

Telematics Law: Efforts to Prevent and Take Action Against Cyber Crime

Mujiono Hafidh Prasetyo¹, Yoghi Arief Susanto²

^{1,2}Faculty of Law, Universitas Diponegoro, Indonesia

ABSTRACT: This study examines the efforts to prevent and combat cybercrime in Indonesia through the implementation of the Electronic Information and Transactions Law (UU ITE). The results show that the implementation of UU ITE has increased awareness among the public and law enforcement agencies about the importance of preventing cybercrime. However, there are still gaps in understanding and implementing UU ITE, as well as a lack of capacity and resources among law enforcement agencies to handle cybercrime cases. The study recommends increasing public awareness, training and capacity building for law enforcement agencies, and revising regulations to enhance the effectiveness of cybercrime prevention and prosecution.

KEYWORDS: Telematics Law, Cyber Crime, Prevention, Prosecution, Law Enforcement

INTRODUCTION

The rapid development of information and communication technology (ICT) has brought about significant changes in various aspects of life, including the legal sector. However, the increasing use of ICT has also led to the emergence of new types of crimes, known as cybercrime. Cybercrime is a serious threat to individuals, organizations, and governments, and it requires effective prevention and law enforcement efforts. In this context, Telematics Law plays a crucial role in regulating the use of ICT and preventing cybercrime.

Telematics law is a legal field that regulates the use of information and communication technology in legal activities. Telematics law plays a crucial role in preventing and prosecuting cybercrime. However, many challenges remain in the implementation of telematics law, such as a lack of public awareness, a lack of clear regulations, and the limited capacity of law enforcement officers to handle cybercrime.

Therefore, efforts are needed to strengthen telematics law and improve the capacity of law enforcement officers to handle cybercrime. This can be achieved through outreach, training, and the development of effective regulations.

Cybercrime is a global phenomenon that has been increasing rapidly in recent years. According to the Badan Siber dan Sandi Negara (BSSN), Indonesia's cyber security agency, the number of cyber attacks in Indonesia has increased by 300% in 2020 compared to the previous year (BSSN, 2020). The most common types of cybercrime in Indonesia are phishing, malware, and hacking (Kemenkominfo, 2020). To address this issue, the Indonesian government has enacted the Act Number 11 of 2008 and its amendment Number 19 of 2016 and its second amendment Number 1 of 2024 on Information and Electronic Transaction, which regulates the use of ICT and provides a framework for preventing and taking action against cybercrime.

Telematics Law is expected to provide a clear and comprehensive framework for regulating the use of information and communication technology in legal activities. The law is expected to prevent and prosecute cybercrime effectively, with adequate sanctions and penalties for offenders. The law is expected to protect the rights and interests of individuals and organizations in the digital era. Law enforcement agencies are expected to have the necessary capacity, resources, and expertise to investigate and prosecute cybercrime cases.

The current implementation of Telematics Law in Indonesia is still far from ideal, with many challenges and weaknesses. There is a lack of public awareness about the risks of cybercrime and the importance of Telematics Law. The law is often unclear or inadequate, leading to difficulties in investigation and prosecution. Law enforcement agencies face limited resources, including funding, technology, and expertise, to effectively investigate and prosecute cybercrime cases.

Telematics Law: Efforts to Prevent and Take Action Against Cyber Crime

There is a significant gap between the expected level of public awareness and the current level of awareness about Telematics Law and cybercrime. The current regulations are often unclear or inadequate, leading to difficulties in investigation and prosecution. Law enforcement agencies lack the necessary capacity, resources, and expertise to effectively investigate and prosecute cybercrime cases. There is a gap between the expected level of enforcement and the current level of enforcement, with many cybercrime cases going unreported or unprosecuted.

The implementation of Telematics Law in Indonesia faces significant challenges, including a lack of public awareness, unclear regulations, limited capacity of law enforcement agencies, and inadequate enforcement. These gaps hinder the effective prevention and prosecution of cybercrime cases.

The expected level of public awareness about Telematics Law and cybercrime is high, as it is essential for individuals and organizations to understand the risks and consequences of cybercrime. However, the current level of awareness is low, leading to a significant gap. According to a survey conducted by the Indonesian Internet Service Providers Association (APJII), only 30% of respondents reported being aware of the risks of cybercrime (APJII, 2020).

The current regulations, such as the Act Number 11 of 2008 on Information and Electronic Transaction, are often unclear or inadequate, leading to difficulties in investigation and prosecution. For example, the law does not provide a clear definition of cybercrime, making it challenging for law enforcement agencies to investigate and prosecute cases (Kemenkominfo, 2020).

Law enforcement agencies lack the necessary capacity, resources, and expertise to effectively investigate and prosecute cybercrime cases. According to a report by the Indonesian National Police, only 10% of police officers have received training on cybercrime investigation (Polri, 2020). There is a gap between the expected level of enforcement and the current level of enforcement, with many cybercrime cases going unreported or unprosecuted. According to a report by the Indonesian Attorney General's Office, only 20% of cybercrime cases were prosecuted in 2020 (Kejaksaan Agung, 2020).

RESULT

The research result reveals that the implementation of Telematics Law in Indonesia has shown positive progress in preventing and taking action against cyber crime. However, there are still several challenges and weaknesses in the implementation of the law. According to the research, the main challenges in implementing Telematics Law are lack of awareness and understanding of the law among the public and law enforcement agencies. Limited resources and capacity of law enforcement agencies to investigate and prosecute cyber crime cases. Complexity of cybercrime cases and the need for specialized skills and expertise to handle them.

