Cybercrime and Data Security: The Role of Criminal Law in Coping Digital Threats

Mohamad Ismed

Email: ismedismed@gmail.com

University of Jayabaya, Jakarta, Indonesia

Article Info

Received: 2023 -08-28
Revised: 2024 -12-23
Accepted:2024-12-30

Keywords:
Cybercrime, Data Security, Criminal Law, Regulation, Law Enforcement.

Abstract

Development rapid digital technology has bring benefit big for society, but also improve risk cybercrime, especially related with data security. Various forms of cybercrime such as hacking, phishing, ransomware, and misuse of personal data the more threaten individuals, companies, and institution government. In the context of this, law criminal own role important in give protection and mitigation digital threats through clear regulations and enforcement effective law. Research This aiming for identify threatening forms of cybercrime data security, analyzing regulation law criminal in handle cybercrime, and evaluate effectiveness enforcement law in to overcome digital threats. The methods used is approach normative legal and empirical with analysis to regulation applicable legislation, studies literature, as well as various form weakness regulation based on from observation and interview from stakeholders. Research results This show that law criminal law in Indonesia is still face various challenge in protect data security from crime increasingly cyber complex. Although has There is regulation like Constitution Electronic Information and Transactions and Constitution Personal Data Protection, existing rules Still fragmented and more focused on security system compared to personal data protection in a way comprehensive. In addition, the limitations capacity apparatus enforcer law, weakness coordination between institutions, less sanctions give effect deterrent, and challenge jurisdiction in case cross country increasingly to complicate effort enforcement law. Modus operandi of cybercrime that continues developing, such as phishing, malware, and ransomware, are increasingly increase risk data theft and disturbance operational for individuals, companies and security national

1. INTRODUCTION

The rapid progress of information and communication technology has brought significant transformations to human life, changing how individuals and society interact, work, and access information. The internet and digital networks have become essential infrastructure supporting various daily activities, enabling instant communication without geographical barriers through social media, email, and instant messaging platforms (Putra, 2018). In the field of education, digital technology has expanded access to online learning resources, virtual classrooms, and e-learning platforms, allowing students to acquire knowledge without being physically present in a classroom. This convenience has also impacted the workplace, where remote work has become increasingly common, facilitating more efficient and flexible global collaboration (Astono, 2021).

In the economic sector, digitalization has transformed traditional business models into technology-based ones, with the emergence of e-commerce, digital financial services, and blockchain technology enhancing financial transaction efficiency. Businesses can now reach global markets more easily through digital platforms, while electronic payment systems simplify transactions for consumers (Disemadi & Kang, 2021). In governance, the implementation of e-government and data-driven systems has improved transparency and the efficiency of public services, enabling citizens to access administrative services more quickly and conveniently (Rosmayati, 2023). However, despite these benefits, the increasing reliance on digital technology also presents new challenges, such as data security threats, cybercrime, and the digital divide, which must be addressed for the development of inclusive and sustainable technology.

Cybercrime has become a serious threat in the digital era, with widespread impacts on individuals, businesses, and governments. As technology rapidly evolves, various forms of cybercrime continue to emerge, including hacking, personal data theft, malware attacks, and financial crimes such as phishing and skimming (Aini & Lubis, 2024). Cybercriminals exploit security vulnerabilities in digital systems to steal information, damage technological infrastructure, or even commit extortion through ransomware attacks. Cyberattacks not only cause financial losses but also threaten victims' privacy and reputations, undermining trust in digital security systems and disrupting a nation's economic and social stability (Balaka et al., 2024). The complexity of cybercrime has increased with the emergence of new technologies such as artificial intelligence (AI), the Internet of Things (IoT), and cloud computing, presenting additional challenges in data security. Cyberattacks are no longer solely conducted by individuals or small groups but also involve organized crime syndicates operating across borders. This makes combating cybercrime more difficult, requiring international cooperation, strict legal regulations, and enhanced public awareness and digital literacy (Raihana et al., 2023).

