

Topic: Human Right Issues of Artificial Intelligence (AI) Gaps and Challenges, and Affected Future Legal Development in Various Countries

Shifting Legal Paradigms in The Digitalization Era

Budi Yardi ¹⁾, Alwan Hadiyanto ²⁾, Anis Mashdurohatun ³⁾ & Jawade Hafidz ⁴⁾

¹⁾ Faculty of Law, Universitas Islam Sultan Agung (UNISSULA) Semarang, Indonesia, E-mail: budiyardi.std@unissula.ac.id

²⁾ Faculty of Law, Universitas Riau kepulauan (UNRIKA) Batam, Indonesia, E-mail: budiyardi.std@unissula.ac.id

³⁾ Faculty of Law, Universitas Islam Sultan Agung (UNISSULA) Semarang, Indonesia, E-mail: anism@unissula.ac.id

⁴⁾ Faculty of Law, Universitas Islam Sultan Agung (UNISSULA) Semarang, Indonesia, E-mail: jawade@unissula.ac.id

Abstract. *Humans now live in a modern civilization that demands everything to be fast, effective, and efficient. Modernity has become an identity that seems to be inherent in all aspects of human life. Cyberspace has been deliberately created to facilitate human work or interaction between people in different locations. However, many users misuse this convenience, leading to cybercrime, which creates new problems that must be addressed by the government regarding regulations in the national legal system and the handling of cybercrime.*

Keywords: *Digital Era; Legal Paradigm; Shifting.*

1. Introduction

The Rapid Development of Science, Knowledge and Technology (IPTEK), especially in the field of electronics and informatics, is acknowledged by many to bring various conveniences (blessings) to human life. Conversely, without realizing it, this progress can also bring disaster or catastrophe to human civilization itself. Humans now live in a modern civilization that demands everything to be fast, effective, and efficient. Modernity has become an identity that seems to be attached to all aspects of human life.

Shifting Legal Paradigms in The Digitalization Era
(Budi Yardi, Alwan Hadiyanto, Anis Mashdurohatun & Jawade Hafidz)

Topic: Human Right Issues of Artificial Intelligence (AI) Gaps and Challenges, and Affected Future Legal Development in Various Countries

Anything else is considered old-fashioned, traditional, and outdated. The development of science and technology has led to various changes in the fields of politics, economics, social, and culture. One of the developments in science and technology that is progressing very rapidly is the development in the field of information technology. This is marked, among other things, by the birth of the internet, which is scientifically called cyberspace.

Cyberspace is an electronic medium in a computer network that is widely used for one-way and two-way communication online. Cyberspace comes from the words cybernetics and space. Cyberspace itself was first introduced by William Gibson, who stated that cyberspace is a globally connected reality, supported by computers, computer-accessed, multidimensional, artificial, or virtual. This means that every internet connection that exists is a window, where representations of objects that are not physically real will be seen and heard, but rather more of a style, character, and action of data creation in the form of pure information creation. Cyberspace is deliberately created to facilitate human work or interaction between one person and another who are in different places. The progress of technology and information has implications for the use of the internet for e-commerce, e-business, e-banking activities, as well as providing cyber liberty (cyberliberty) for both commerce (commercial cyberliberty) and social (civil cyberliberty).

Where humans can easily, freely, sophisticatedly, and quickly carry out transactions without having to meet face to face (face to face), make transfers and access information, and so on. However, it must be realized that cyber freedom through the internet can be misused to carry out cyberthreats, cyberterrorism, and cyber talking, as well as making it easier for someone to commit crimes that damage morals, such as gambling, prostitution, and pornography.

2. Research Methods

From the explanation above, it certainly has serious problems regarding the development of Indonesian society, which generally experiences changes from time to time, so it is necessary to answer regarding: 1. To what extent is cyberspace jurisdiction regulated in the national legal system? 2. How is cybercrime handled?

3. Results and Discussion

3.1. Jurisdiction of Cyberspace in the National Legal System

"Legal thought cannot be separated from the environment of its time. It is often seen as an answer to legal problems or a challenge to dominant legal ideas at a given time. Therefore, even if it aspires to express an idea universally, it is beneficial if the theory has a background

Shifting Legal Paradigms in The Digitalization Era
(Budi Yardi, Alwan Hadiyanto, Anis Mashdurohatun & Jawade Hafidz)

Topic: Human Right Issues of Artificial Intelligence (AI) Gaps and Challenges, and Affected Future Legal Development in Various Countries

based on specific legal theories. Throughout history, societal customs have changed over time and become a matter of great importance.

