Cogent Social Sciences

ISSN: 2331-1886 (Online) Journal homepage: www.tandfonline.com/journals/oass20

Cybercrime in the new criminal code in Indonesia

Sigid Suseno, Ahmad M. Ramli, Ranti Fauza Mayana, Tasya Safiranita & Bernadette Aurellia Nathania Tiarma

To cite this article: Sigid Suseno, Ahmad M. Ramli, Ranti Fauza Mayana, Tasya Safiranita & Bernadette Aurellia Nathania Tiarma (2025) Cybercrime in the new criminal code in Indonesia, Cogent Social Sciences, 11:1, 2439543, DOI: 10.1080/23311886.2024.2439543

To link to this article: https://doi.org/10.1080/23311886.2024.2439543

Published online: 07 Jan 2025.

COGENT SOCIAL SCIENCES
2025, VOL. 11, NO. 1, 2439543
https://doi.org/10.1080/23311886.2024.2439543

LAW, CRIMINOLOGY & CRIMINAL JUSTICE | RESEARCH ARTICLE

OPEN ACCESS

Check for updates

Cybercrime in the new criminal code in Indonesia

Sigid Suseno, Ahmad M. Ramli, Ranti Fauza Mayana, Tasya Safiranita and Bernadette Aurellia Nathania Tiarma

Center of Cyber Law & Digital Transformation Faculty of Law Universitas Padjadjaran, Indonesia

ABSTRACT

Indonesia's new Criminal Code (KUHP), enacted in 2023. It will bring significant changes to the country's legal system, particularly in the area of cybercrime. With the proliferation of digital crimes, the focus of the updated code is to strengthen Indonesia's criminal code. Besides serving as a basis for criminal law, the new Code repeals a number of provisions of the previous legislation, particularly on cybercrime. This research uses a normative legal approach, analysing legal principles, systematics and relevant facts, with key legislation including Law No. 1 of 2024 on the Amendment of Law No. 11 of 2008 on Electronic Information and Transactions and Law No. 1 of 2023 on the Criminal Code. The amendments cover various aspects such as defamation and insults, blasphemy, privacy violations, threats and intimidation, moral offenses and pornography and other related cybercrimes. The amandments aim to better address the challenges of the digital age and reduce conflicts between the ITE law and the new Criminal Code. The research concludes that cybercrime in Indonesia is increase rampantly, exacerbated by the growing use of Artificial Intelligence.

ARTICLE HISTORY
Received 25 June 2024
Revised 18 September 2024
Accepted 29 October 2024

KEYWORDS
Criminal Code; cybercrime; IET Law; criminal law

SUBJECTS
Criminology – Law; Asian Law; Criminal Law & Practice

1. Introduction

Indonesia has now entered the era of Society 5.0, where technology coexists with and is inseparable from human life. The transition from Industry 4.0 to Society 5.0 is marked by the advent of new technologies such as the Internet of Things (IoT), Artificial Intelligence (AI), Cloud Computing and others. These technologies are expected to make production processes and work more effective and efficient. Technology now collaborates with humans, rather than replacing them entirely.

The Fifth Industrial Revolution demands an integration between humans and technology. There have been many misconceptions that human jobs will be entirely replaced by technology. However, the fact remains that human creative thinking cannot be replaced by technology. Humans are still needed to operate and manage technology.

The technology resulting from the current industrial revolution is driving modern society on a massive scale and influencing everything, including government, international trade, communication and travel. Digital technology is further revolutionizing the world, and since the advent of the World Wide Web and the Internet, society has become more complex and advanced (Carlaw et al., 2006).

The development of technology has a dual nature. While technological advancements facilitate human life by providing broader access to information, they also give rise to various new modes of cybercrime. In this highly dynamic digital era, cyberattacks have become a significant concern. The rapid development of information technology offers benefits to the global community, but it also opens wide doors for skilled and organized cyber criminals (Herera & Hasan Sebyar, 2023). Business information, personal data and critical infrastructure all face potential threats that could endanger social and economic stability (Herera & Hasan Sebyar, 2023).

CONTACT Sigid Suseno sigid.suseno@unpad.ac.id Center of Cyber Law & Digital Transformation Faculty of Law Universitas Padjadjaran, Indonesia

The development of cybercrime continues to be a compelling discourse on the international stage. While few deny that the internet has significantly impacted criminal behavior, there is even less consensus on this matter. Even when countries agree that cybercrime is a problem, there seems to be no overall consensus on how to address it (Wall, 2007). Technologies such as AI and increasingly common sensing capabilities have produced more practical data and information, but they also become potential targets for cyberattacks (Heartfield et al., 2018).

Cybercrime has become one of the most urgent issues faced by all societies worldwide, especially in the context of the ongoing digital transformation era. Cybercrime is not just a local problem but a global one that requires cooperation among countries to mitigate its dangers (Vitus, 2023). In the digital transformation era, nearly all aspects of life are connected online, from business and finance to the health sector and infrastructure. This data is highly vulnerable and critical, making society a potential target for cybercrime.

Cybercrime presents a significant challenge that society must address seriously. It can result in losses for individuals, governments, institutions and other relevant parties. To effectively combat cybercrime, individuals and governments need to understand cybercrime schemes and the contemporary internet behavior trends of cyber criminals (Arora, 2016). Among all the cybercrimes committed in various countries, cyber-terrorism is the most prominent aspect.

As Indonesia enters the digital era, the threat of cyberattacks becomes increasingly real and concerning. The rapid development of technology facilitates access to information, but it also has negative impacts by widening opportunities for cybercriminals. Initially, these cybercrimes could not be adequately addressed through the Indonesian Criminal Code (KUHP) alone. Therefore, the government enacted Law No. 11 of 2008 on Electronic Information and Transactions (EIT Law), which has now undergone its second amendment through Law No. 1 of 2024.