One of the most rampant forms of cybercrime is the misuse of personal data, where sensitive information is exploited without consent for various purposes, including identity theft, financial fraud, and social manipulation (Situmeang, 2021). In the 21st century digital era, personal data has become a highly valuable "commodity"

for both businesses and cybercriminals. The increasing shift from physical to digital activities—such as social media use, online transactions, and data-driven applications—often leads individuals to unknowingly share vast amounts of personal information (Arrasuli & Fahmi, 2023). Data such as names, addresses, phone numbers, and online activity records become easy targets for those seeking to misuse them. Security loopholes in digital systems, combined with low public awareness of data protection, further exacerbate the situation. As a result, the misuse of personal data can lead to financial harm, reputational damage, and threats to privacy and individual freedom (Kurniawati & Yunanto, 2022).

In Indonesia, regulations concerning personal data protection are outlined in several laws, including Law No. 10 of 1998 on Banking, Law No. 36 of 2009 on Health, Law No. 24 of 2013 on Population Administration, and Law No. 19 of 2016, which amends Law No. 11 of 2008 on Electronic Information and Transactions (Hisbulloh, 2021). However, Article 26(1) of the ITE Law, which addresses electronic information containing personal data, does not explicitly define data protection principles, data owners' rights, or adequate government and stakeholder responsibilities in data management. As a result, there is a lack of clarity regarding the limitations on personal data usage and effective protection mechanisms for the public (Annan, 2024).

Additionally, Article 26(2) states that the consequences of a personal data breach are limited to compensation for damages, without imposing stricter sanctions on offenders. This highlights the weak position of personal data owners, particularly in cases where they are unaware that their data has been misused. The state's role in personal data protection remains passive, leading to suboptimal enforcement (Rizal, 2019). Although laws recognize individuals' rights to self-protection, specific aspects of personal data protection have not yet been comprehensively regulated. As bureaucratic reforms continue to promote digitalization in government services, the challenges in personal data protection are becoming even greater (Niffari, 2020).

Study This focus on several problem main related to cybercrime and data security in perspective law criminal. First, how shape and characteristics cybercrime threat data security in the digital age. Second, to what extent is the regulation law criminal law in Indonesia has protect data security from cybercrime threats, especially in the ITE Law and regulations others. Lastly, what just weakness in system law Indonesian criminal law in handle cybercrime and personal data protection, including in aspect enforcement law.

Study This aiming For analyze shape and characteristics cybercrime threat data security and evaluate effectiveness regulation law criminal law in Indonesia in handle threat In addition, the research this also aims For identify weakness in system law criminal related to cybercrime and personal data protection as well as formulate strategies that can strengthen role law criminal in to overcome digital threats. As for the benefits from study This is give outlook for maker policy in compile more regulation strict and comprehensive, helpful apparatus enforcer law in increase effectiveness Handling cybercrime cases, as well as increase awareness public will importance personal data protection in the digital age.

2. METHODS

This study employs both normative and empirical legal methods to analyze the role of criminal law in addressing cybercrime threats and ensuring personal data protection. The normative legal approach involves examining existing laws and regulations in Indonesia, such as the Information and Electronic Transactions Law (ITE Law), the Personal Data Protection Law, and other relevant regulations related to cybersecurity (Efendi et al., 2016). Additionally, this research aims to assess the effectiveness and shortcomings of these legal provisions. A document study of legal literature, scholarly journals, and court decisions is conducted to understand the principles of criminal law in handling cybercrime cases and the extent to which the law provides optimal protection for public personal data.

On the other hand, the empirical legal approach is used to examine how criminal law is implemented in handling cybercrime cases in Indonesia. This research includes interviews with law enforcement officials, academics, and other relevant stakeholders to gain practical insights into the challenges and obstacles faced in enforcing cybercrime laws (Yanova et al., 2023). Furthermore, the study analyzes past cybercrime cases to understand how existing regulations are applied in practice and the extent to which legal protection for victims is effectively realized. By combining normative and empirical approaches, this research aims to provide comprehensive recommendations for strengthening the role of criminal law in combating digital threats and enhancing personal data protection in the digital era.

