



CYBER INSTITUTIONS IN HANDLING BANKING CRIMES IN INDONESIA

Putu Agung Putra Baharata¹, Putu Dima Indra²

¹ Faculty of Law, University of Jember, Jember, Indonesia

E-mail: putrabaharata@gmail.com

² Faculty of Law, University of Jember, Jember, Indonesia

E-mail: dimaindra@gmail.com

Corresponding Author: Putu Agung Putra Baharata

ABSTRACT

The formulation in the context of overcoming cyber crimes in the banking sector, where the existence of the establishment of cyber institutions within the Indonesian Police is inseparable from the cases that have hit the banking world. Online-based loans do not only have a good impact on society, but also have negative effects, such as fraudulent persons. The mode of online loan-based fraud occurs in people who are in a state of economic problems or it could also be due to negligence because the lure of easy loans and very low interest. This problem can actually be overcome by triggering factors from the community to learn and participate in pursuing the development of existing technology.

Keywords: Cyber Institutions, Cyber Crimes, Banking.

INTRODUCTION

Technological developments are currently a lot of changes and modifications to adapt to the times. With the development of technology, it is not something that must be avoided because indeed with the presence of technology, it makes it easier for all fields that were originally done manually. These changes must be realized by the community. There are not many people who are able or can be said to be technologically illiterate in public awareness of technological developments. This condition is indeed a problem for the community, especially people who do not have internet access. This problem can actually be overcome by triggering factors from the community to learn and participate in pursuing the development of existing technology. Because it is an internal factor in society that is less aware of the importance of technological developments.

The purpose of the existence of a cyber institution within the Police in Indonesia is to answer all challenges in technological developments in principle to facilitate all human activities.

With this easy access, the community can certainly use it to increase time efficiency in carrying out their activities.¹ The principle of this technology encourages people to continue learning and keep up with the times. Because indeed the development of the current era is so rapidly developing, where the speed is the driving factor is technology, both in the form of information and other electronic media.

Cyber institutions within the Police also provide information about technological developments in the form of information and electronic media which are becoming a trend in Indonesia.² This can be seen in all activities as in the economic world, especially banking, which has implemented information technology using electronic media which is vulnerable to crimes. The existence of cyber institutions within the Police, especially in the world of banking, cannot be separated from triggers. One of them is that crimes that occur in online lending today seem to flood the banking sector with the lure of an easy process and no complicated methods.³ One of the reasons for this online loan is the technological development factor. If we look at it in general, the loan process requires a long mechanism and method. Because of this, the purpose of online-based lending is to simplify and speed up the process.

RESEARCH METHODS

Research methods have an important role in providing answers to problems that are the object of research by researchers regarding the existence of cyber institutions in the context of overcoming criminal acts in the banking sector. Therefore, the research method used is normative juridical research using a statutory analysis knife as positive law in answering these problems. This study uses a statutory approach as a basis for analysis with sources from primary and secondary legal materials which will later become the problem.

RESULTS AND DISCUSSION

Basis for the Establishment of Cyber Institutions to Combat Criminal Acts in the Banking Sector in Banking

The world of banking is currently the most advanced subject of technological developments that use an electronic basis in its implementation. Of course, behind the electronic basis is a medium for the occurrence of criminal acts that are used by perpetrators for crimes. That's why we need a special institution that is focused on fighting cyber crimes in Indonesia.

The existence of the establishment of a cyber institution within the Indonesian Police is inseparable from the cases that have hit the banking world. Online-based loans do not only have a good impact on society, but also have negative impacts, such as fraudulent persons. The mode of online loan-based fraud occurs in people who are in a state of economic problems or it could

¹ Ahmad M. Ramli, 2004, *Cyber Law Dan Haki Dalam Sistem Hukum Di Indonesia*, PT Refika Aditama, Bandung. h. 9

² *Ibid.* h. 12

³ Ani Eko Wahyuni, Bambang Eko Turisno, Raden. 2019. *Praktik Finansial Teknologi Ilegal Dalam Bentuk Pinjaman Online Ditinjau Dari Etika Bisnis*, *Jurnal Pembangunan Hukum Indonesia*, 1(3), h. 108

also be due to negligence because the lure of easy loans and very low interest.⁴ This then triggers the existence of victims of fraud in which the community is urged to penetrate a certain amount of money under the pretext of the disbursement process.⁵ Such a mode by the public is often deceived by these lures. Therefore, online loans really need certification to get this legality.

