IJAMESC, Vol. 2 No. 06, December 2024
DOI: https://doi.org/10.61990/ijamesc.v2i6.383 e-ISSN 2986-8645

CRIMINAL LAW REFORM IN THE FACE OF THE SOCIETY 5.0 ERA AGAINST CYBER CRIME

Nopit Ernasari[1]*, Naib[2]
[1.2]Universitas Pamulang, Indonesia
*Corresponding Author:
nopiternasari94@gmail.com

Abstract
Society 5.0 brings a major transformation in the social order through the integration of advanced technologies that blur the boundaries between the physical and virtual worlds. In this context, cybercrime has emerged as a serious challenge that requires adequate legal handling. This article examines the urgent need for criminal law reform in Indonesia to anticipate and respond to cybercrime in the Society 5.0 era. Through normative analysis and review of existing policies, this study assesses the effectiveness of current regulations. The proposed reforms include strengthening a legal framework that is more adaptive to technological innovations, increasing the capacity of law enforcement in dealing with digital crimes, and adjusting penalties for crimes that occur in cyberspace. The article also highlights the importance of international collaboration in cyber law enforcement. In conclusion, without a comprehensive reform of the criminal law, Indonesia risks falling behind in efforts to deal with the threat of cybercrime in the Society 5.0 era.

Keywords: Law Reform, Society 5.0, Cyber Crime, Technology, Law Enforcement

1. Introduction

Rapid developments in the realm of information and communication technology have led the world towards a new phase known as "Society 5.0". This era is characterized by the close integration between humans and technology, where artificial intelligence, the internet of things, and other technologies become an integral part of daily life. This transformation of society not only brings positive impacts, but also poses challenges and changes in various aspects of life, including in the context of criminal law. In Society 5.0, changes in behavior patterns and crime are becoming increasingly complex along with the rapid adoption of technology. Cybercrime, digital fraud, and other cybersecurity challenges are becoming increasingly serious threats. Therefore, the need for criminal law reform is essential to answer the social and technological dynamics that continue to develop.

Society 5.0 provides a strong impetus to achieve efficiency and balance between the use of technology and the protection of human rights. While technology provides innovative solutions in law enforcement, the protection of privacy and individual rights is becoming increasingly important. In this context, criminal law reform needs to ensure that these aspects are accommodated in a balanced manner, creating an adaptive and responsive legal framework.

Criminal law reform is essentially an effort to review and reshape (reorient and reform) the law in accordance with the general socio-political, socio-philosophical, and cultural values of Indonesian society. Therefore, the exploration of the values that exist in the Indonesian nation in an effort to reform the Indonesian criminal law must be carried out in order to cover the socio-political, socio-philosophical, and socio-cultural aspects of the

Indonesian people. Barda Nawawi Arief, said that the reform of the criminal law essentially contains meaning: an effort to reorient and reform the criminal law in accordance with the central values of socio-political, socio-philosophical, and socio-cultural of Indonesian society that underlie social policies, criminal policies, and law enforcement policies in Indonesia. (Arief, 2005)

The 1945 Constitution of the Republic of Indonesia, Article 1 paragraph (3) expressly states that Indonesia is a country of law. As a state of law, of course, the administration of the State and its government is based on the principles of universal legal principles and local wisdom. This proportional integration and acculturation gave birth to synthesis as manifested in the State's objectives as formulated in the Preamble to the 1945 State Constitution and the State's foundation, namely Pancasila. All components of the Indonesian nation must make Pancasila a vortex point of power and the 1945 Constitution as a basic law that must be obeyed without exception in exercising state power. The implementation of the principle of the State of law in the future will experience challenges in its time.