3. RESULTS AND DISCUSSION

Forms and Characteristics of Cybercrime that Threaten Data Security in the Digital Era

In the digital era that continues developing, threat to online security is increasingly increase along with rapid progress technology. One of the aspects that become attention main is various types of cybercrime that are increasingly complex and difficult controlled. Cybercrime is not Again limited to action simple like hacking social media accounts, but has develop become more attacks sophisticated, such as personal data theft, fraud digital -based, ransomware attacks, to sabotage infrastructure important owned by government and companies big (Djanggih & Qamar, 2018). Attack cyber This No only harm individual with theft identity and abuse information personal, but also has an impact on the sector economy and security national. In addition, cybercrime the more organized with existence groups hackers operating at the level international, using technology advanced for infiltrate to system and steal information valuable (Wahyudi, 2013).

For understand and overcome risk this is important for We For dive into the variety of types cybercrime that threatens data security that may lurk behind our digital screen.

1. hishing

Phishing is one of the most common and dangerous forms of cybercrime, where perpetrators attempt to trick victims by disguising themselves as trusted entities to steal personal information, such as passwords, credit card numbers, or banking

account details. The modus operandi of phishing usually involves emails, text messages, or fake websites designed to closely resemble official sites (Dm et al., 2022). Victims who are unaware often fall for these scams and unknowingly enter their personal information, which is then used by cybercriminals for identity theft, financial fraud, or unauthorized access to their accounts.

Additionally, phishing can be carried out through social engineering techniques, where perpetrators manipulate victims psychologically by sending messages that appear urgent or important, such as account suspension notices or transaction confirmation requests. The impact of phishing attacks can be highly detrimental to both individuals and organizations. Victims may lose access to their important accounts, suffer financial losses, or become targets of further cybercrimes such as digital extortion. For companies, phishing attacks can lead to sensitive data breaches, reputational damage, and significant financial losses.

2. Malware

Malware, short for malicious software, refers to harmful programs designed to damage, steal, or gain unauthorized access to data. Malware comes in various forms, including viruses, worms, trojans, ransomware, spyware, and adware. Viruses and worms spread quickly from one device to another, causing system damage or deleting critical data. Trojans often disguise themselves as legitimate programs to deceive users into installing them, while ransomware encrypts victims' data and demands a ransom, usually in cryptocurrency, to restore access (Rachmadie, 2020).

Spyware secretly monitors user activities to steal private information, while adware displays malicious advertisements that can lead users to malware-infected websites. The impact of malware can be devastating for both individuals and organizations. Affected individuals may lose personal data, become victims of identity theft, or lose access to their devices. For companies and large institutions, malware can lead to confidential data breaches, operational system failures, and serious cybersecurity threats.

3. Ransomware

Ransomware is a type of malware designed to encrypt a victim's data, making it inaccessible without a decryption key held by the attacker. Once the data is locked, the perpetrator demands a ransom, often in cryptocurrency like Bitcoin, in exchange for restoring access. Ransomware attacks are commonly spread through phishing emails, malicious websites, or security vulnerabilities in operating systems and software (Ramadhan, 2023).

Once ransomware infects a device, all important files—ranging from personal documents to corporate operational systems—become inaccessible. Some ransomware attacks even include a "double extortion" tactic, where attackers not only encrypt data but also threaten to leak sensitive information if the ransom is not paid. The consequences of ransomware attacks can be severe, affecting individuals, businesses, hospitals, government institutions, and multinational corporations. In addition to causing major operational disruptions, ransomware attacks can result in data leaks and substantial financial losses. Moreover, paying the ransom does not guarantee data recovery, as attackers may withhold the decryption key or even target

the same victims again in the future.

