *Shariah* stating that prayer is obligatory, therefore if someone fails to pray, then the offender will be punished by *ta'zir*, because this kind of sin is not found in the text which explicitly states the form and amount of punishment.
2. *At-ta'zir li Al-maslahah Al-ummah*. *Ta'zhir* punishment in this form is usually imposed on people who disturb and damage the interests, order and public benefit. The Prophet once imprisoned a man who was accused of stealing a camel. However, when the accused was not proven to have stolen the camel, the Prophet released him. Based on the Prophet's actions, the scholars argue that imprisonment is a form of *jarimah takzir* to maintain public order in Medina at that time. This type of *ta'zhir* can also be applied to acts that are not classified as sinful but because they are not forbidden by *sharia* but are prohibited because they can disturb public order and punishment is given to the perpetrator for violating it, such as the right to

⁴ M Nurul Irfan and Masyrofah, *Fiqih Jinayah* (Jakarta: AMZAH, 2013). 138

⁵ Ismail Rumadhan, *Pembaharuan Jarimah Dalam Fiqih Jinayah* (Surabaya: Nariz Bakti Mulia, 2013). 46

⁶ Irfan and Masyrofah, *Fiqih Jinayah*. 141

own a firearm which is considered illegal if it does not have official permission from the authorized institution.

Ta'zhir punishment determined by the party authorized to determine it, namely the government, can include several types of punishment, namely *first*, the death penalty, the Hanafi school of thought states that it is permissible to impose the death penalty for criminals who commit repeated acts after being punished ta'zhir with other punishments, while according to the Maliki, Shafi'i and Hanbali schools of thought, the death penalty can only be imposed on homosexual offenders because there is a text that states the permissibility of homosexual offenders to be sentenced to death whether the perpetrator is *muhsan* or *ghairu muhsan*. *Second*, flogging, in giving flogging punishment, scholars differ in their opinion regarding the maximum limit of this punishment, Abu Hanifah said that the maximum number of lashes for ta'zhir is only 39 times, while other madhhabs argue that the number of lashes due to ta'zhir punishment cannot exceed the number of lashes on jarimah qazaf, namely 80 lashes. *Third*, imprisonment, in determining the minimum limit of this prison sentence, the Shafi'i school of thought views that imprisonment should not exceed the limit of one year which is the maximum time of had adultery, in viewing imprisonment as had adultery, Hanafi scholars state that imprisonment is not a had punishment, but a form of ta'zhir punishment so there is no maximum limit. *Fourth*, the punishment of crucifixion, this type of punishment can only be applied to the crime of al-hirabah as a form of teaching and public announcement of guilt.⁷

Ta'zhir punishment determined by *ulil amri* which in this case is the legitimate government of a particular region can implement this punishment in accordance with the mechanisms that apply in their respective regions, Indonesia as a country with a presidential system recognizes the division of power into executive, legislative and judicial.⁸ This division of institutions also affects how ta'zhir punishment is formed and applied. The legislative institution as the holder of power in legislating the law starting from planning, drafting, discussing and authorizing or stipulating the law to then be approved together with the executive institution to be applied in Indonesia and become public property and is open and binding for every citizen.⁹

Cybercrime

The term cybercrime can be interpreted as an unlawful act by using means or relating to computer systems or networks illegally by offering, distributing information through means of computer systems or networks. Cyber crime can also be understood as a crime that uses information technology and is a form of transnational crime that does not recognize national borders, non-violence, no physical contact and anonymous. The expansion of cybercrime is not only related to computers, but can also be related to any electronic device that can be used as a means of arising criminal acts either directly or indirectly by utilizing the network as the main means in this crime.¹⁰ The characteristics of cybercrime that make the perpetrators of cybercrime very difficult to trace and the criminal elements are difficult to prove, especially the limitations of regulations and the rapid development of technology make regulations governing this type of crime still limited.

Cybercrime is divided into several forms of crimes and criminal offenses, namely:

⁷ Vichi Novalia et al., "Ta'zhir Dalam Pidana Islam: Aspek Non Material," *Terang: Jurnal Kajian Ilmu Sosial, Politik Dan Hukum* 1 (2024): 225–34, <https://doi.org/10.62383/terang.v1i2.222>.