The existence of cyber institutions within the Police which are formed within the Police as a repressive and preventive form related to cyber crimes as a crimes that occurs through the internet media which is so wide and free that it is prone to occur in the banking sector, so that One of the big difficulties in dealing with cybercrimes problems committed by one of the most crucial problems raised by cybercrimes is a jurisdictional issue related to the extent to which a country can apply its legal sovereignty or in other words the extent to which a country is capable of adjudicating a case with international nuances related to banking.

Cyber crimes in the banking sector in its implementation must pay attention to jurisdictional issues in a country to apply its legal sovereignty or in other words the extent to which a country's ability to hear cases with international nuances.⁶ Jurisdictional issues in this cybercrimes. Efforts that can be made are the implementation of controls carried out by existing judicial bodies and holding international agreements regarding cyberspace regulation and forming an international organization that specifically regulates cyberspace and providing a basis for self-regulation by internet users to minimize the occurrence of cybercrimes crimes.⁷ Handling of cyber crimes cases that occur are not resolved completely, for example in hacking ATMs through digital and other crimes that take actions to break through other people's programs to damage, manipulate/change and steal data and peek at customer deposits in various banks or other sensitive data centers for self gain. Although both penetrate the security of other people's computers. Illegal sites are still allowed so that this makes cyber crimes grow and get out of control.

Cyber institutions within the Police will later be able to take preventive action through the completion of illegal online-based money lending practices. This is prone to legal problems, such as online loan cases that have been found by the police, who are currently still undergoing legal proceedings involving a student from the city of Pontianak who was trapped in illegal online loans. The victim started borrowing money worth Rp. 1.4 million with a return of Rp. 1.4 million. Then the victim increased her loan to Rp. 3 million, after not paying 3 months, the online lender asked for a refund of Rp. 19 million.⁸

⁴ Rosyadi, I. 2007. "Penegakan Hukum dalam Masyarakat Indonesia". *Jurnal Sains Dan Inovasi*, 3(2), h. 79

⁵ Sari, Alfihca Rezita. 2018. *Perlindungan Hukum Bagi Pemberi Pinjaman Dalam Penyelenggaraan Financial Technology Berbasis Peer To Peer Lending Di Indonesia*, Yogyakarta: Fakultas Hukum Universitas Islam Indonesia.. h. 43

⁶ Abdul Wahid dan Mohammad Labib, 2005, *Kejahatan Mayantara (Cyber Crimes)*, Refika Aditama, Bandung, h. 18

⁷ Muladi dan Diah Sulistyani R.S., 2016, *Kompleksitas Perkembangan Tindak Pidana dan Kebijakan Kriminal*, Alumni, Bandung. h. 86

⁸ <https://www.suara.com/news/2021/10/27/144959/apes-mahasiswa-ini-utang-pinjol-rp-12-juta-setelah-3-bulan-membengkak-jadi-rp-19-juta> diakses pada tanggal 9 januari 2023.

Based on the case above as an effect of the absence of a special institution that resolves the case due to legal regulations in the context of law enforcement in online loans. On the other hand, human resources in fighting cyber crimes are not enough to use law enforcement officers in law enforcement, the legal aspects used are not concrete. because the basic legal aspects are regulated. The basis that provides legal legality for online-based money lending has been regulated based on the Financial Services Authority Regulation Number 77/POJK.01/2016 Concerning Information Technology-Based Money Lending Services and Bank Indonesia Regulation Number 19/12/PBI /2017 of 2017 concerning Implementation of Financial Technology. these two legal products as a basis for implementing online-based money lending.