4. DDoS

A Distributed Denial-of-Service (DDoS) attack is a type of cyberattack aimed at making an online service unavailable to legitimate users. This attack is carried out by overwhelming a server, network, or system with excessive traffic, ultimately overloading its capacity and rendering it unresponsive. DDoS attacks are often executed using botnets—a network of infected devices controlled remotely by hackers without the knowledge of the device owners. These attacks can last from minutes to days, depending on the scale and objectives of the attacker (Suwiknyo, 2021).

The impact of DDoS attacks can be highly damaging, especially for businesses that rely on online services, such as e-commerce, digital banking, or public service platforms. When systems become inaccessible, businesses suffer financial losses, lose customer trust, and experience reputational damage. Additionally, DDoS attacks are sometimes used as a distraction to divert security teams' attention while cybercriminals infiltrate systems or steal sensitive data. To prevent and mitigate DDoS attacks, organizations can implement strong firewalls, deploy early detection systems, and use network security services capable of filtering suspicious traffic before it reaches the main server.

5. Carding

Carding is a form of cybercrime involving the theft or unauthorized use of someone else's credit or debit card information to conduct fraudulent online transactions. Stolen card data is often obtained through illegal methods such as phishing, malware that captures payment details, or data breaches on insecure websites with inadequate security systems. Additionally, cybercriminals frequently purchase stolen card information from the dark web, where credit card details are sold in bulk at varying prices depending on their balance limits and security levels (Kurniawan & Soeskandhi, 2022).

The impact of carding is severe for both cardholders and financial institutions. Victims often realize they have been targeted only after noticing unauthorized transactions on their account statements. Besides causing financial losses, carding also erodes public trust in digital payment systems. To counter carding, banks and financial service providers must continuously enhance their security systems using encryption technologies, two-factor authentication, and real-time fraud detection systems. Additionally, card users should practice safe online transaction habits by only using trusted websites and never sharing their card details with unknown parties.

6. Typosquatting

Typosquatting, also known as URL hijacking, is a cybercrime that exploits users' typographical errors when entering website addresses in their browser. Typosquatters create domains with names that closely resemble legitimate websites but have slight variations, such as adding or omitting letters, using different domain extensions, or replacing similar-looking characters (e.g., replacing the letter "o" with the number "0"). The main objective of this attack is to trick users into visiting fake sites, which are often used to steal personal information, spread malware, or display

malicious advertisements.

The impact of typosquatting can be particularly dangerous if fake sites are used to steal login credentials for banking accounts, emails, or social media (Maulana, 2022). Large companies may also suffer reputational damage if customers fall victim to fraudulent websites impersonating their official services. To avoid typosquatting threats, users should always double-check website addresses before pressing "Enter" and use bookmarks to access frequently visited sites. Meanwhile, companies can protect their brand by registering similar domain variations and implementing security measures such as SSL (Secure Sockets Layer) certificates to verify the authenticity of their official websites.

Criminal Law in Indonesia in Protect Data Security from Cybercrime Threats

In Indonesia, attacks cyber become an increasingly common issue worrying along with increasing digitalization in various sector. Various incident hacking to system information national show that awareness will threat cyber Still low, both among individuals, institutions, and maker policy (Parulian et al., 2021). One of the reason main is lack of strong and comprehensive regulation in arrange security cyber, so that Lots organization that has not own standard adequate data protection. In addition, many stakeholders interests that still exist lay to risk cyber and technology security, make response to threat become slow and lacking effective. As a result, the system information important, including service public and digital banking, vulnerable to attack potential cyber detrimental to the country and public wide (Najwa, 2024).

The provisions regarding personal data information in Indonesia are still regulated partially and have been mentioned in several sectoral laws that regulate the confidentiality of personal information/data. There are at least 32 laws whose material is related to the regulation of personal data, ranging from the financial sector, taxation, security, population, archiving, telecommunications law enforcement, banking to the health sector. The author will explain several laws related to personal data that affect the use of technology.