⁸ Widyati, *Negara Hukum, Konstitusi Dan Pembentukan Peraturan Perundang-Undangan* (Semarang: Unisulla Press, 2016). 32

⁹ Abdul Qadir Audah, *Islam Dan Perundang-Undangan* (Bulan Bintang, 1959).

¹⁰ Harahap, "Resiko Kejahatan Teknologi Dan Informasi Cyber Crime Dan Analisis Inovasi Pencegahan Resiko Cyber Crime Di Indonesia."

1. Unauthorized Access to Computer System and Service, Crimes committed by entering or infiltrating a computer network system illegally, without permission or without the knowledge of the owner of the computer network system he entered. Usually the perpetrator (hacker) does it with the intention of sabotage or theft of important and confidential information.
2. Illegal Content, It is a crime to enter data or information into the internet about something that is untrue, unethical, and can be considered unlawful or disturbing public order. For example, the posting of a hoax or slander that discredits the dignity or self-esteem of another party or matters related to pornography or the posting of information that is a state secret, agitation and propaganda against the legitimate government, and so on.
3. Data Forgery, It is a crime of falsifying data on important documents stored as scriptless documents (low security documents) over the internet. This crime is usually aimed at e-commerce documents by making it appear as if a typo has occurred which will ultimately benefit the perpetrator.¹¹
4. Cyber Espionage, It is a crime that utilizes the internet network to conduct spying activities on other parties, by entering the target party's computer network system. This crime is usually aimed at important documents or data stored in a computerized system.
5. Hacking, Hacking is a form of breach. This crime is the unauthorized use or access to computer or network resources to exploit identified security vulnerabilities in the network. Hacking can be used to collect personal data or information which is used for Criminals to damage websites or used as part of a denial of service by flooding internet Servers with so many requests, for example, links that have been clicked that the computer cannot respond fast enough so it can overload the server causing it to crash (overload) on the network or the network becomes completely paralyzed. Another commonly encountered mode is to send an OTP (on time password) by posing as a party from a certain institution to hack the victim's device. This type of crime also includes skimming after hacking into someone's account to steal financial-related data and conduct illegal transactions using that data.¹²
6. Spam, Spam is unsolicited email (electronic mail), this mail is usually sent in bulk to countless recipients around the world and is often associated with certain products. Spam emails are also used to send emails for the purpose of phishing (fraud to steal someone's personal data) by sending malware (viruses) that can help maximize the potential profit for criminals either to perform extortion, steal money, or sell personal data that has been stolen for a specific purpose.
7. Semantic attacks, Semantic attacks are data modification and dissemination of personal information. The modified information can be done without the use of a computer although new opportunities can be found by using a computer. To set someone in the wrong direction or to cover tracks, the dissemination of false information can be used for various other cyber-related crimes.
8. Cyberattacks, Cyber attacks are a type of offensive maneuver used by countries, individuals, groups, or organizations that target computer information systems, infrastructure, computer networks and or personal computer devices by various means of malicious actions, altering or destroying the specified target by breaking into vulnerable systems. This act can be labeled as cyberterrorism in a different context because the target of this criminal act is much broader and can attack certain institutions or even a country by destroying network infrastructure to have a large and massive impact.¹³

¹¹ Cahyo Hidayatullah, "Jenis Dan Dampak Cyber Crime," *Proceeding Saintek* 2 (2023): 216–21.

¹² Muhammad Antoni Aldriano and Mas Agus Priyambodo, "Cyber Crime Dalam Sudut Pandang Hukum Pidana," *Jurnal Kewarganegaraan* 6 (2022): 2169–75.

¹³ Hidayatullah, "Jenis Dan Dampak Cyber Crime."