The Existence of Cyber Institutions in Combating Crimes

Cyber institutions within the Police to answer cyber crimes problems that occur in the banking sector. The legal products used to regulate online-based money lending lack strong legal standing. Because regulations made by a state agency in its implementation reap many problems. The problem is that the rule of law has not been able to cover the basic rules which are actually regulated by law. Its position is so weak that when there is a problem, a similar rule is remade with the same legal position. Because of this, online-based money lending is really needed in legal protection with legal products in the form of laws.⁹

The legal issue in the implementation of online-based banking is that in the operation of services carried out by electronic media, it means that the activities carried out in online-based transactions.¹⁰ So that the legality that will be received is electronic-based by storing all data and documents in the transaction, but still the party conducting the contract is between the lender and the recipient of the loan. cyber field, Anomi theory can be used as an analytical tool to find the causes of people committing cyber crimes. The theory of anomie assumes that crimes arises because in society there are no norms governing an activity, in practice there are groups of people who reject the presence of law to regulate activities in cyberspace, virtual worlds are free spaces so that the government does not have the authority to intervene in these activities, including regulating legal means, in its implementation there is a gap between the characteristics of crimes and conventional criminal law. The characteristics of the use of the internet as a basis for activities are cross-border so that it is difficult to know the jurisdiction, even though the conventional criminal law in force in Indonesia relies heavily on territorial boundaries. The provisions of conventional criminal law are apparently not able to optimally resolve cases in activities and the internet.¹¹

Based on the neutralization theory which focuses on the aspect of the existence of actors who describe themselves as people who are powerless in dealing with societal pressures (for example, lack of affection from parents, being in bad associations or environments) and the two

⁹ Sanyoto. 2008. *Penegakan Hukum di Indonesia*. Jurnal *Dinamika Hukum*, 8(3), h. 199

¹⁰ Suprayitno, Edi dan Nur Ismawati. 2008. "Sistem Informasi Fintech Pinjaman Online Berbasis Web", Jurnal *Sistem Informasi Teknologi Informasi dan Komputer*, 9(2). h. 147

¹¹ Smith, Scott S, 2016, *Internet Crimes Report*, Federal Bureau of Investigation, Internet Crimes Complaint Center, Washington D.C. h. 119

actors are of the view that actions carried out does not cause great harm to society. cyber crimes The existence of social control theory can be used as an analytical tool to look for factors that cause people to commit cyber crimes.¹² so that the perpetrator commits a crimes because the social bond in a person is weakened or even that person no longer has social ties with the community. This happens especially among teenagers who are very vulnerable to becoming perpetrators and victims of these cyber crimes.¹³

Thus, seen from the crimes prevention policy, these non-penal efforts have a strategic position and play a key role that must be intensified and made effective. There are important steps that can be taken by each country in overcoming cyber crimes as follows:

1. By modernizing the national criminal law and its procedural law, in harmony with international conventions related to cyber crimes.
2. Improving the national computer network security system.
3. Increase the understanding and ability of law enforcement officials regarding preventive, investigative and prosecution of cases related to cyber crimes.
4. Public awareness of cyber crimes must be increased. Cooperation between countries in prevention efforts must be increased

Crimes prevention in the field of cyber where there is evidence as the main reference in avoiding the existence of a crimes, this evidence in cyber crimes making a computer a target is any action using a computer that is directed at computer data, computer systems, or computer networks, or all three together . The act was carried out in a virtual space, not a real space.¹⁴ so that all activities prohibited by laws and regulations occur in cyberspace. Evidence also plays a very important role in investigating terrorism cases, because currently communication between the perpetrators in the field and their leaders or intellectual actors is carried out by utilizing facilities on the internet to receive orders or convey conditions in the field because the perpetrators know tracking on the internet is more difficult than tracking via cellphone. .

In solving cybercrimes, it is carried out in a non-penalty way because the crimes prevention policy through the "non-penalty" channel is more of a preventive measure before the crimes occurs. Therefore, the main objective is to deal with factors conducive to the occurrence of crimes centered on social problems or conditions that can directly or indirectly give rise to or foster crimes.¹⁵

CONCLUSION

Basis for the Establishment of Cyber Institutions in Combating Crimes in the banking sector is a solution considering the existence of legal regulations that are still weak due to the mark of cases in the banking world such as the case of illegal online loans. Number

¹² Vadza, K. 2013. "Cybercrimes and its Categories". *Indian Journal of Applied Research*, 3(5), h.180