1. **According to Law Number 11 of 2008 concerning Electronic Information and Transactions**

Regulations related to the use of technology involving electronic data or information have been regulated in Law Number 19 of 2016, which is an amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE). In this regulation, there are provisions regarding personal data, but the law does not provide a clear definition of what is meant by personal data. In addition, protection of personal data in the ITE Law has not been regulated comprehensively. The provisions in this law only mention that the use of information technology involving personal data is part of personal rights (privacy rights), including the individual's right to enjoy their personal life without interference, communicate without intervention from other parties, and monitor and access their personal information. However, this regulation is still general and does not provide concrete protection for personal data which is increasingly vulnerable in the digital era.

As a form of implementing the rules in the ITE Law, more technical regulations regarding electronic transaction system organizers (PSTE) have been regulated in the relevant Ministerial Regulation. This regulation provides a more specific definition of personal data, namely as certain individual data that is stored, maintained, kept true, and its confidentiality protected. Thus, the protection of personal data relies more on derivative regulations than the ITE Law itself. This shows that the main law focuses more on regulating electronic transactions and information in general, while more specific aspects, such as personal data protection, are regulated in more detailed regulations at the sectoral policy level.

Unfortunately, this approach poses its own challenges, especially in creating an integrated and robust personal data protection system in Indonesia. Because personal data protection regulations are spread across various sectoral regulations, there is a potential for inconsistency in their implementation. This can cause confusion for the public and digital service providers in understanding their obligations and rights regarding personal data. In several other countries, personal data protection has been regulated in specific laws that provide a clearer and more detailed legal framework, such as the General Data Protection Regulation (GDPR) in the European Union. Therefore, Indonesia needs to consider drafting more centralized and comprehensive regulations to ensure that personal data protection can be effectively enforced across all sectors.

Article 26 of the ITE Law provides condition that every use of personal data in an electronic media must moreover formerly get agreement the owner of the data concerned. The parties who violate can sued on losses incurred. The contents from Article 26 of the ITE Law, namely as following:

1) Except otherwise determined by regulations legislation, use every information through electronic media concerning personal data somebody must done on the consent of the person concerned.
2) Every person who is violated his rights as intended verse 1 can to propose lawsuit on losses incurred based on Constitution.
3) Every organizer system electronic must delete information electronic and / or document electronics that are not relevant that is under his control on request of the person concerned based on determination court.
4) Every organizing system electronic must sad mechanism deletion information electronics and/ or document electronics that are not relevant in accordance with provision regulation legislation.
5) Provision regarding procedures deletion information electronics and/ or document electronic as the meaning of paragraph 3 and paragraph 4 is regulated in regulation government

Article 15 of the Law Information and Electronic Transactions (ITE Law) requires every Organizer Electronic System (PSE) for operate the system with safe, reliable, and responsible answer use ensure optimal service. Terms This applicable for all organizer systems, both those operating in the sector government, commercial, and individual. This is means that every managing party system electronic must ensure security of stored data, preventing leakage information, as well as ensure that the

system used No easy hacked or misused by unauthorized parties responsible answer. In more context broad, responsible answer This covers implementation steps security like data encryption, authentication users, as well as monitoring to threat cyber that can bother operational system. In addition, the organizer the system is also expected for own mechanism recovery If happen incident security, so that can minimize impact negative effects caused to users. With Thus, the provisions This aiming for increase trust public to system electronic as well as ensure that digital transactions and communications can in progress in a way safe and efficient.

Furthermore, the provisions stipulated in ITE Law against persons or the party which is perpetrator crime against personal data with access without permission or without agreement over other people's data is regulated in Article 30. Article 30 of the ITE Law regulates about action access without permission against personal data or information electronic belongs to someone else as form crime known cyber with illegal access terms. Provisions This aiming for protect system electronic from infiltration or access No valid that can endanger data security and privacy. In its implementation, the system security electronic must designed with a mechanism capable of limit access based on classification users and levels the authority held, such as system authentication layered, data encryption, and firewalls that prevent hacking. With existence regulation this, the perpetrator who with on purpose enter to in system without permission can charged sanctions law in accordance applicable regulations. Therefore that, the implementation data and system security electronic become aspect crucial in prevent the occurrence violation as well as ensure personal data protection from threat crime increasingly cyber complex.