Indonesia has its own Law No. 11 of 2008 on Electronic Information and Transactions, which addresses cybercrimes and has recently undergone its second amendment with the issuance of Law No. 1 of 2024. The ITE Law serves as a legal framework governing electronic transactions, personal protection, electronic transactions, copyrights and other intellectual property in the digital domain. It aims to facilitate the development of the digital economy in Indonesia and provide a sense of security and legal certainty for internet users and providers in the country (Kurniawan, 2023).

In addition to the EIT Law, Indonesia has also introduced the latest Criminal Code (KUHP), enacted on 2 January 2023, through Law No. 1 of 2023. This new Criminal Code was designed to offer Indonesia a contemporary legal foundation for criminal matters that is not rooted in colonialism. Numerous clauses have been amended and adapted to the circumstances and objectives of Dutch colonialism in Indonesia. The endeavor to establish a National Criminal Code is significant because, following the old Criminal Code, the government introduced special laws that nullified certain articles of the old Criminal Code (Manullang et al., 2023).

The Criminal Code (KUHP) serves as Indonesia's legal framework governing criminal offenses and penalties. Historically, it was established by the Dutch East Indies government in 1918. Initially, the KUHP heavily mirrored the Dutch legal system, but it has since evolved to align with the context and requirements of Indonesian society (Renggong, 2017). Since Indonesia gained independence, the KUHP has played a pivotal role in shaping a criminal justice system that ensures legal certainty and fairness (Malau, 2023).

In addition to responding to prevailing crimes, technological advancements and societal changes influence the process of amending the KUHP. Any revisions must be approached with caution, involving various stakeholders and drawing from both experience and current dynamics. The present KUHP has undergone significant modifications and must also be equipped to address cybercrime challenges.

In Society 5.0, there is a strong dependence on digital infrastructure, which means technologies such as AI, the IoT, and big data are extensively used in everyday life. This widespread adoption has led to an increase in cybercrime. As more services and critical infrastructure become internet-based, the likelihood of hacking, data breaches and cyber-attacks has grown. The new Criminal Code reflects these concerns by modifying existing laws and adding provisions that address various types of cybercrimes. For example, articles related to data theft, unauthorized access to computer systems, and the

illegal use of digital platforms have been expanded or clarified to better protect users in the era of Society 5.0.

Indonesia's legal system needs to adapt to the evolving forms of cybercrime, especially within the Criminal Code (KUHP). Security and legal order in the digital domain are crucial to instilling confidence in individuals when they interact or transact online. Hence, a deep understanding of the latest cybercrime developments and how Indonesia's legal framework, particularly in criminal law, can prevent and combat these offenses is imperative. In light of this, the research will tackle two key questions:

1. How are the developments and challenges of cybercrime modes in Indonesia?
2. How does the new Criminal Code address cybercrimes in Indonesia?

2. Methodology

This research employs a normative juridical approach in legal study. It involves examining legal principles, legal systematics and existing facts (Soerjono & Mamuji, 2010). The research is descriptive-analytical, focusing on delineating the provisions related to cybercrime in Indonesia's new Criminal Code. This research is further supported by empirical data collected through interviews with legal practitioners, surveys of affected parties, and an analysis of recent cybercrime cases, providing a practical perspective on the application of Indonesia's new Criminal Code provisions.

The method not only employs a Normative Juridical approach but also includes descriptive-analytical and online literature research. Considering this is a new area of study in Indonesia, it is essential for Indonesia to have more concrete regulations governing the matter. In this article, we analyze the issue from various legal perspectives and current social conditions.

3. Development cybercrime in Indonesia

3.1 Definition of cybercrime

Technology emerges from human creativity in designing practical material objects. The crimes resulting from the development of applications and the internet are referred to as cybercrimes. Internationally, cyber law encompasses legal terms concerning the use of information and communication technology. It is also known as information technology law, virtual world law and cyber law (Maskun, 2013).

The Convention on Cybercrime, Budapest 2001, categorizes cybercrimes into four types:

1. Offenses against the confidentiality, integrity and availability of computer data and systems;
2. Computer-related offenses;
3. Content-related offenses;
4. Offenses related to infringements of copyright and related rights.

According to Mcdonnell and Sayers, cyber threats encompass three types (Kementerian Pertahanan Indonesia, 2014):

1. Hardware threats
   These arise from installing a device that executes specific commands within a system, disrupting networks and other hardware devices.
2. Software threats
   These result from software designed to steal, manipulate information and cause damage.
3. Data/information threats
   These stem from the dissemination of specific data or information for particular purposes.

Generally, cybercrime can be classified into two categories: conventional cybercrime and new cybercrime. Conventional cybercrime refers to cybercrimes that existed before the creation of computer systems or the internet, such as theft, defamation, fraud and others. Meanwhile, new cybercrime refers to

crimes that emerged with the development of computer systems. Examples include hacking, virus dissemination and others.

Cyberattack threats represent a form of threat in the modern or nonmilitary era that can trigger national disintegration through the motives of individual or specific group interests. Many examples of cyberattack actions are often encountered in daily life, such as (Ariyaningsih et al., 2023):

1. Cybercrime
   In cybercrime, perpetrators frequently engage in illicit activities such as data manipulation or transmission to achieve specific objectives. Cybercriminals are individuals proficient in hacking and can collaborate from diverse locations. Examples of ongoing cybercrimes include identity theft, targeted espionage, credit card fraud and more.
2. Cyberterrorism
   Cyberterrorism entails the actions of terrorist networks aiming to sow terror to disrupt a country's political stability, social order and economic welfare. Instances of cyberterrorism include assaults on government websites, interception of political communication networks, electronic data theft, banking breaches and others.
3. Cyber Warfare
   Cyber warfare represents an evolution of cyberattacks and cybercrime. It constitutes warfare conducted in the digital domain. Cyber warfare differs from traditional physical warfare in its methods of attack and defense. It involves operations targeting or defending digital assets. The primary instruments utilized in cyber warfare are computer systems and the internet. Unlike conventional warfare, the targets are not geographical territories but entities existing in cyberspace.