Cyber crime also has various negative impacts arising from this crime, both small-scale negative impacts and large-scale negative impacts, namely:

- a. In e-commerce, the use of e-commerce applications is affected by cybercrime. Cybercrime causes various losses for both application developers and users, this negative impact certainly causes a lack of user confidence in the e-commerce concerned, besides the risk of losing customer data can also harm the e-commerce application developer as well as various attacks on application security that can harm the parties involved in this e-commerce.¹⁴
- b. Impact on banking, the results of this study indicate that financial institutions contain a higher risk of crime than other institutions. The more customers who utilize internet banking facilities can provide opportunities for cybercrime perpetrators to commit crimes against customers. Given that today is the digital era, so that more and more people are utilizing their expertise in using technology and not a few of them are actually misusing the technology.¹⁵
- c. The potential loss of a country's state data is also one of the negative impacts of this type of cyber crime, which can disrupt the sovereignty of a country if state data can be accessed and hacked by unknown parties.
- d. Loss of data and privacy, one of the risks of cybercrime is the potential loss of personal data due to being hacked with various types of hacks which also have the potential to eliminate the privacy of the network owner itself. The risk of losing personal data without the owner realizing it can be misused by irresponsible parties, causing losses.¹⁶

This cybercrime uses internet access that does not only occur within a region but can be done outside the territory of the region, this becomes an obstacle in the investigation by the authorities because the authority of the institution is sabotaged by territories with different jurisdictions. Another obstacle in handling cybercrime in Indonesia is the limited number of experts in conducting investigations, which is a factor that affects the success of police officers in eradicating cybercrime cases, with a very minimal number of expert members being a stone obstacle in eradicating cybercrime cases that cannot be resolved in an efficient time. The existing obstacles do not make efforts to improve laws related to cybercrime stop running, but continue to run in line with the development of cybercrime that continues to move.

Ta'zhir Law as An Alternative Sanction To Cybercrime Law in Indonesia

Cybercrime has started to increase since the rapid development of technology, especially at the beginning of the 21st century, the significant development of the cyber world has made the gaps for crime and crime in the cyber world also open. The vulnerability of cyber security is also utilized by irresponsible parties to commit various forms of cybercrime. In Indonesia, studies on cybercrime have been conducted by the Research and Development Center for Law and Justice of the Indonesian Supreme Court since 2004 with the publication of an academic paper on cyber crimes. The study conducted by the Supreme Court was also followed up by the Ministry of Communication and Information by issuing a cybersecurity strategy Permen Kominfo No.26/PER/M.Kominfo/5/2007 on the security of the use of internet protocols of technology-based telecommunications networks which was later established into Kominfo regulation No.16/PER/M.Kominfo/10/2010, which was then

¹⁴ Siti Kurnia Rahayu, Siti Ruqoyah, Sanniyah Berliana, Sekar Budi Pratiwi, "Cybercrime Dan Dampaknya Pada Teknologi E-Commerce."

¹⁵ Suharyadi, Said Sambara, and Kamri Ahmad, "Kejahatan Dunia Maya (Cyber Crime) Dalam Perspektif Hukum Islam," *Journal Of Lex Generalis (JLS)* 1 (2020): 761–73.

¹⁶ Hidayatullah, "Jenis Dan Dampak Cyber Crime."

updated again through the regulation of the Minister of Transportation and Kominfo No.29/PER/M.Kominfo/12/2010.¹⁷

The development of cyber crime which is a type of crime that is not mentioned and not regulated in Islamic criminal law makes ta'zhir punishment a solution in providing sanctions for cyber criminals in Indonesia. The discussion of Islamic criminal law that highlights the existence of *ta'zhir* punishment makes it possible for the discussion of cyber crime to be accommodated by the concept of ta'zhir. Cybercrime in the perspective of ta'zhir can be seen from two different perspectives of ta'zhir, cybercrime can be considered as a form of *ta'zhir li al-ma'ashi* because it is contrary to Islamic law itself, cybercrimes such as theft of personal data and other important data and theft of money through networks can be considered as a form of immorality, other forms of immorality that may arise from cybercrime are acts of extortion and the spread of illegal content such as the spread of pornographic content or the spread of fake news that causes commotion and unrest in the community. If cybercrime is viewed from the form of *ta'zhir li al-maslahah al-ammah*, then cybercrime is clearly detrimental to public interests and disturbs public peace, even on a wider scale it can harm the state due to cybercrime such as sabotage, hacking and various other cybercrimes. Cybercrime in the context of Islamic criminal law, especially in the discussion of *ta'zhir*, has enough conditions to determine the punishment denied.