¹³ Krimiyarsi. 2015. "Criminal Law Enforcement of Cyber Porn / Cyber Sex in Order to Fighting Crimes in Indonesia". *International Journal of Business, Economics and Law*, 8, (4), h. 101

¹⁴ Hermawan, R. 2019. "Kesiapan aparaturn pemerintah dalam menghadapi cyber crimes di Indonesia". *Jurnal Media Hukum*, 6(1) h. 3-4

¹⁵ Lubis, Rini R. 2017. "Potensi Pengguna Internet Indonesia dalam Counter-Cyber Radicalization". *Jurnal Pertahanan dan Bela Negara*, 7(2)h. 29

77/POJK.01/2016 Concerning Information Technology-Based Lending and Borrowing Services and Bank Indonesia Regulation Number 19/12/PBI/2017 of 2017 concerning Implementation of Financial Technology. these two legal products as a basis for ^{implementing} online-based money lending. The legal products used to regulate online-based money lending lack strong legal standing. Because regulations made by a state agency in its implementation reap many problems.

Cyber institutions as a solution in law enforcement in the field of cyber crimes are very effective in tackling criminal acts, because cyber crimes is the object of cyber crimes through cyber media, so a non-penal mechanism is needed to avoid all crimes that will continue. Bearing in mind that legal regulations in the cyber field are very weak both in terms of regulation and enforcement, then non-penal settlement is a concrete step in tackling cyber crimes. So that the Government is actually serious in making a policy in the cyber sector, so besides weak law enforcement, regulations are also being strengthened, especially in the settlement of cyber crimes where the crimes is not visible in reality because it is carried out through cyber media.

BIBLIOGRAPHY

- Abdul Wahid dan Mohammad Labib, 2005, *Kejahatan Mayantara (Cyber Crimes)*, Refika Aditama, Bandung,
- Ahmad M. Ramli, 2004, *Cyber Law Dan Haki Dalam Sistem Hukum Di Indonesia*, PT Refika Aditama, Bandung. h
- Muladi dan Diah Sulistyani R.S., 2016, *Kompleksitas Perkembangan Tindak Pidana dan Kebijakan Kriminal*, Alumni, Bandung.
- Sari, Alfihca Rezita. 2018. *Perlindungan Hukum Bagi Pemberi Pinjaman Dalam Penyelenggaraan Financial Technology Berbasis Peer To Peer Lending Di Indonesia*, Yogyakarta: Fakultas Hukum Universitas Islam Indonesia..
- Smith, Scott S, 2016, *Internet Crimes Report, Federal Bureau of Investigation, Internet Crimes Complaint Center*, Washington D.C.
- Ani Eko Wahyuni, Bambang Eko Turisno, Raden. 2019. *Praktik Finansial Teknologi Ilegal Dalam Bentuk Pinjaman Online Ditinjau Dari Etika Bisnis*, *Jurnal Pembangunan Hukum Indonesia*, 1(3), h
- Hermawan, R. 2019. "Kesiapan aparaturnya pemerintah dalam menghadapi cyber crimes di Indonesia". *Jurnal Media Hukum*, 6(1) h
- Krimiyarsi. 2015. "Criminal Law Enforcement of Cyber Porn / Cyber Sex in Order to Fighting Crimes in Indonesia". *International Journal of Business, Economics and Law*, 8, (4),
- Lubis, Rini R. 2017. "Potensi Pengguna Internet Indonesia dalam Counter-Cyber Radicalization". *Jurnal Pertahanan dan Bela Negara*, 7(2)
- Rosyadi, I. 2007. "Penegakan Hukum dalam Masyarakat Indonesia". *Jurnal Sains Dan Inovasi*, 3(2),
- Sanyoto. 2008. *Penegakan Hukum di Indonesia*. *Jurnal Dinamika Hukum*, 8(3),
- Suprayitno, Edi dan Nur Ismawati. 2008. "Sistem Informasi Fintech Pinjaman Online Berbasis Web", *Jurnal Sistem Informasi Teknologi Informasi dan Komputer*, 9(2). h
- Vadza, K. 2013. "Cybercrimes and its Categories". *Indian Journal of Applied Research*, 3(5)