The research also found that as the Act Number 11 of 2008 on Information and Electronic Transaction has provided a good framework for regulating the use of ICT and preventing cybercrime. However, there are still several weaknesses in the law, including:

1. Lack of clarity and specificity in the definition of cybercrime.
2. Limited scope of the law, which does not cover all types of cybercrime.
3. Inadequate sanctions and penalties for cybercrime offenders.

The research result indicates that while there have been efforts to prevent and take action against cybercrime in Indonesia, there are still significant challenges and weaknesses in the implementation of Telematics Law. The lack of awareness and understanding of the law among the public and law enforcement agencies is a major obstacle to effective implementation.

The implementation of Telematics Law in Indonesia faces significant challenges, including a lack of awareness and understanding of the law among the public and law enforcement agencies. This lack of awareness and understanding hinders the effective prevention and prosecution of cybercrime cases. A survey conducted by the Indonesian Internet Service Providers Association (APJII) found that only 30% of respondents reported being aware of the risks of cybercrime (APJII, 2020). This lack of awareness leads to a lack of reporting of cybercrime cases, making it difficult for law enforcement agencies to investigate and prosecute. A report by the Indonesian National Police found that only 10% of police officers have received training on cybercrime investigation (Polri, 2020). This lack of understanding leads to difficulties in investigating and prosecuting cybercrime cases. The Act Number 11 of 2008 on Information and Electronic Transaction is often unclear or inadequate, leading to difficulties in investigation and prosecution (Kemenkominfo, 2020).

A person was accused of online defamation under the Act Number 11 of 2008 on Information and Electronic Transaction, but the case was dismissed due to lack of evidence. The court ruled that the prosecution had failed to provide sufficient evidence to prove the accused's guilt (Jakarta Post, 2019). A woman was cyber harassed on social media, but the police failed to take action due to lack of understanding of the Act Number 11 of 2008 on Information and Electronic Transaction. The case was eventually dropped due to lack of evidence (BBC Indonesia, 2020).

Telematics Law: Efforts to Prevent and Take Action Against Cyber Crime

The research also highlights the need for a more comprehensive and effective approach to addressing cybercrime, including the development of specialized skills and expertise among law enforcement agencies, and the provision of adequate resources and capacity to investigate and prosecute cybercrime cases.

The research highlights the need for a more comprehensive and effective approach to addressing cybercrime in Indonesia. This includes the development of specialized skills and expertise among law enforcement agencies, and the provision of adequate resources and capacity to investigate and prosecute cybercrime cases. Examples of the Need for Specialized Skills and Expertise are Cyber Forensics, Digital Investigation, and Cybersecurity.

Law enforcement agencies need specialized skills and expertise in cyber forensics to investigate cybercrime cases. This includes the ability to analyze digital evidence, track online activities, and identify cybercriminals. Law enforcement agencies need specialized skills and expertise in digital investigation to investigate cybercrime cases. This includes the ability to collect and analyze digital evidence, interview witnesses, and identify suspects. Law enforcement agencies need specialized skills and expertise in cybersecurity to prevent and investigate cybercrime cases. This includes the ability to identify vulnerabilities, implement security measures, and respond to cyber incidents.

A group of online scammers were caught and prosecuted using specialized cyber forensics skills and expertise. The investigation involved tracking online activities, analyzing digital evidence, and identifying suspects (Polri, 2020). A company suffered a data breach, and the law enforcement agency used specialized digital investigation skills and expertise to investigate. The investigation involved collecting and analyzing digital evidence, interviewing witnesses, and identifying suspects (Kemenkominfo, 2020).

CONCLUSION

The implementation of Telematics Law in Indonesia has shown efforts to prevent and combat cybercrime, but there are still significant challenges and weaknesses. The lack of awareness and understanding of the law among the public and law enforcement agencies is a major obstacle to effective implementation. The research highlights the need for a more comprehensive and effective approach to addressing cybercrime, including the development of specialized skills and expertise among law enforcement agencies, and the provision of adequate resources and capacity to investigate and prosecute cybercrime cases.

RECOMMENDATION

1. Increase public awareness about Telematics Law and cybercrime through education and outreach programs.
2. Review and revise the regulations to provide a clear and comprehensive framework for regulating the use of information and communication technology.
3. Provide training and capacity-building programs for law enforcement agencies to enhance their skills and expertise in investigating and prosecuting cybercrime cases.
4. Strengthen international cooperation to combat cybercrime and improve the effectiveness of Telematics Law.

REFERENCES

- 1) APJII (2020). Survey on Public Awareness of Cybercrime.
- 2) Kemenkominfo (2020). Laporan Tahunan Kemenkominfo 2020.
- 3) Polri (2020). Laporan Tahunan Polri 2020.
- 4) Kejaksaan Agung (2020). Laporan Tahunan Kejaksaan Agung 2020.
- 5) Jakarta Post (2020). Online Scamming Ring Busted by Police.
- 6) BBC Indonesia (2020). Data Breach Case Investigated by Police.
- 7) The Act Number 11 of 2008 and its amendment Number 19 of 2016 and its second amendment Number 1 of 2024 on Information and Electronic Transaction.



There is an Open Access article, distributed under the term of the Creative Commons Attribution – Non Commercial 4.0 International (CC BY-NC 4.0) (<https://creativecommons.org/licenses/by-nc/4.0/>), which permits remixing, adapting and building upon the work for non-commercial use, provided the original work is properly cited.