The extraordinary information technology revolution is able to change the order and shift of guidance very quickly, in the past there was an industrial revolution, now there is an information technology revolution. In the information revolution, the role of humans is quantitatively getting smaller, but qualitatively getting higher. Through information technology, humans are able to explore the universe, be able to see any hemisphere, see other countries without having to come to their destination, but simply through information technology. All natural events can be accurately calculated and predicted. Law was initially based on deeds and actions that were factual or manual. In the future, legal acts will experience new problems, the information technology revolution will change paradigms, concepts and theories, although it will not change philosophy. All fields including law are required to adapt. Anyone and anything that does not adapt evolutively will become a victim. (Abdullah, 2017)

Society 5.0 is a new term used to denote the world of the future. This society is based on ubiquiti, machine learning, internet of things, big data, cloud computing, cryptography and biometrics. All of these technologies will be combined to create technology in modern life. The new way of life will inevitably affect human values, concepts, and behavior. Society 5.0 is a character value that must be developed and a tolerance that must be fostered along with the development of innovative, creative and critical competencies. Society 5.0 aims to integrate cyberspace and physical space into a single unit that can be easily equipped with artificial intelligence. In this era, it focuses on human work and activities to human-centered, which is based on technology. It seems difficult to do in a developing country like Indonesia, but that doesn't mean it can't be done because at this time Japan has proven to be a country with the most advanced technology, this era is also able to create new jobs and cause other impacts.

Thus, the law should also provide protection to internet users in good faith and take strict action against internet criminals who cause a lot of harm to others. As a result of the Covid-19 pandemic that hit the world, the threat actors increased like a collapsed durian. Never imagined, there are new opportunities to launch cyber threats, both to individual users, governments and enterprises. The pandemic has imposed boundaries between work and personal life. At the same time, enterprises and the education world must compete with hybrid work styles, while companies are also looking to accelerate their migration to the cloud. Regulators around the world also discuss data and privacy issues.

The current era of information technology is two opposite parts, in addition to making a positive contribution to improving human welfare, progress and civilization, as well as making a negative contribution to the means of committing crimes that ignore the proximity of distance. This cybercrime is known as "cybercrime".

2. Theoretical Background

2.1 Cybercrime

Cybercrime is a new form of threat that has never existed before in society. Hacking, cracking, defacing, sniffing, carding, phishing, spamming, or scam are a series of dangerous internet crimes and can also penetrate government-owned public infrastructure whose impact causes many national losses and unsettles the wider community. Cybercrime is known as a modern conventional crime. Public law in the form of jurisdiction, ethics of online activities, consumer protection, regulatory bodies, data protection, private law (IPR, E-commerce, Insurance) are part of the state's basic strength to fight these crimes.

The development of technology certainly brings various implications that must be immediately anticipated and also watched out. This effort has given birth to a legal product in the form of Law Number 19 of 2016 Jo Law Number 11 of 2008 concerning Information and Electronic Transactions (UU ITE). The basic thing of the ITE Law is an effort to accelerate the benefits and functions of law (regulations) within the framework of legal certainty. (Sudikno Mertokusumo, 1993).

2.2 Society 5.0

In the era of Society 5.0, cybercrime is increasing and difficult to deal with because criminals can hide behind complex and difficult to track computer networks. Therefore, an effective legal system is needed in handling cybercrime in order to reduce the level of crime in protecting the public from cybercrime.

Realizing an effective legal system in handling cybercrime in the era of society 5.0 needs to be supported by capable legal tools. This includes regulations that are in accordance with the development of information and communication technology. In addition, it is also necessary to form a law enforcement agency and a team of experts who monitor and are able to handle various types of cybercrime.

Since 1983, Indonesia has experienced cybercrime, especially in the financial industry. Various forms of cybercrime, such as software piracy, encryption breaches, stolen credit card use, bank fraud, the spread of pornographic content, and other forms of cybercrime, all occurred in Indonesia in the years that followed.8 In addition to the smuggling of pornographic photos in cyberspace, other computer-related crimes in Indonesia include pagejacking (mousetrapping), spam (junk mail), interception, cybersquatting, and typosquatting. Meanwhile, hacking, vandalism, DoS/DDoS attacks, the spread of viruses/worms, and the installation of logic bombs are examples of crimes committed against computer systems and networks. (Faith Gordon, 2022) (widiyanti, 2022).