Article 32 of the ITE Law regulates about action deletion, destruction, or data changes as form violation law that can harm data owner. Deletion of data in context This No only just remove information from system, but also includes the action that caused the data to not can recognized, accessed, or used as should be by the owner. This process can done with various way, such as obstruct access, encrypt data permanent without permission, or modify data structure so that system No Again can read it with true. In addition, data destruction can also happen through technique such as data wiping or overwriting, which aims to for destroy information in a way permanent. Changes or modification against the data can covers manipulation information, good with objective misleading, abusing, or for interest certain that violate law. Therefore that, the rules This give protection law for data owner from threats that can remove or damage information important, and ensure that perpetrator the crime committed action the can charged sanctions in accordance with applicable law.

ITE Law only give protection to information or electronic data in context security system, such as burglary system computers and access illegal. However, the regulation This not yet optimal in ensure protection to various form cybercrime others, including personal data breach. Personal data that is privacy is very much related with personal space and territoriality, where personal space is disturbed when There is intervention party others, while territoriality related with right ownership somebody on a environment certain. Privacy Alone nature subjective, where each

individual own control to level openness information his personal. Unfortunately, many regulations outside the Criminal Code do not in a way clear classify personal data breach as crime, so that cause constraint in implementation law. As a result, the certainty law and protection right individual against personal data Still difficult realized.

2. Constitution Number 27 of 2022 concerning Personal Data Protection

On October 17, 2022, Indonesia officially to validate Constitution Number 27 of 2022 concerning Personal Data Protection (PDP Law). Law This is milestone important in state efforts to protect personal data its citizens in the increasingly digital era develop rapidly. With development technology increasingly information advanced, protection against personal data become a very vital issue for guard right privacy individual as well as security information in cyberspace.

Law Number 27 of 2022 aims to for give more protection Good against personal data citizen. Law This ensure that every individual own right for control and safeguard his personal data from abuse. Regulation This arrange in a way strict how data is collected, processed, used, and shared by third parties third, including government and companies, in order to prevent detrimental action data owner. In addition, the law This obligatory every data manager for guard security information from leakage or attack cyber, so that risk theft or data exploitation can minimized. With existence protection more laws clear, expected Constitution This can increase trust public to digital system used in various sectors, including government and business. Clarity regulation will create a more digital ecosystem safe and transparent, so that public can transact and interact digitally without worry to misuse of his personal data. Ultimately, this law expected capable push development a more digital economy responsible responsible and sustainable.

This law No only applicable for personal data managed by the government, but also includes sector private. Every organization, both within and abroad, which collects, processes, or storing personal data Indonesian citizens, mandatory comply provision in Constitution This. In addition, the PDP Law also provides protection to rights individual on his personal data. Every individual entitled access personal data managed by the party data controller and own right for fix data if found inaccuracy. In addition, individuals can request deletion of personal data (right to erasure) if the data is No Again required or processing No valid. Not only that, individuals also have the right interesting prior agreement given related processing of his personal data, providing control full to data owner on related information with himself.

In general explicit, form personal data protection in the PDP Law is confession to the rights held by personal data subjects that is for:

a. Get clarity information about who, why and how personal data the will used, includes clarity identity, basis interest law, purpose requests and use of personal data, as well as accountability the requesting party (Article 5).
b. Complete personal data including update and fix error or inaccuracy of personal data (Article 6).
c. Access and obtain copy of personal data (Article 7).
d. End processing, deleting and destroying personal data his own (Article 8).

e. Interesting return agreement processing (Article 9)
f. Submit object on profiling actions that become base taking decisions that have an impact law (Article 10).
g. Postpone or limit processing (Article 11).
h. Demanding and receiving change make a loss on violation (Article 12)
i. Obtaining, using and sending personal data in form that can read by system electronics. (Article 13).