When addressing cybercrime, a profound understanding of the technical aspects of the technology used as a tool for criminal activities is essential. This understanding aids in determining the appropriate regulations to prosecute such actions.

Several factors can precipitate cybercrime. First, there is a lack or absence of education provided by educational institutions like schools or parents on proper internet usage, leading to widespread misuse. Second, the rapid advancement of internet usage not aligned with societal welfare contributes to widening social disparities. Third, the ease of accessing information or content via the internet plays a significant role. The more accessible the information, the deeper society delves into the internet.

As is the case in Indonesia, cybercrime can target anyone. Various cases of different types of cybercrimes have been reported to the relevant authorities in Indonesia. This has prompted the Indonesian government to enhance cybersecurity measures to prevent the spread of these crimes. The Indonesian government has implemented several factual solutions to address various types of cybercrimes, including the establishment of the National Cyber and Encryption Agency (BSSN) since 2017, strengthening the legal framework through the Electronic Information and Transactions Law (UU ITE), forming a cybercrime unit within the Indonesian National Police, and promoting the importance of cybersecurity in critical sectors, such as banking, healthcare and telecommunications.

The actions taken so far have not fully accommodated the diverse types of cybercrime. Therefore, additional solutions are needed to maximize efforts, such as enhancing technological security and involving more IT experts in Indonesia as a collaborative approach to preventing cybercrime. This is important because cybercriminal activities are not only carried out with one specific goal but can also have various other objectives.

Individuals or networks engaging in cybercrimes typically have underlying motives for their actions. These motives can be broadly categorized into two groups: (1) intellectual motives and (2) economic, political and criminal motives. Intellectual motives involve crimes aimed at self-gratification and showcasing one's prowess in designing and implementing information technology. On the other hand, economic or political motives are driven by personal or group interests or aimed at harming individuals or groups. The latter category often has broader targets and is commonly orchestrated by companies or institutions (Umbara & Setiawan, 2022).

3.2 Development and impacts of cybercrime in Indonesia

The types of cybercrime are increasing alongside technological advancements each year. It is often observed that with the discovery of new technologies by humans, new forms of cybercrimes emerge, depending on how these technologies are utilized. Some examples of prevalent cybercrimes include personal data leakage or misuse, cyberpornography, spamming, online gambling, phishing, carding and AI misuse.

Cybercrimes related to the misuse or illegal access of personal data are governed by Law No. 27 of 2022 on Personal Data Protection. Prohibitions on personal data usage are outlined in Articles 65-66, while criminal provisions regarding the illegal use of personal data are detailed in Articles 67 to 73. These prohibitions encompass:

1. Unauthorized acquisition or collection of personal data.
2. Unauthorized disclosure of personal data.
3. Unauthorized use of personal data.
4. Creation of false personal data or falsification of personal data.

Carding is a prevalent form of cyber fraud where individuals use stolen or counterfeit credit cards in the virtual domain. This type of crime is widespread in Indonesian society, with some viewing it as a symptom of systemic shortcomings. Efforts to combat carding often involve cyber investigations to track and access the data used in these fraudulent activities (Ginara et al., 2022).

Online gambling has become a focal point for government scrutiny. It involves various electronic devices like smartphones and computers to conduct gambling activities over the internet. In online gambling, participants can wager on a wide array of games including poker, roulette, slots and others (Situmeang et al., 2023). Gambling activities are regulated by the Criminal Code (KUHP), specifically Article 426, which imposes a maximum prison sentence of 9 years and a fine of up to category VI for individuals who:

1. Offer or facilitate gambling opportunities as a means of livelihood or participate in gambling activities;
2. Provide opportunities for the public to gamble or engage in gambling enterprises, regardless of whether specific conditions or procedures are met to utilize those opportunities;
3. Engage in gambling activities as a source of livelihood.

Online gambling has resulted in numerous negative impacts, including financial loss, addiction and even violence. The government has taken various measures to combat online gambling. The Indonesian National Police Headquarters reported that from 2022 to August 2023, a total of 866 suspects involved in online gambling were apprehended (CNN Indonesia, 2023).

The development of services on digital platforms has also led to the emergence of new forms of cybercrimes. One example is financial technology (fintech) lending platforms. Fintech lending, commonly referred to as online lending (*pinjol*), is a service particularly vulnerable to significant misuse. The convenience offered by fintech lending often entices individuals to borrow from these platforms. However, this convenience can lead to various criminal activities, such as extortion, fraud, the unauthorized dissemination of personal data and aggressive debt collection practices. Many fintech lending platforms operate illegally. The Task Force on Vigilance (SWI), in collaboration with the Indonesian National Police, has shut down more than 3000 illegal fintech lending platforms from 2018 to 2021 (Indradjaja et al., 2022).

Besides fintech lending, one of the tools that can be exploited for cybercrime is AI. AI refers to machines' ability to mimic human intelligence. According to Simon, AI is artificial intelligence applied in research, application and instruction related to computer programming to execute tasks requiring human intelligence (Sari & Harwika, 2022). Despite AI's numerous benefits in enhancing efficiency, its rapid advancement raises concerns among AI experts regarding potential impacts. One form of cybercrime facilitated by AI is deepfake.

Deepfake, a blend of 'deep learning' and 'fake', entails crafting hyper-realistic videos through digital manipulation, portraying individuals saying or doing things that never happened. Deepfake relies on

neural networks that analyze datasets to learn how to imitate someone's facial expressions, speech patterns and behaviors (Westerlund, 2019). Essentially, deepfake leverages facial mapping technology and AI to interchange one person's face with another's in a video.

The widespread occurrence of cybercrime has extensive impacts on society, encompassing social, economic and financial realms. From a social standpoint, cybercrime exposes individuals to the risks of theft and misuse of personal identity, fostering insecurity and fear within communities (Fakhriah & Mutmainnah, 2024). The compromise of personal data can also lead to various other crimes, including cyber terrorism, the illicit trade of personal information, and more.