2.3 Technology

The internet provides various conveniences in many aspects of human life because it has changed distance and time to be infinite. The existence of chat, e-mail and web-cam facilities is a solution to the problem of long-distance communication that has been using phones at high costs. Meanwhile, for the educational community, the internet is the most complete world library and an effort to develop E-Learning. As for the banking world,

cyberspace is used to provide ease of transactions for its customers without having to go to the bank. Likewise in the development of democratic life, where opinions, criticisms and suggestions can be submitted in the discussion or comment section available on each central and regional government institution website, without having to participate in demonstrations.

These conveniences are the positive side of the use and utilization of the internet. However, it is undeniable that not all activities on the internet are always positive, but the internet also has a negative side, namely being used as a medium to commit various forms of crime. Technological developments always have an impact both directly and indirectly, both in a positive and negative sense and will greatly affect every attitude of action and mental attitude of every member of society. (Hamzah, 1992)

3. Methods

The research used in writing is normative juridical. The sources of legal materials used in this study are primary legal materials and secondary legal materials. The primary materials used are law books. The types of approaches used in this study are the legislative approach, the case approach and the legal concept analysis approach. The data processing method used is an analysis method which is then outlined in the descriptive analysis paper. (Nasution, 2016).

4. Results and Discussion

The Society 5.0 era is an extension of the evolution of technology that has influenced society since primitive times. This concept emerged in response to the disruption turmoil caused by the Industrial Revolution 4.0 in 2019. The Society 5.0 era focuses more on the more effective and optimal use of existing technologies in the Industrial Revolution 4.0 era. The main principle is to connect people, objects, systems, and other elements virtually and process data by applying artificial intelligence (Artificial Intelligence). In the Society 5.0 Era, different practices from the Industrial Revolution 4.0 are seen in the way data and information are managed. In the Society 5.0 era, information collected from various sources, including the Internet of Things (IoT), Big Data, artificial intelligence, and robots, is not only analyzed by humans. Instead, this data is processed and understood by artificial intelligence (AI) systems, which then produce optimal solutions. This opens up opportunities to achieve a level of efficiency that far exceeds human capacity to process and interpret data.

The 1.0 era describes the time when humans lived as hunters and knew writing. The 2.0 Era is marked by the development of agriculture, while the 3.0 Era is the time when humans begin to get to know industry and utilize machines in daily life. The 4.0 era, which preceded Society 5.0, presented a revolution in computer technology and the internet, which has been profound in various aspects of human life.

Community development in the Society 5.0 era Technological developments in the Society 5.0 era are expected to overcome various social challenges faced by society, such as:

1) Educational Transformation: Technology enables more inclusive and personalized learning. AI can be used to create a curriculum that is tailored to each individual's needs.
2) Smart Health: With AI and IoT, disease diagnosis can be done faster and more accurately. The healthcare system will be increasingly integrated with technology, making it easier to access services.

3) Improved Quality of Life: With smart cities, people will experience an increase in the comfort of life. More efficient transportation systems, smarter resource management, and more secure security systems are just a few examples.
4) Industry 4.0 to Society 5.0: Industrial automation continues to evolve. Humans work hand in hand with robots and AI to increase productivity and efficiency.
5) Social Inclusion: Technology in Society 5.0 focuses not only on economic development, but also on improving the quality of life of the entire society, including those with physical or social limitations.

Challenges Faced Although society 5.0 brings a lot of potential, there are several challenges that must be faced:
1) Equal Access: Not all people or countries have the same access to advanced technology, so there is potential for increased inequality.
2) Ethics and privacy: The use of data at scale raises privacy concerns. The ethical question of Limitations in data collection and use is an important debate.
3) Unemployment: The organization of jobs by robots and AI can lead to the loss of conventional jobs, although there are new job opportunities in the technology sector.