Law must be able to adapt to the development of the existing society, especially considering that Indonesia is a developing country. Therefore, law needs to shift to achieve justice, as is the purpose of law itself. After independence, Indonesia was determined to build a national law based on the personality of the nation through law development. In general, Indonesian law is directed towards written law. Etymologically, "jurisdiction" is legal power, legal authority, and legal dispute. Jurisdictiegenschit (Dutch) means a dispute about the authority to adjudicate (between two judicial bodies)." Note: I have translated the text to the best of my ability, taking into account the context and nuances of the language. Please let me know if you have any questions or require further clarification.

Cyberspace has emerged as a contemporary digital product capable of transcending the boundaries of space and time, including national borders that have traditionally confined territorial jurisdiction. According to Howard Rheingold, cyberspace is an imaginary or virtual space of an artificial nature, where individuals engage in everyday social activities in novel ways.

To assess the extent to which the legal paradigm of cyberspace falls under national jurisdiction, we can examine the perspectives of various experts, including Mochtar Kusumaatmadja. In this context, Kusumaatmadja modifies the concept of law as a rule with the concept of law as a tool for social engineering, drawing on Roscoe Pound's theory. Therefore, the traditional view of law as lagging behind societal developments ("...het recht hinkt achter de feiten aan") must be abandoned.

Cyberspace has become the latest digital product capable of breaking through the boundaries of space and time, including countries that have been limited by territorial boundaries. According to Howard Rheingold, cyberspace is an imaginary or virtual space that is artificial, where everyone does anything they usually do in everyday social life in new ways.¹

To examine the extent to which the jurisdiction of the legal paradigm of cyberspace in national law can be seen from the perspective of several experts, one of whom is Mochtar Kusumaatmadja. In this case, he modifies the concept of law as a rule with the concept of law as a means of development (law as a tool of social engineering) in Roscoe Pound's theory.

¹ Yasraf Amir Piliang, "Public Space dan Public Cyberspace: Ruang Publik dalam Era Informasi", tersedia di website <http://www.bogor.net/idkf/idkf-2/public-space-dan-public-cyberspace-ruang-publik-dalam-era-inf>, diakses pada tanggal 14 Juni 2021

Topic: Human Right Issues of Artificial Intelligence (AI) Gaps and Challenges, and Affected Future Legal Development in Various Countries

Therefore, the traditional view of law that follows the development of society ('...het recht hinkt achter de feiten aan') must be abandoned.²

The presence of modern law today is influenced by the history of the past, involving the reciprocal relationship between law, society, and the development of the modern state. Modernity has the following characteristics:³

- a. Has a written form.
- b. The law applies to the entire territory of the State.
- c. Law is an instrument used consciously to realize the political decisions of its people.

Before the emergence of the ITE Law No. 11 of 2008, which has now been amended to become the ITE Law No. 19 of 2016, to ensnare perpetrators of cybercrime, special laws and general provisions were used, such as: Law Number 36 of 1999 concerning Telecommunications; Law Number 5 of 1999 concerning the Prohibition of Monopolistic Practices and Unfair Business Competition; Law Number 8 of 1999 concerning Consumer Protection; Law Number 19 of 2002 concerning Copyright; Law Number 14 of 2001 concerning Patent Rights; Law Number 15 of 2001 concerning Trademarks, and the Criminal Code. In practice, the most frequently used are Law Number 36 of 1999 concerning Telecommunications and the Criminal Code. Indonesia is a constitutional state with many cultures and customs practiced by its people. Moreover, the legal umbrella held by this nation consists of positive law, Islamic law, and customary law. Harmonization among the three is very much needed in the process of progress and renewal of existing law in Indonesia. In its formation, the government must be able to pay attention to the legal culture that exists in society and the way the community views the law.⁴

The government, through its policies, has enacted a law known as the ITE Law, which aims to address issues arising within society. This law was formed through a joint agreement in a plenary meeting between the government and the House of Representatives. The results of

² Mochtar Kusumaatmadja, *Pembinaan Hukum dalam Rangka Pembangunan Nasional*, Bandung: Binacipta, 1975, hal.7-9

³ Satjipto Rahardjo, *Ilmu Hukum*, Bandung: Citra Aditya Bakti, 1982, hlm. 213-214

⁴ Raharjo A, *Cybercrime: Pemahaman dan upaya pencegahan kejahatan berteknologi*. Citra Aditya Bakti, 2002, hal.79