Economically, cybercrime imposes costs for system recovery, law enforcement, and productivity losses. Economic instability not only directly impacts these areas but also sets off ripple effects (Fakhriah & Mutmainnah, 2024). For instance, banks affected by personal data breaches may lose customer trust, affecting investors' confidence in the institution.

According to the National Security Index, Indonesia's cybersecurity index stood at only 38.96 points out of 100 in 2022, placing it third lowest among G20 countries. Globally, Indonesia ranks 83rd out of 160 countries in the report (Daeng et al., 2023). This contrasts with the significant growth of internet users in Indonesia, which increased by 13%, ranking fourth after India, China, and the United States. Given this continuous growth, regulations to combat cybercrime should be developed to be more sophisticated and comprehensive.

According to data from the National Cyber and Crypto Agency (BSSN), there have been 22 cyberattacks related to the COVID-19 pandemic, including attacks by hackers like Blackwater Malware, DanaBot Banking Trojan, Spynote RAT and COVID-19 trackers (Ariyaningsih et al., 2023). This underscores the importance for Indonesia to be more vigilant and recognize that cybercrime demands serious attention. With more Indonesian citizens accessing the internet, the potential for cybercrimes to infiltrate information systems increases.

Based on this data, the Indonesian government is striving to maximize the implementation of cyber laws to prevent the expansion of cybercrime. However, there are several challenges in applying cyber laws in Indonesia, such as the rapid pace of technological innovation which often outpaces the development and updating of legal frameworks, jurisdictional challenges because cybercrimes frequently occur across borders and require lengthy legal processes, and the still limited public awareness and education regarding cybersecurity.

One of the solutions implemented by the government is the enactment of the new Criminal Code (KUHP), which has led to changes in several existing regulations, including the Information and Electronic Transactions Law (UU ITE). The introduction of the new KUHP facilitates the application of Indonesian criminal law to crimes that cross-national boundaries. Additionally, since 2017, the Ministry of Communication and Information Technology has launched initiatives to enhance the critical thinking skills of Indonesian citizens in using digital media.

4. Regulation of cybercrime in the new Indonesian Criminal Code

4.1 Formation of the new Indonesian Criminal Code

The endeavor to establish a national Criminal Code (KUHP) has become exceedingly crucial, especially considering that after the enactment of the old Criminal Code, special laws were introduced that rendered several articles of the old Criminal Code non-applicable (Manullang et al., 2023). Barda Nawawi argues that in formulating a new Criminal Code, inspiration or the wisdom of national development based on Pancasila cannot be overlooked. The reform of national criminal law must be grounded in the fundamental ideals of Pancasila. Opinions concerning the reconstruction of articles should rightfully be incorporated into the Draft Criminal Code through the legislative review process.

The government has also made strides towards constructing a new Criminal Code. Efforts to reform the Criminal Code commenced as early as 1958, marked by the establishment of the National Law Development Institute (LPHN). The drafting of the new Criminal Code began in 1963 during the First National Legal Seminar, which underscored the urgency of crafting a new Criminal Code (Manullang

et al., 2023). Progressing to 1993, the formulation of the Criminal Code was essentially completed. However, these efforts were halted by a change in the Minister of Justice.

Discussions on the Draft Criminal Code were reignited in 1998 and continued during Yusril Izra Mahendra's tenure from 2001 to 2004. Subsequently, discussions on the Draft Criminal Code were prioritized as a national legislative agenda. The Draft Criminal Code was then endorsed by the DPR (House of Representatives) during the 2014–2019 period. On 6 December 2022, the DPR ratified the Draft Criminal Code into law. The Criminal Code embodies the evolution of legal science and criminal law practice in Indonesia. In its formulation, the Criminal Code has considered the development of norms and societal needs.

The new Criminal Code retains essential principles previously stipulated in the old Criminal Code. These principles include the principle of non-retroactivity, territoriality, protection, passive national principle and universality. These principles serve as the cornerstone for the enforcement of Indonesian criminal law, encompassing cybercrime. With these principles in place, it is hoped that the enforcement of laws against cybercrime can be optimized.

Article 12 of the Criminal Code defines a criminal act as an act that is penalized by criminal sanctions and/or actions according to the law. For an act to be considered a criminal offense, it must involve elements that are illegal or contrary to the prevailing law in society.

In the process of drafting the new Criminal Code, attention must be given to nonjuridical elements. One crucial nonjuridical element is technological advancement. The government, in its role as a regulator, must anticipate the technology development toward something progressive. Regulations should provide guidance that can adapt to ensure that technological development and use can effectively contribute to the prosperity of society and the nation.

The increasingly sophisticated development of information technology is evident in the emergence of the IoT, AI, Big Data and other innovations. This suggests that Industry 5.0 is advancing faster than expected. Industry 5.0 is a concept where humans collaborate with technologies like smart machines to enhance efficiency (Ramli & Ramli, 2022). While technology was previously not considered a legal aspect, it now significantly influences the creation and enforcement of laws (Ramli & Ramli, 2022).

The implementation of the new Criminal Code (KUHP) will not immediately and swiftly prevent the occurrence of cybercrime. In its application, there are certainly challenges, particularly related to technology. Its rapid development has led to new types of crimes, such as deepfakes and AI-based fraud. This requires regular updates to ensure that all types of cybercrime can be effectively prevented. In practice, the law often lags behind technological advancements. Indonesia, with its continental European legal system, relies heavily on written regulations for law enforcement.

Another challenge in implementing the new Criminal Code (KUHP) is the readiness of the courts and law enforcement officers, as enforcing laws against cybercrime requires specialized training and specific competencies. Hence, legal interpretations are essential for judges to adjudicate cases in line with current technological progress. This is certainly related to the availability of technological infrastructure in Indonesia, which must be adequate to support law enforcement against cybercrime. There must be a balance between technological infrastructure and the quality of the human resources involved in implementing the existing regulations.