A digitally connected society 5.0 has led to an increase in the potential and patterns of crime in cyberspace. The types of cybercrime that emerged and developed in this era include:
1) Phishing and Digital Scams: Phishing techniques using fake emails or messages are becoming more sophisticated, with AI capable of mimicking human interactions and tailoring messages to make them more convincing.
2) Ransomware: cybercriminals use malicious software (malware) that locks access to the victim's data and demands a ransom to unlock that access. In Society 5.0, ransomware becomes more sophisticated and targets more critical systems such as healthcare infrastructure or governments.
3) IoT hacking: With the increasing number of IoT devices used in daily life (such as smart homes, autonomous vehicles), these devices are becoming new targets for criminals. IoT often has security loopholes, and cybercriminals can take control of those devices.
4) Data misuse and privacy: In Society 5.0, personal data is a very valuable asset. Massive data collection by companies and governments opens up opportunities for the theft of personal data which can then be misused for fraud, false identity, or sold on the black market.

Some of the main factors that affect the increase in cybercrime in the society 5.0 era, include:
1) Increasing Connectivity and Data Usage: in Society 5.0, all aspects of human life are connected to digital technology. The use of IoT, AI, and big data creates large volumes of data and interconnected systems, which, if not properly protected, are easy targets for cybercriminals.
2) Technological Advancement and Security Loopholes: along with the adoption of advanced technologies such as IoT, the potential for security loopholes is also increasing. Complex systems are difficult to manage and often have loopholes that can be exploited by cybercriminals.

3) Cyber Anonymity: Cybercriminals often take advantage of cyber anonymity to launch attacks without being easily traced. In the era of society 5.0, technology is increasingly enabling attacks that are more difficult to track, including cross-border attacks.

AI technology, which is supposed to make people's lives easier, is also used by cybercriminals to launch more sophisticated attacks. AI is used to create attacks that are difficult to detect, such as creating viruses that can adapt to security systems. Deepfake technology that uses AI to create content that looks real can be used for fraud, defamation, or extortion crimes.

1) To address the increasingly complex threat of cybercrime in Society 5., a collective effort from various parties is needed:
2) Cybersecurity improvements: Governments, companies, and individuals must improve cybersecurity, including the use of strong encryption, firewalls, and regular software updates.
3) Education and awareness: The public must be educated about the threat of cybercrime and how to protect themselves. Awareness of phishing techniques, secure password management, and the use of anti-virus software are important.
4) Regulation and International Collaboration: Cybercrime is often cross-country, requiring clear regulations and international collaboration in dealing with these crimes. Strong law enforcement and cooperation between countries are also crucial in dealing with cybercrime.
5) Security AI Development: The use of AI is not only for crime, but also for security. AI-based security systems can detect abnormal patterns in the network that indicate an attack, even before the damage occurs.

The behavior of society and human civilization around the world has been changed by the advancement of information and communication technology. In addition, rapid social change and the elimination of state boundaries are the result of advances in information technology. Apart from its positive effects on society, growth, and civilization, information technology today can also be used for criminal purposes. Since the invention of computers as one of the capabilities of science and technology products, the fields of telecommunications, media, and computing have been integrated. The Internet is a product of the convergence of several forms of communication and media technology as well as computer technology. The internet has given people something completely new. (Finna Nazran, 2022) (Ari Dermawan, 2021) (Budhijanto, 2014)

There is no regulatory contradiction between the Criminal Code and Law No. 19 of 2016 Jo Law No. 11 of 2008 concerning Information and Electronic Transactions regarding the regulation of fraudulent activities carried out through the internet. Both can apply simultaneously (jo), but the Lex Specialis derogat legi Generali provision means that the former will take precedence. Because the Criminal Code is a law that explains the elements of fraud, the ITE Law is prioritized because it has the specificity to ensnare fraud crimes through the internet.