Topic: Human Right Issues of Artificial Intelligence (AI) Gaps and Challenges, and Affected Future Legal Development in Various Countries

this agreement contain important mandates for the public to build ethics in internet usage, encouraging them to be more careful and wise in using social media.⁵

On November 25, 2016, the Revised ITE Law was enacted with the number UU No. 19 Tahun 2016. In accordance with Article 87 of Law No. 12 of 2011, which states that "Legislation shall come into force and have binding force on the date of its promulgation, unless otherwise stipulated in the relevant legislation," Law No. 19 of 2016 has legal force since November 25, 2016, and all Indonesian citizens are deemed to be aware of and obligated to comply with it. Law No. 19 of 2016, which originated from a joint agreement in a plenary meeting between the DPR and the Government on November 27, 2016, has an important mandate for the public to build ethics in the use of social media so that they are more careful in the social media realm. The ITE Law regulates how to act in a good social manner. This law restricts the public from providing information that is considered detrimental to others and leads to criminal acts. In its regulation, the role of Human Rights must be truly considered because the principles of justice and equality before the law are closely related to it.⁶

The ITE Law essentially regulates the use of information and electronic transactions conducted through computers or other electronic media. The information covered by this law is not limited to text, images, or sounds, but also includes emails, telegrams, and others. The scope of this law is very broad. As stipulated in Article 2, this law applies to anyone who engages in legal acts, both within the territory of Indonesia and outside of it, that have legal consequences within Indonesia. Even actions committed outside of Indonesia that harm Indonesian interests fall under the scope of this law, as all transactions are inherently cross-border in nature.

This law also expands the definition of intellectual property rights (IPR). Article 25 of this law states that websites and intellectual works contained therein are protected as IPR. This law also aims to combat the misuse of other people's identities. For example, Article 26 states that the use of someone's personal data must be done with the consent of the person concerned. The same applies to the distribution of information containing gambling, insults, and extortion or threats. This prohibition is stipulated in Article 27. The penalty, as written in Article 45, is a maximum imprisonment of six months or a fine of Rp1 billion.

⁵ Moh. Mahfud MD, *Membangun Politik Hukum Menegakkan Konstitusi*, Jakarta: Rajawali Press, 2012, hal. 46

⁶ Morissan, dkk., *Teori Komunikasi Massa* Bogor: Ghalia Indonesia, 2010, hlm.83

Topic: Human Right Issues of Artificial Intelligence (AI) Gaps and Challenges, and Affected Future Legal Development in Various Countries

3.2. Handling Cyber Crim

According to Andi Hamzah, viewing computer crime is not as a new crime but rather as an ordinary (traditional) crime, because it can still be resolved through the Criminal Code. Likewise, a study by the United States Congress concluded that there are three categories of criminal offenses in the field of computers, namely: the use of incorrect data into the computer, altering or destroying information or archives and theft, whether electronically or in other ways: money, fines, goods, facilities or valuable data.⁷

Cybercrime is a crime committed by individuals or groups who have the knowledge and skills to operate computers and other telecommunication devices. This crime typically involves damaging, stealing, and using data illegally. According to Abdul Wahib and Mohammad Labib, cybercrime is a dangerous type of crime that harms individuals, society, and the state. It is inaccurate to describe cybercrime as a 'crime without victim,' as it can have a layered impact on both private and public victims. Private rights can be threatened, disrupted, damaged, or even lost due to the actions of individuals or groups who exploit their superior knowledge and technology through methods classified as cybercrime.⁸

The qualification of cybercrime, as quoted by Barda Nawawi Arief, is the qualification of cybercrime according to the Convention on Cybercrime 2001 in Budapest, Hungary, namely :⁹

1. Illegal access: This refers to intentionally entering or accessing a computer system without authorization.
2. Illegal interception: This refers to intentionally and without authorization, eavesdropping or intercepting the transmission and emission of non-public computer data to, from, or within a computer system using technical aids.
3. Data interference: This refers to intentionally and without authorization, damaging, deleting, changing, or erasing computer data.
3. System interference: This refers to intentionally causing serious disruption or hindrance without authorization to the functioning of a computer system.
4. Misuse of Devices: This refers to the misuse of computer equipment, including computer programs, computer passwords, and access codes.

⁷ Andi Hamzah, *Hukum Pidana Yang Berkaitan Dengan Komputer*, Sinar Grafika, Jakarta, 1993, Hal 9.