4.2 Regulation of cybercrime between law No. 1 of 2024 on Electronic Information and Transactions and the Indonesian Criminal Code

The regulation concerning cybercrime in Indonesia can be interpreted broadly or narrowly. Broadly speaking, cybercrime covers all criminal activities carried out using electronic means. This implies that all traditional crimes stipulated in the Criminal Code (KUHP) can be classified as cybercrimes under the broad category, provided that electronic systems are involved. However, if interpreted narrowly, cybercrime regulation falls under the Information and Electronic Transactions Law (EIT Law). The EIT Law itself does not explicitly define cybercrime but categorizes various cybercrimes based on the Convention on Cybercrimes.

After relying on the old Criminal Code derived from the Dutch colonial legal document *Wetboek van Strafrescht* for a long time, Law No. 1 of 2023 on the Criminal Code has been enacted, marking a new

era in Indonesia's criminal legal system. The regulations outlined in the new Criminal Code under Law No. 1 of 2023 will serve as a guide for law enforcement authorities, encompassing regulations concerning principles or other forms of digital crimes that may extend to perpetrators beyond Indonesia's borders (Hidayat, 2023).

One crucial aspect of the new Criminal Code is the principle of territoriality. Article 4 of the new Criminal Code stipulates that the criminal provisions of this Law apply to any person who commits:

1. Criminal acts within the territory of the Unitary State of the Republic of Indonesia;
2. Criminal acts on Indonesian ships or aircraft; or
3. Criminal acts in the field of information technology or other criminal acts, the consequences of which are experienced or occur within the territory of the Unitary State of the Republic of Indonesia or on Indonesian ships and aircraft.

Article 4, especially clause c, underscores that cybercrimes and other transnational crimes, which are borderless in nature, can be prosecuted under Indonesian law if their consequences are felt within Indonesian territory. Legislators have recognized the diverse challenges posed by future crimes. Although the National Criminal Code was crafted decades ago, its provisions are continuously updated to keep pace with the advancements of the times (Hidayat, 2023).

In addition to Article 4, Article 5 also governs the criminal provisions applicable to individuals outside the territory of Indonesia who commit offenses that jeopardize the interests of the Republic of Indonesia. These offenses include:

1. Threats to state security or the process of state governance;
2. Violations against the dignity of the President, Vice President or Indonesian officials abroad;
3. Counterfeiting currency, seals, national stamps, stamps or securities issued by the Indonesian government, or fraudulent use of credit cards issued by Indonesian banks;
4. Offenses against the economy, banking sector and trade of Indonesia;
5. Compromising the safety or security of maritime and aviation transportation;
6. Endangerment of buildings, equipment and national assets of Indonesia;
7. Compromising the safety or security of electronic communication systems;
8. Actions contrary to the national interests of Indonesia;
9. Violations against Indonesian citizens based on international agreements with the country where the offense occurred.

Points c, d and g can also serve as the basis for combating cybercrimes. Currently, there are numerous cases of cybercrimes involving document forgery, particularly those related to trade or banking. The safety and security of electronic communication systems are also crucial elements highly susceptible to interception, considering their widespread use, even among government officials.

The challenge of applying the Criminal Code in terms of jurisdiction involves harmonizing Indonesian law with international standards, which also includes regulations on the recognition and enforcement of laws from other countries. Additionally, gathering evidence in cybercrime cases presents a challenge, especially when relevant data is located outside national jurisdiction. In such cases, a process for requesting access to data or evidence stored abroad is necessary, requiring international cooperation on privacy and data protection regulations in other countries. Therefore, effective collaboration between the government, law enforcement agencies, and international partners is essential to ensure that Indonesian cyber law can be applied fairly and effectively across all jurisdictions.

Not only does it provide greater protection for borderless crimes, but the provisions on cybercrimes in the new Criminal Code also revoke several provisions previously found in the EIT Law. For instance, Article 27, paragraphs (1) and (3) of the ITE Law. Article 27, paragraph (1), deals with the distribution or access to information or electronic documents containing obscenity. Article 28, paragraph (2), regarding the dissemination of hate speech information, has also been restructured in the new Criminal Code. Additionally, the Criminal Code also revokes Article 30, Article 31, paragraph (1), Article 31, paragraph (2),

Article 36, Article 45, paragraph (1), Article 45, paragraph (3), Article 45A, paragraph (2), Article 46, Article 47 and Article 51, paragraph (2).

One of the regulations reconstructed by the new National Criminal Code is the norm regarding defamation. The rampant defamation occurring on social media and digital platforms is a legal issue that continues to be debated. This cannot be separated from the effectiveness and power of a digital platform based on a safe harbor policy (Ramli, 2023). With the model of safe harbor regulation, every individual is positioned as the owner of their own mass media.

Defamation is a challenging criminal offense to enforce. The Criminal Code revises the provisions on defamation under Chapter XVII on Defamation Offenses. Article 433, paragraph (1), stipulates that anyone who orally impugns the honor or reputation of another person by accusing them of something, intending for it to be publicly known, shall be liable for defamation, punishable by imprisonment for up to 9 (nine) months or a fine of category II.

This formulation clarifies the definition of defamation offenses and ensures more proportional penalties. Additionally, this article safeguards individuals who did not intend for their remarks to become public.

Furthermore, subsequent provisions are regulated in Article 433, paragraph (3), which states that the acts described in paragraph (1) and paragraph (2) are not punishable if performed in the public interest or in self-defense. These articles not only differentiate between slander and libel but also include the criteria of 'public interest or self-defense' as grounds for the offense. With Article 433, individuals expressing opinions or truths through social media cannot be subjected to criminalization.

The implementation of defamation regulations in the new Criminal Code requires a process for the public to understand, considering the right to freedom of expression. There is a risk that law enforcement could be misused to restrict free speech, so it is crucial to balance law enforcement with the right to freedom of expression. This balance ensures that the protection of reputations does not create reluctance among the public to participate in discussions and express their opinions.