Islamic criminal law has the spirit of justice and brings goodness to everyone who is bound by it, these basic principles also apply to conventional criminal law, but the factor that makes the two different is the basic foundation of both, Islamic criminal law is built on the basic principles of Islamic shari'a while conventional criminal law is only based on considerations of goodness alone. It is an undeniable reality that both types of law can also be integrated to accommodate the needs of the law that continues to grow as long as both run with the same principles and do not collide with each other.¹⁸ Ta'zhir punishment can also be used to deal with any crime that arises, but in the scope of cybercrime, ta'zhir law can be applied for the following reasons.

1. Flexibility in dealing with various crimes, ta'zhir punishment which is not clearly defined regarding the type of punishment and what crimes should be punished makes ta'zhir punishment important in dealing with various modern problems such as cybercrime that continues to develop. This undefined ta'zhir punishment becomes a kind of gap for the government to formulate regulations related to cybercrime in accordance with its development. The growing cybercrime has made the government pass Law Number 11 of 2008 concerning Information and Electronic Transactions, in this Law the forms of cybercrime are regulated in Chapter VII from Article 27 to Article 37. In general, this law has regulated the prohibition of disseminating information that violates decency, gambling, defamation and extortion and threatening in article 27. Other forms of crime that are also regulated are the prohibition of spreading fake news and news that can trigger conflict in the community contained in article 28. These two articles focus on discussing the content that is spread, while article 29 discusses the prohibition of sending threats of violence and fear through cyberspace. Other articles in this Law have also touched on forms of cybercrime such as hacking, sabotage, as well as discussing prohibitions related to electronic data, such as stealing data, eliminating data, changing data and disseminating data. Since its enactment in 2008, the ITE Law has undergone two amendments and improvements, namely:¹⁹
First, the issuance of Law Number. 19 of 2016 concerning the amendment of Law Number. 11 of 2008 and the addition of several new forms of crime that have not been accommodated such as

¹⁷ Harahap, "Resiko Kejahatan Teknologi Dan Informasi Cyber Crime Dan Analisis Inovasi Pencegahan Resiko Cyber Crime Di Indonesia."

¹⁸ Marsaid, *Al-Fiqh Al-Jinayah* (Palembang: Rafah Press, 2020). 78

¹⁹ Aldriano and Priyambodo, "Cyber Crime Dalam Sudut Pandang Hukum Pidana."

the existence of article 28 paragraph (1) which states “prohibits every person intentionally, and without the right to spread false and misleading news that results in consumer harm in electronic transactions”. This article is generally an expansion of article 28 in Law Number. 11 of 2008 which does not regulate the rights of consumers to obtain correct information, this article is intended to regulate transactions in e-commerce applications that have begun to emerge and develop since 2014. In addition, Article 27 paragraph (3) and Article 28 are also considered as rubber articles and can cause multiple interpretations, so they were revised in Law Number.19 of 2016. This flexibility makes ITE Law develop to accommodate the various changes that occur in the fast-paced cyber world. The amendment of Law No. 11 of 2008 into Law Number. 19 of 2016 is a response to the community's desire to clarify and perfect the articles that have existed in the previous law.

Second, the second revision to perfect the existing ITE Law was again carried out through Law No. 1 of 2024 by agreeing on changes to several articles and the addition of 5 articles to the second amendment to Law Number. 19 of 2016. These changes include electronic evidence (contained in Article 5), electronic certification (Article 13), electronic transactions (Article 17), prohibited acts (Article 27, Article 27 (a), Article 27 (b), Articles 28-29, and Article 36) and criminal provisions (Article 45, Article 45 (a), Article 45 (b)). The amendments to this Law also complement the material around digital identity in the implementation of electronic certification, child protection in the implementation of electronic systems, international electronic contracts and the role of the government in encouraging the birth of a fair, accountable, safe and innovative digital ecosystem. This relatively rapid change of less than ten years shows that the rapid changes to the changes and the various interpretations of the articles in the previous law make changes and additions to some provisions as part of the flexibility of ta'zhir punishment in responding to the times.