⁸ Abdul Wahib dan Mohammad Labib, *Kejahatan Mayantara (Cyber crime)*, Refika Aditama, Bandung, 2005, Hal. 15

⁹ Barda Nawawi Arief, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan*, Jakarta: Kencana Predana Media Group, 2007, hlm. 246-247

Topic: Human Right Issues of Artificial Intelligence (AI) Gaps and Challenges, and Affected Future Legal Development in Various Countries

5. Computer-related Forgery: This refers to the falsification by intentionally and without authorization, entering, changing, or deleting authentic data into non-authentic data with the intention of using it as authentic data.
6. Computer-related Fraud: This refers to fraud by intentionally and without authorization, causing the loss of goods/property of others by entering, changing, or deleting computer data or by interfering with the functioning of a computer/computer system, with the aim of obtaining economic benefit for oneself or others.

One of the emerging issues related to the development of transnational crime is law enforcement against cybercrime perpetrators. Transnational crime in cybercrime clearly intersects with jurisdictional issues. In cyberspace, it is difficult to prosecute offenders because they are located outside Indonesian territory. This then becomes the jurisdictional issue of cybercrime enforcement in Indonesia. This means which law will be applied in handling cybercrime.

The phenomenon of cybercrime in Indonesia is increasing with various cases, such as the case of the use of the Mustika Ratu Com domain name in 2000. Mustika Ratu reported Chandra Sugiono for engaging in unfair competition by using the Mustika Ratu company/domain name on Chandra Sugiono's website. Chandra Sugiono, who at that time was the GM of PT. Martha Tilaar, was charged with article 382 bis of the Criminal Code and article 19 Jo 48 of Law Number 5 of 1999 concerning the Prohibition of Monopolistic Practices and Unfair Business Competition with a demand of 6 months imprisonment or a fine of at least 25 billion and a maximum of 100 billion and also charged with Law Number 15 of 2001 concerning trademarks. In examining the case, the panel of judges at the South Jakarta District Court ruled that the alleged act was not proven. Therefore, Tjandra Sugijono was acquitted of all charges (*vrijspraak*), but at the Supreme Court level, he was charged with 4 months imprisonment.

Cybercrime opens up opportunities for violations of intellectual property rights (IPR) such as copyrights, trademarks, and others, for example, related to the use of the domain names of companies, big brands, or those that are already well-known without the permission of the owner. Law enforcement in Indonesia faces difficulties in dealing with the proliferation of cybercrime. Some of the causes include the limited human resources available to law enforcement agencies, namely those who are intensively involved in computer crime, crimes using computer facilities, and cybercrime.

This is because these crimes require special skills on the part of law enforcement officers. As a result, investigations are often inconclusive. The investigation methods are also special, not all

Topic: Human Right Issues of Artificial Intelligence (AI) Gaps and Challenges, and Affected Future Legal Development in Various Countries

investigators can do it. There must be police officers assigned to the field of the internet, commonly known as cyber police. To prove the traces of hackers, crackers, and phreakers in carrying out their actions, especially those related to computer programs and data, the facilities of the Indonesian National Police are inadequate because there is no forensic computer. This facility is needed to uncover digital data and record and store evidence in the form of soft copies (images, programs, etc.). In this case, the Indonesian National Police still does not have adequate forensic computing facilities. The forensic computing facilities that will be established by the Indonesian National Police are expected to be able to serve three important things: evidence collection, forensic analysis, and expert witness. It is indeed difficult for law enforcers to carry out their duties optimally without being equipped with legal instruments that regulate cybercrime.

In addition, the mechanism within law enforcement agencies regarding cybercrime is also not yet well established. Although the ITE Law exists and provides a minimum level of legal certainty for crimes in cyberspace, there is still a possibility of different interpretations in the application of articles to the perpetrators. For instance, in the Prita Mulyasari case, she was initially charged with Articles 310 and 311 of the Criminal Code concerning defamation, which carry a maximum penalty of 9 months and 1 year and 4 months in prison, respectively, for defamation committed in writing. However, with the enactment of the ITE Law, which regulates electronic mail, the law could also be used as a basis for charging defamation committed through email.