In addition to the regulations on defamation, the new Criminal Code also addresses illegal access. Illegal access was previously addressed in Article 30 in conjunction with Article 46 of the EIT Law. Article 30 of the EIT Law states:

(1) Any person who intentionally and without right or unlawfully accesses a computer and/or electronic system by any means with the intention of obtaining Electronic Information and/or Electronic Documents.
(2) Any person who intentionally and without right or unlawfully accesses a Computer and/or Electronic System by any means with the intention of obtaining Electronic Information and/or Electronic Documents.
(3) Any person who intentionally and without right or unlawfully accesses a Computer and/or Electronic System by any means by violating, bypassing, exceeding or breaking security systems.

The penalties for individuals who violate these provisions are outlined in Article 46, which states:

(1) Any person who fulfils the elements as described in Article 30 paragraph (1) shall be punished with imprisonment for up to 6 (six) years and/or a fine of up to Rp600,000,000.00 (six hundred million Indonesian Rupiah).
(2) Any person who fulfils the elements as described in Article 30 paragraph (2) shall be punished with imprisonment for up to 7 (seven) years and/or a fine of up to Rp700,000,000.00 (seven hundred million Indonesian Rupiah).
(3) Any person who fulfils the elements as described in Article 30 paragraph (3) shall be punished with imprisonment for up to 8 (eight) years and/or a fine of up to Rp800,000,000.00 (eight hundred million Indonesian Rupiah).

The new Criminal Code clearly nullifies the provision regarding illegal access in the EIT Law. Article 322, which governs illegal access, stipulates the following:

1. Any person intentionally and without authorization or unlawfully accessing another person's Computer and/or Electronic System through any means shall be subject to imprisonment for up to 6 (six) years or a fine of up to category V.
2. Any person intentionally and without authorization or unlawfully accessing a Computer and/or Electronic System with the intention of obtaining Electronic Information and/or Electronic Documents shall face imprisonment for up to 7 (seven) years or a fine of up to category V.
3. Any person intentionally and without authorization or unlawfully accessing a Computer and/or Electronic System by violating, bypassing, exceeding, or breaking security systems shall be subject to imprisonment for up to 8 (eight) years or a fine of up to category VI.

Cybercrimes involving illegal access are actions that can be easily committed by anyone, but sometimes they occur unintentionally due to ignorance. In this context, it is essential to enhance public understanding through education about what constitutes illegal access and its legal consequences. Additionally, addressing cybercrimes related to illegal access requires careful consideration of individual privacy rights to avoid infringing on personal freedoms.

The regulation of cybercrimes in the EIT Law and the new Criminal Code carries legal protection implications for the community's legal interests, particularly concerning computer data or electronic data, electronic information, electronic documents, and computer systems or electronic systems that are not publicly accessible, whether privately or state-owned. Other interests such as property, morality, honor, national security and others must also be considered (Suseno, 2012).

The new Criminal Code also addresses interception or wiretapping activities. This is outlined in Article 258, which states:

(1) Any person who illegally listens to, records, redirects, alters, obstructs and/or records transmissions of Electronic Information and/or Electronic Documents that are not public, whether through communication cable networks or wireless networks, shall face imprisonment for up to 10 (ten) years or a fine of up to category VI.
(2) Any person who broadcasts or disseminates the outcomes of conversations or recordings as mentioned in paragraph (1) shall be subject to imprisonment for up to 10 (ten) years or a fine of up to category VI.
(3) The provisions of paragraph (1) do not apply to those who enforce legislative provisions or carry out official orders as specified in Article 31 and Article 32.

Wiretapping involves breaching or infiltrating networks, systems, or computers without authorization (Khasanah & Sutrabi, 2023). In English, hacking is known by various terms such as eavesdropping, bugging and wiretapping. Eavesdropping entails covertly listening to others' conversations, while bugging involves electronic surveillance, including covertly capturing, listening to or recording conversations through electronic devices. Wiretapping, on the other hand, refers to the covert interception of conversations by law enforcement with judicial authorization (Gardner, 2004).

Wiretapping offenses have occurred frequently in Indonesia, even on an international scale. One notable wiretapping incident in Indonesia involves Australia intercepting communications of the Indonesian government in 2009, particularly targeting individuals around the Indonesian Presidential Palace, including the president's family. This interception was part of the operational activities of the Australian Signals Directorate.

It is worth noting that Article 258 makes an exception for interception activities carried out by individuals executing official orders or conducting wiretapping in accordance with statutory regulations. Wiretapping is often conducted by law enforcement agencies to gather evidence or carry out sting operations. For instance, the Corruption Eradication Commission (KPK) conducts wiretapping to apprehend corrupt individuals.

In addressing the evolving cybercrimes, the Indonesian government has made efforts to create regulations that align with current conditions, such as the implementation of the new Criminal Code (KUHP). The KUHP includes provisions on hate speech, defamation, the spread of false information, and wiretapping. In addition to enacting more advanced regulations, Indonesia must also enhance its technology

security to prevent easy hacking or interception of information and communication technology within the country. This also involves improving monitoring and evaluation to ensure the new Criminal Code is implemented effectively and periodically.

Overall, the Criminal Code introduces more proportionate regulations for cybercrime sanctions. Unlike the previous EIT Law, which separated offenses and their corresponding penalties, the Criminal Code consolidates these aspects into a single article or paragraph, simplifying comprehension and enforcement. The principles of cybercrime offenses in the Criminal Code emphasize that a virtual criminal act must satisfy formal elements, such as meeting the conditions stipulated in the law, as well as material elements, including engaging in unlawful actions or cyber illegal acts.

5. Conclusion

The Indonesian government has ratified the new Criminal Code to establish a distinct legal framework for Indonesia and move away from laws inherited from the colonial era. Discussions surrounding the new Criminal Code have persisted for decades, with a continuous focus on evolving societal values. One such evolving value pertains to information and communication technology, which has now become integral to people's lives but also serves as a tool for cybercrime. As regulators, the government not only formulates policies based on theory but also considers real-life circumstances.