Indonesia as a country of law always prioritizes all state and community activities in accordance with the law. Therefore, Indonesia is trying to reform criminal law, one of which is with the enactment of Law Number 1 of 2024 concerning the Second Amendment to Law No. 19 of 2016 Jo Law No. 11 of 2008 concerning Electronic

Information Technology. Because activities in the field of computer-based technology are very important for society and can easily spread human rights.

A form of cybercrime that has a close relationship with the use of computer-based technology and telecommunication networks, namely Unauthorized Access to Computer Systems and Services, is a crime committed into a computer network system without permission or without the knowledge of the owner of the computer network system. Hackers do it by sabotaging or stealing important and confidential information, but there are also those who do it only because they feel challenged to try their skills by penetrating a system that has a high level of protection. This kind of crime is increasingly rampant with the development of internet technology. One of the hacker cases. In 2016, Tiket.com and Citilink were attacked by hackers, a group of teenagers managed to hack the online ticket buying and selling site, tiket.com on Citilink's servers. The losses experienced by Tiket.com amounted to 4.1 billion, while Citilink amounted to 2 billion.

The government's challenges in the era of society 5.0 in strengthening cybersecurity include: insufficient availability of technology experts and security technical experts to design and implement cybersecurity strategies. The risks that occur due to the cross-border nature of cyber security, which makes countries with weak cyber security crime strategies can interfere with the cybersecurity of other countries. The use of anonymization tools, for example to block chain currencies or cryptocurrencies, in crimes that use the internet makes it easier to create policies.

Various efforts can be taken to solve Internet crimes, both preemptively, preventively, and repressively. Preparatory efforts can be carried out by ratifying international cybercrime agreements into the legal system in Indonesia. The Council of Europe Agreement is a form of international agreement, and some of its covenants have been ratified into the legal system in Indonesia. Preventive cybercrime countermeasures can be carried out by developing security, increasing energy for computer features, ability and discipline in using these features in cyberspace. These activities can be in the form of actions that can be carried out either individually, national policies, or globally. Meanwhile, repressive cybercrime countermeasures can be carried out by ensnaring the perpetrators of criminal acts to be handled in accordance with the law. The law determines the interests of the victim by providing restitution, compensation, or assistance which is the responsibility of the perpetrator with the State as the provider. (Thantawi, 2001)

Currently, the regulations used as a legal basis for cybercrime cases are Law Number 1 of 2024 concerning the Second Amendment to Law No. 19 of 2016 Jo Law No. 11 of 2008 concerning Electronic Technology Information. With the existence of this ITE Law, it is hoped that it can protect the information technology user community in Indonesia, this is important considering the number of internet technology users who are increasing from year to year. The increasing use of the internet on the one hand provides a lot of convenience for humans in carrying out their activities, on the other hand it makes it easier for certain parties to commit a criminal act, this technological advancement also affects the lifestyle and mindset of humans, in fact, currently there are many crimes using information technology. The phenomenon of cybercrime that is growing rapidly that does not know territorial boundaries must indeed be watched out for because this crime is somewhat different from other crimes in general.

Criminal law reform has a significant influence on the protection of human rights (HAM), especially in dealing with cybercrime. Crime in cyberspace is growing rapidly along with technological advances and the increasingly widespread use of the internet.

Therefore, the reform of the criminal law is essential to respond to the new challenges that arise, while ensuring that the protection of human rights is maintained.

Cybercrime often involves the theft or misuse of personal data, such as account hacking or leakage of personal information. Criminal law updates may include stricter regulations on the protection of personal data. This is crucial to avoid misuse of data that could harm individuals. Countries such as the European Union have adopted regulations such as GDPR (General Data Protection Regulation) that give citizens the right to protect personal data.