2. In addition to having a strong deterrent effect, the criminal sanctions imposed on cyber criminals in the form of imprisonment and fines also have a deterrent effect on criminals. Islamic criminal law as a living law means that criminal sanctions provide a deterrent effect for criminals as well as a warning for others who do not do it to stay away from criminalized acts. The provision of criminal sanctions and non-criminal sanctions such as written warnings is also a sign that the act should not be done because it is contrary to existing legal norms. The theory of punish and reward makes the existence of punishment a warning not to repeat the action, while the provision of rewards can trigger a person to commit the same action repeatedly. The provision of punishment in the perspective of Islamic law is not considered as a reward, but is seen as a form of correction and provides a deterrent effect and has a repressive meaning as a threat to those who want to commit an act against the law by upholding the rule of law for everyone who tries to go against the law. Islam views punishment with a strong deterrent effect as a preventive measure because it can prevent the occurrence of unlawful acts which have implications for the birth of public benefits for all people because the presence of deterrent properties makes benefits created in the midst of society.²⁰
3. The nature of ta'zhir punishment which is educational in nature also contributes to improving behavior through the existence of electronic information and transaction laws so that everyone involved in activities in the cyber world is wiser and more careful. One concrete example of behavior improvement efforts is in the issue of defamation as contained in Law Number. 11 of 2008 in article 27 paragraph (3) concerning insults and defamation, in this article each party can report the other party if they feel defamed, with this there are many criminal cases due to mutual

²⁰ Muhammad Taufan Djafri et al., “Hukum Islam Dan Efek Jera Pemidanaan Di Indonesia,” *Bustanul Fuqaha: Jurnal Bidang Hukum Islam* 4 (2023), <https://doi.org/10.36701/bustanul.v4i1.926>.

reporting, in relation to criminal defamation can be sentenced to 4 years, but in Law Number. 1 of 2024 criminal penalties with the same case the penalty period is reduced to two years and a maximum fine of 400 million rupiah. The educational form of the birth of Law Number. 1 of 2024 is the presence of Article 45 paragraph (6) concerning slander, the presence of this article educates everyone not to easily report other people with accusations of defamation if they cannot prove the accusation then they can be punished with the offense of slander with a period of imprisonment for 4 years and a maximum fine of 750 million rupiah. Penalties related to slander that are greater than the crime of defamation make everyone more careful in reporting defamation.²¹

Ta'zhir punishment applied in the establishment of cybercrime regulations in Indonesia through the formation of legislation related to cybercrime and improvements to the law makes ta'zhir as an alternative in determining criminal sanctions against cybercrime in Indonesia, although the types of punishment imposed are imprisonment and fines that are not specifically regulated in Islamic criminal law, but the author views that criminal penalties in the form of imprisonment and fines as a form of adjustment of ta'zhir punishment with modern law, as well as a form of integration between Islamic criminal law and Indonesian criminal law.

CONCLUSION

The punishment that has been determined by Shari'ah for some forms of jarimah cannot be changed, while other types of punishment that are not specifically regulated but only discuss general principles can be changed according to the needs and interests that existed at the time the punishment was determined, this type of punishment is also called ta'zhir. The development of ta'zhir law in line with its nature, which is adaptive to various changes, is very suitable to be applied to various criminal acts that are not regulated in Islamic criminal law. One of the forms of criminal acts that have emerged lately is crime by utilizing technology and networks both to steal personal data and digital-based money theft, sabotaging a person's network or certain agencies without permission, spreading various fake news through electronic media, distributing various illegal content through electronic media, changing data, defamation and incitement by utilizing electronic media are forms of cyber crime that are prevalent.