With the implementation of the new Criminal Code, several provisions in existing legislation have been amended, including those in the EIT Law. Provisions in the EIT Law regarding hate speech, defamation, dissemination of false information and wiretapping are now addressed within the new Criminal Code. This consolidation of criminal acts and sanctions aims to enhance clarity and ease of understanding.

Moreover, the enactment of the new Criminal Code facilitates the application of Indonesian criminal law to borderless crimes, given that cybercrimes often transcend geographical boundaries and are transnational in nature. This encompasses Indonesian citizens committing crimes abroad and foreign nationals posing threats to Indonesia's cybersecurity. Consequently, combating cybercrimes is expected to become more efficient.

In addition to implementing more advanced regulations, Indonesia must also bolster its technological security to prevent the easy hacking or interception of information and communication technology within the country. This can be achieved by engaging numerous IT experts in Indonesia. Collaborative efforts between law enforcement agencies and experts will significantly contribute to the fight against cybercrimes. Furthermore, promoting understanding and education among the general public, who interact closely with technology in their daily lives, is essential.

Another significant aspect of this legal evolution is the emphasis on technology security. While the new Criminal Code acknowledges the importance of strengthening cybersecurity, translating this acknowledgment into concrete actions is imperative. This involves not only the implementation of advanced security measures and technologies but also the establishment of robust protocols and public-private partnerships. Enhancing public awareness about cybersecurity threats and investing in continuous security improvements will be essential in safeguarding Indonesia's digital infrastructure against potential vulnerabilities.

In conclusion, the new Criminal Code marks a pivotal step in Indonesia's legal response to cybercrime, yet its success will depend on how well it is implemented and adapted to real-world conditions. Ensuring that law enforcement is well-prepared, safeguarding fundamental freedoms, and advancing technology security are all critical components of this endeavor. By addressing these areas thoughtfully and proactively, Indonesia can build a legal framework that effectively responds to the challenges of the digital age, fostering a secure and equitable online environment for its citizens.

Authors' contribution

Sigid Suseno:

1. Write articles and analyze regulations used as data.
2. Review the work and participate in checking.

3. Provide final approval for submitted journal articles
4. Agree be accountable for all aspects of the work in ensuring that questions related to the accuracy or integrity of any part of the work are appropriately investigated and resolved.

Ahmad M. Ramli:

1. Conceptualize topic and write this journal
2. Analyze regulations used as data.
3. Provide final approval for submitted journal articles.
4. Agree be accountable for all aspects of the work in ensuring that questions related to the accuracy or integrity of any part of the work are appropriately investigated and resolved.

Ranti Fauza Mayana:

1. Write and interpretate the substances to make this journal.
2. Carry out reviews during the journal writing process.
3. Provide final approval for submitted journal articles.
4. Agree to be accountable for all aspects of the work in ensuring that questions related to the accuracy or integrity of any part of the work are appropriately investigated and resolved.

Tasya Safiranita:

1. Write and conceptualize the main idea of this journal.
2. Correspondence and communicate with the journal during the manuscript submission, peer-review and publication process.
3. Provide final approval for submitted journal articles.
4. Agree to be accountable for all aspects of the work in ensuring that questions related to the accuracy or integrity of any part of the work are appropriately investigated and resolved.

Bernadette Aurellia Nathania Tiarma:

1. Write and analyze the regulations related to this journal topic.
2. Drafting and editing the journal.
3. Final approval of the version to be published;
4. Agree to be accountable for all aspects of the work in ensuring that questions related to the accuracy or integrity of any part of the work are appropriately investigated and resolved.

Disclosure statement

The authors of this journal declare that there are no relevant financial or nonfinancial competing interests to report.

Funding

This research's funding was received from Faculty of Law, Universitas Padjadjaran.

About the authors

Sigid Suseno is the Dean of Faculty of Law, Universitas Padjadjaran and also a cybercrime expert. He has written several journal publications, including books.

Ahmad M. Ramli is an Intellectual Property and Cyber Law expert from Universitas Padjadjaran. He is also actively works as an arbitrator at BANI.

Ranti Fauza Mayana is an Intellectual Property and Industrial Design Law expert from Universitas Padjadjaran. She has written a lot of publications, including books.

Tasya Safiranita is a Digital Copyright expert from Universitas Padjadjaran. She is actively teaching as a lecturer, and has written many books and journal article.

Bernadette Aurellia Nathania Tiarma is a graduate student from Faculty of Law, Universitas Padjadjaran. She is also active in writing journal and has co-wrote a book.

Data availability statement

Data can be made available upon reasonable request. The data that support the findings of this study are openly available in the internet through search engines. The regulations used as datas in this journal are openly available in https://peraturan.bpk.go.id/.

References

Ariyaningsih, S., Andrianto, A., Kusuma, A. S., & Prastyanti, R. A. (2023). Korelasi Kejahatan Siber dengan Percepatan Digitalisasi Indonesia. *Justisia: Jurnal Ilmu Hukum*, *1*(1), 1–11. https://doi.org/10.56457/jjih.v1i1.38

Arora, B. (2016). Exploring and analyzing internet crimes and their behaviours. *Perspectives in Science*, *8*, 540–542. https://doi.org/10.1016/j.pisc.2016.06.014

Carlaw, K., Oxley, L., Walker, P., Thorns, D., & Nuth, M. (2006). Beyond the hype: Intellectual property and the knowledge society/knowledge economy. *Journal of Economic Surveys*, *20*(4), 633–690. https://doi.org/10.1111/j.1467-6419.2006.00262.x

CNN Indonesia. (2023). *Polri Tangkap 866 Tersangka Judi Online dari 685 Kasus Sejak 2022*. https://www.cnnindonesia.com/nasional/20230831140426-12-992945/polri-tangkap-866-tersangka-judi-online-dari-685-kasus-sejak-2022

Daeng, Y., Levin, J., Karolina, M. R., Prayudha, N. P., Ramadhani Noverto, S., & Imanuel, V. (2023). Analisis Penerapan Sistem Keamanan Siber Terhadap Kejahatan SIber di Indonesia. *Innovative: Journal of Social Science Research*, *3*(2), 1135–1145.