4. Conclusion

1. Legal Reform in Indonesia: Balancing Progress with Human Rights Legal reform is essential to keep pace with the changing times. Laws must adapt to regulate and resolve issues arising from new phenomena. As a nation governed by law, Indonesia should prioritize the quality of its legal products and their effectiveness in maintaining order within society. The Information and Electronic Transactions Law (UU ITE) regulates responsible online behavior. It restricts the dissemination of information deemed harmful to others and potentially criminal. In enacting this law, the role of Human Rights must be carefully considered, as it is deeply intertwined with the principles of justice and equality before the law. 2. Challenges of Cybercrime Enforcement in Indonesia Law enforcement in Indonesia faces difficulties in addressing the rise of cybercrime. Several factors contribute to this challenge, including: Limited Human Resources: There is a shortage of personnel with expertise in computer crime, cybercrime, and online crime. These offenses require specialized skills that not all investigators possess. Dedicated cyber police units are necessary. Inadequate Investigative Tools: Law enforcement lacks sufficient resources to effectively investigate cybercrime. This includes the absence of

Shifting Legal Paradigms in The Digitalization Era
(Budi Yardi, Alwan Hadiyanto, Anis Mashdurohatun & Jawade Hafidz)

Topic: Human Right Issues of Artificial Intelligence (AI) Gaps and Challenges, and Affected Future Legal Development in Various Countries

forensic computer equipment needed to uncover digital evidence, record data, and store soft copy evidence (images, programs, etc.).

5. References

Journals:

AP Edi Atmaja, "Kedaulatan Negara Di Ruang Maya: Kritik UU ITE Dalam Pemikiran Satipto Rahardjo", Jurnal Opinio Juris, Vol. 16, Mei-September 2014

Heru Soeprapto, "Kejahatan Komputer dan Cyber (Serta Anisipasi Pengaluran Pencegahan Di Indonesia)", Jurnal Hukum Bisnis, Volume 7, 2001

Renny N.S. Koloay, "Perkembangan Hukum Indonesia Berkenaan Dengan Teknologi Informasi Dan Komunikasi", Jurnal Hukum Unsrat, Vol. 22, No.5, 2016

Books:

Abdul Wahib dan Mohammad Labib, *Kejahatan Mayantara (Cyber crime)*, Refika Aditama, Bandung, 2005;

Andi Hamzah, *Hukum Pidana Yang Berkaitan Dengan Komputer*, Sinar Grafika, Jakarta, 1993

Barda Nawawi Arief, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan*, Jakarta: Kencana Predana Media Group, 2007;

Mochtar Kusumaatmadja, *Pembinaan Hukum dalam Rangka Pembangunan Nasional*, Bandung: Binacipta, 1975

Moh. Mahfud MD, *Membangun Politik Hukum Menegakkan Konstitusi*, Jakarta: Rajawali Press, 2012

Morissan, dkk., *Teori Komunikasi Massa* Bogor: Ghalia Indonesia, 2010

Prasetyo dan Abdul Halim, *Ilmu Hukum dan Filsafat Hukum*, Yogyakarta: Pustaka Pelajar, 2007

Raharjo A, *Cybercrime: Pemahaman dan upaya pencegahan kejahatan berteknologi*. Citra Aditya Bakti, 2002

Satjipto Rahardjo, *Ilmu Hukum*, Bandung: Citra Aditya Bakti, 1982

Shifting Legal Paradigms in The Digitalization Era
(Budi Yardi, Alwan Hadiyanto, Anis Mashdurohatun & Jawade Hafidz)



Topic: Human Right Issues of Artificial Intelligence (AI) Gaps and Challenges, and Affected Future Legal Development in Various Countries

Subekti, Kamus Hukum, Jakarta: Pradnya Paramita, 1983

Werner J. Severin dan James W. Tankard, Teori Komunikasi Sejarah, Metode, dan Terapan di Dalam Media Massa, Jakarta: Kencana Prenada Media Group, 2009

Regulation:

Electronic Information and Transactions Law Number 11 of 2008, which has now been amended to Electronic Information and Transactions Law Number 19 of 2016;

Law Number 1 of 1946 concerning Criminal Law;

Law Number 1 of 2023 concerning Criminal Law, an amendment to Law Number 1 of 1946 concerning Criminal Law;

Law Number 14 of 2001 concerning Patents;

Law Number 15 of 2001 concerning Trademarks;

Law Number 19 of 2002 concerning Copyright;

Law Number 36 of 1999 concerning Telecommunications;

Law Number 5 of 1999 concerning the Prohibition of Monopolistic Practices and Unfair Business Competition;

Law Number 8 of 1999 concerning Consumer Protection;

Shifting Legal Paradigms in The Digitalization Era
(Budi Yardi, Alwan Hadiyanto, Anis Mashdurohatun & Jawade Hafidz)