Cybercrime that continues to grow with a variety of modes makes the presence of Law Number. 11 of 2008 concerning information and electronic transactions as an effort to protect everyone's cyber activities and punish people who are against the law with criminal threats. The ta'zhir law offered by Islamic criminal law as one of the solutions in providing sanctions for cyber criminals is evident with its flexibility in participating in revising ITE Law Number. 11 of 2008 into Law Number. 19 of 2016. The flexibility and adaptiveness of ta'zhir law again occurred with the second amendment to Law Number. 11 of 2008 into Law Number. 1 of 2024. Ta'zhir punishment is also in line with the concept of modern law, which is to create a deterrent effect as a preventive measure to prevent the recurrence of cybercrime as well as a form of repression by upholding the rule of law for every party who violates the law, besides that ta'zhir punishment is also considered as a rehabilitative effort to maintain and change the behavior of cybercrime and also as a form of education for everyone to be wise and careful in doing activities in the cyber world.

References

Book

²¹ Munir, "Kajian Pasal 27 A UU No. 1 Tahun 2024 Tentang Perubahan Kedua UU No. 8 Tahun 2008 Tentang ITE," *Fundamental: Jurnal Ilmiah Hukum* 2 (2024): 1–12, <https://doi.org/10.34304>.

- Audah, Abdul Qadir. *Islam Dan Perundang-Undangan*. Bulan Bintang, 1959.
- Irfan, M Nurul, and Masyrofah. *Fiqih Jinayah*. Jakarta: AMZAH, 2013.
- Marsaid. *Al-Fiqh Al-Jinayah*. Palembang: Rafah Press, 2020.
- Rokhmadi. *Hukum Pidana Islam*. Semarang: Karya Abadi Jaya, 2015.
- Rumadhan, Ismail. *Pembaharuan Jarimah Dalam Fiqih Jinayah*. Surabaya: Nariz Bakti Mulia, 2013.
- Widyati. *Negara Hukum, Konstitusi Dan Pembentukan Peraturan Perundang-Undangan*. Semarang: Unisulla Press, 2016.

Journal

- Aldriano, Muhammad Antoni, and Mas Agus Priyambodo. "Cyber Crime Dalam Sudut Pandang Hukum Pidana." *Jurnal Kewarganegaraan* 6 (2022): 2169–75.
- Djafri, Muhammad Taufan, Ni'man Samad, Mustaufiq, and Misbahuddin. "Hukum Islam Dan Efek Jera Pemidanaan Di Indonesia." *Bustanul Fuqaha: Jurnal Bidang Hukum Islam* 4 (2023). <https://doi.org/10.36701/bustanul.v4i1.926>.
- Harahap, Nita Maharani. "Resiko Kejahatan Teknologi Dan Informasi Cyber Crime Dan Analisis Inovasi Pencegahan Resiko Cyber Crime Di Indonesia" 3 (n.d.): 52–59.
- Hidayatullah, Cahyo. "Jenis Dan Dampak Cyber Crime." *Proceding Saintek* 2 (2023): 216–21.
- Munir. "Kajian Pasal 27 A UU No. 1 Tahun 2024 Tentang Perubahan Kedua UU No. 8 Tahun 2008 Tentang ITE." *Fundamental: Jurnal Ilmiah Hukum* 2 (2024): 1–12. <https://doi.org/10.34304>.
- Novalia, Vichi, Laudza Hulwatun Azizah, Novinda Al-islami, and Surya Sukti. "Ta'zhir Dalam Pidana Islam: Aspek Non Material." *Terang: Jurnal Kajian Ilmu Sosial, Politik Dan Hukum* 1 (2024): 225–34. <https://doi.org/https://doi.org/10.62383/terang.v1i2.222>.
- Siti Kurnia Rahayu, Siti Ruqoyah, Sanniyah Berliana, Sekar Budi Pratiwi, Herry Saputra. "Cybercrime Dan Dampaknya Pada Teknologi E-Commerce." *JISAMAR*, n.d., 632–37. <https://doi.org/https://doi.org/10.52362/jisamar.v5i3.478>.
- Suharyadi, Said Sampara, and Kamri Ahmad. "Kejahatan Dunia Maya (Cyber Crime) Dalam Perspektif Hukum Islam." *Journal Of Lex Generalis (JLS)* 1 (2020): 761–73.