With the update of the criminal law, the enforcement of personal data protection can be clearer and firmer, while still paying attention to the principle of proportionality in law enforcement so as not to excessively violate someone's privacy. Criminal law reform must strengthen the role of the state in protecting its citizens from cybercrime. This includes the restoration of victims' rights, which may include the right to compensation, healing, or further protection (such as protection from the threat of further violence after being a victim of cybercrime).

5. Conclusion

The development of society in the era of Society 5.0, which integrates advanced technologies such as the Internet of Things (IoT), big data, artificial intelligence (AI), and digital communication, has created a new space for cybercrime that is more complex and widespread. Increasingly developed technology makes it easier for criminals to carry out their actions more efficiently, but on the other hand, it also increases the potential losses caused to individuals and society. Cybercrimes such as hacking, online fraud, personal data theft, and the spread of false information have become more difficult to control, due to their transnational nature and operating in an ever-changing cyberspace. In the face of this phenomenon, the reform of criminal law plays a very important role in protecting human rights (HAM). Criminal law updates that are responsive to technological developments can improve the effectiveness of cybercrime countermeasures, while ensuring the protection of basic individual rights, such as the right to privacy, freedom of opinion, and personal data protection. The new criminal law must be able to balance strict law enforcement and respect for the digital freedom that every individual has.

The influence of criminal law reform on human rights protection in the context of cybercrime includes several aspects, such as strengthening regulations related to personal data protection, maintaining freedom of expression in cyberspace, and justice for victims of cybercrime. In addition, a continuously updated criminal law is also needed to create effective international collaboration in addressing cybercrime which often involves perpetrators and victims from various countries. Overall, societal changes towards Society 5.0 bring new challenges in the legal world, especially in regulating and handling increasingly complex cybercrimes. Criminal law reform in line with technological developments must pay attention to the aspect of human rights protection, as well as ensure that law enforcement does not sacrifice individual freedom and privacy in cyberspace.

References

Arief, B. N. (2005). Pembaharuan Hukum Pidana Dalam Perspektif Kajian Perbandingan. Bandung: PT. Citra Aditya Bakti.

Abdullah, P. N. (2017, November 29). Mahkamah Agung Republik Indonesia. (Mahkamah Agung) Retrieved November 29, 2023, from

https://mahkamahagung.go.id/id/artikel/2830/gelombang-on-line-dalam-perkembangan-hukum

Ari Dermawan, E. S. (2021). "Peran Masyarakat Dalam Menaati Hukum dan Mendukung Perkembangan Teknologi Komputer Dalam Bisnis Digital,". Jurnal Pengabdian Masyarakat, 2(3), 569-573.

Budhijanto, D. (2014). Teori Hukum Konvergensi. Bandung: Refika Aditama, 2014.

Faith Gordon, e. (2022). Beyond Cybercrime: New Perspective on Crimw, Harm and DIgital Technologies. International Journal for Crime, Justice and SOcial Democracy(1).

Finna Nazran, F. Y. (2022). "Realizing People's Welfare in Economic Globalization, Perspective of Contitution of Electronic Information and Transaction". Veteran Law, 5(1), 1-14.

Hamzah, A. (1992). Aspek-aspek Pidana dibidang Komputer. Jakarta: Sinar Grafika.

Nasution, B. J. (2016). Metode Penelitian Hukum. Bandung: Mandar Maju.

Pandey, S. K. (2022). A Study on DIgitak Payments System & Consumer Perception: AN Empirical Survey. Journal of Positive School Psychology, 6(3), 221.

Sudikno Mertokusumo, P. (1993). Bab-bab Tentang Penemuan Hukum. Bandung: Citra Aditya Bakti.

Thantawi. (2001). Perlindungan Korban Tindak Pidana Cybercrime dalam SIstem Hukum Indonesia.

Widiyanti, P. w. (2022). Tindak Pidana Pencurian Data Nasabah Dalam Bidang Perbankan Sebagai Cyber Crime. Jurnal Hukum dan Perundang-Undangan , 2(2), 1-21.