Fakhriah, S., & Mutmainnah, I. 2024. Penerapan Sanksi Pidana Terhadap Kejahatan Siber: Sebuah Kajian Terhadap Perkembangan Hukum". *Journal of International Multidisciplinary Research*, *2*(1): 470–477. https://doi.org/10.62504/v0fym498

Gardner, B. A. (2004). *Black Law Dictionary*. Thomson.

Ginara, I. G. K., Widyantara, I. M. M., & Styawati, N. K. A. (2022). Kriminalisasi Terhadap Kejahatan Carding Sebagai Bentuk Cyber Crime Dalam Hukum Pidana Indonesia. *Jurnal Preferensi Hukum*, *3*(1), 138–142. https://doi.org/10.22225/jph.3.1.4673.138-142

Heartfield, R., Loukas, G., Budimir, S., Bezemskij, A., Fontaine, J. R. J., Filippoupolitis, A., & Roesch, E. (2018). A taxonomy of cyber-physical threats and impact in the smart home. *Computers & Security*, *78*, 398–428. https://doi.org/10.1016/j.cose.2018.07.011

Herera, D. A., & Hasan Sebyar, M. (2023). Perlindungan Hukum Terhadap Serangan Siber: Tinjauan Atas Kebijakan Dan Regulasi Terbaru. *Jurnal Hukum dan Kewarganegaraan*, *1*(4), 21–30. https://doi.org/10.3783/causa.v1i3.784

Hidayat R. (2023). *Mengulas Pengaturan Kejahatan Digital dalam KUHP Baru*. https://www.hukumonline.com/berita/a/mengulas-pengaturan-kejahatan-digital-dalam-kuhp-baru-lt63b3c9d523eb8/

Indradjaja, M. A. P., Suseno, S., & Ramadhani, R. H. (2022). Analisis. Penegakan Hukum Tindak Pidana Yang Dilakukan Dalam Lingkup Pinjaman Online Ilegal Di Indonesia. *Paulus Law Journal*, *3*(2), 50–64. https://ojs.ukipaulus.ac.id/index.php/plj/article/view/495. https://doi.org/10.51342/plj.v3i2.364

Khasanah, N., & Sutrabi, T. (2023). Analisis Kejahatan *Cybercrime* Pada Peratasan dan Penyadapan Aplikasi Whatsapp. *Blantika: Multidisciplinary Journal*, *2*(1), 44–55. https://doi.org/10.57096/blantika.v1i2.13

Kementerian Pertahanan Indonesia. (2014). *Pedoman Pertahanan Siber*. Kemhan RI.

Kurniawan M. A E (2023). *Sejarah UU ITE di Indonesia: Perkembangan Regulasi dan Kontroversi Dunia Digtal*. https://narasi.tv/read/narasi-daily/sejarah-uu-ite

Malau, P. (2023). Tinjauan Kitab Undang-Undang Hukum Pidana (KUHP) Baru 2023. *AL-MANHAJ: Jurnal Hukum Dan Pranata Sosial Islam*, *5*(1), 837–844. https://doi.org/10.37680/almanhaj.v5i1.2815

Manullang, S., Orba Verawati Br Tompul, Y., Kusumadewi, L. Y., Krisnalita., & M., Mutiarany. (2023). Daya Ikat KUHP Nasional Terhadap Eksistensi Undang-Undang Khusus Sebelumnya Ditinjau Dari Perspektif Filsafat Hukum. *Jurnal Pendidikan Tambusai*, *7*(2), 17340–17346. https://doi.org/10.31004/jptam.v7i2.9112

Maskun. (2013). *Criminal law: Cyber crime and criminal law in Indonesia*. Jakarta: Kencana.

Ramli, A. M. (2023). *Pasal-pasal "Cybercrime" UU ITE Dicabut oleh UU KUHP Baru*. https://nasional.kompas.com/read/2023/02/13/06450041/pasal-pasal-cyber-crime-uu-ite-dicabut-oleh-uu-kuhp-baru?page=all

Ramli, A. M., & Ramli, T. S. (2022). *Hukum Sebagai Infrastruktur Transformasi Indonesia*. Refika Aditama.

Renggong, R. (2017). *Hukum Pidana Khusus: Memahami delik-delik diluar KUHP*. Prenada Media.

Sari, A. P., & Harwika, D. M. (2022). Legal liability of artificial intelligence in perspective of civil law in Indonesia. *International Journal of Social Science Research and Review*, *5*, 57–60.

Situmeang, T. A., Amos, R., Ariska, & T. M., Ali. (2023). Tinjauan Hukum Tentang Pengaruh Judi Online Terhadap Perceraian. *Innovative: Journal of Social Science Research*, *3*(4), 3808–3817. https://doi.org/10.31004/innovative.v3i4.3891

Soerjono, S., & Mamuji, S. (2010). *Penelitian Hukum Normatif, Suatu Tinjauan Singkat*. Rajawali Pers.

Suseno, S. (2012). *Yurisdiksi Tindak Pidana Siber*. PT Refika Aditama.

Umbara, A., & Setiawan, D. A. (2022). Analisis kriminologis terhadap peningkatan kejahatan siber di masa pandemi covid-19. *Jurnal Riset Ilmu Hukum*, *2*, 81–88. https://doi.org/10.29313/jrih.v2i2.1324

Vitus, E. N. (2023). Cybercrime and online safety: Addressing the challenges and solutions related to cybercrime, online fraud, and ensuring a safe digital environment for all users—A case of African states. *TIJER - International Research Journal*, *10*(9), 975–989.

Wall, D. S. (2007). *Cyber crime: The transformation of crime in the information age*. Replika Press.

Westerlund, M. (2019). The emerge of deepfake technology: A review. *Technology Information Management Review*, *9*, 40–53.