As law positive, Law Personal Data Protection arrange provision sanctions and mechanisms settlement dispute related violation to personal data. If the controller or data processor violates his obligation until cause loss for data subjects, they can charged sanctions administrative. Form sanctions This covering warning written, termination temporary activity data processing, deletion or destruction of personal data, as well as fine administrative which can reach two percent of total revenue annual the company concerned. Sanctions This aiming for to uphold compliance to provision personal data protection as well as give effect deterrent for perpetrator violation.

In terms of happen dispute personal data protection, Act Personal Data Protection set a number of track possible solution taken. Dispute can completed through arbitration, court, or institution settlement dispute alternative. The process of completion This must follow applicable procedural law in accordance with regulation legislation that regulates mechanism settlement dispute in Indonesia. With existence provision this, individual or the party who feels his rights on personal data has violated own track clear law for look for justice. In addition, Law Personal Data Protection also confirms prohibition use of personal data in a way oppose law. Prohibition This covers action collection, disclosure and use of personal data that is not his without valid permission, as well as falsification of personal data with objective to obtain profit potential person harm other party. Violation to prohibition This can charged punishment criminal in the form of prison during four until six year as well as fines ranging from between four until six billion rupiah.

For violators who are corporation, law Personal Data Protection enforce provision more sanctions weight. If a company proven do violation to personal data protection, they can charged fine until tenfold from the maximum limit the fine imposed for individual. In addition, sanctions addition can applied, such as robbery benefits gained from violation, freezing business, prohibition permanent operating, closing place business, revocation permission business, until dissolution corporation. Provisions This show commitment government in take action firm violation against personal data as well as ensure that personal data protection become priority in Indonesia's digital ecosystem.

Weakness Indonesian Criminal Law System in Handling Cybercrime and personal data protection

Protection of personal data No only aiming for increase awareness and respect to importance safeguard individual data, but also to ensure right top citizen protection self from abuse information personal. In the increasingly digital era forward, personal

data become vulnerable assets to various threats, such as theft, misuse, and exploitation by unauthorized parties responsible answer (Fauzy & Shandy, 2022). Therefore that, the government has emit various regulations that govern personal data protection in a number of regulation legislation use ensure that rights individual still protected. However, in order for the protection This can walk in a way effective, required effort improvement implementation and enforcement more laws strict, including supervision to compliance by institutions government and sector private. With existence clear regulations and enforcement strong law, personal data protection can guaranteed, so that public can more believe in interact in the digital world without worry will violation to privacy they.

From several results interview from the enforcers law and academics who become source informant so obtained a number of weakness in system law Indonesian criminal law. Some weakness main includes:

1. Absence Comprehensive and Specific Regulations

System law criminal law in Indonesia is still face challenge big in handle cybercrime and personal data protection consequence absence comprehensive and specific regulations. Although Constitution Electronic Information and Transactions and Constitution Personal Data Protection has enforced, existing regulations Still fragmented and not yet capable accommodate complexity cybercrime that continues developing. Various type attack cyber, such as phishing, hacking, and misuse of personal data, have not set up in a way Details in law positive Indonesia, so that apparatus enforcer law often face difficulty in interpret as well as apply existing rules. In addition, the lack of clear standards in regulation cause difference in the process of investigation and prosecution, so that enforcement law become no consistent and vulnerable to gap law that can exploited by the perpetrator crime.

Apart from the aspects technical, absence Specific regulations also have an impact on the weakness protection rights individual against personal data. Law Personal Data Protection of course has give framework law basic, but Still Lots aspects that need to be considered clarified, such as mechanism supervision, standards data security, and procedures enforcement sanctions to violations. In addition, there has not been existence institution independent which is special supervise compliance to personal data protection the more weaken effectiveness existing regulations. This is resulting in still height incident data leak without existence strict sanctions for responsible party answer. With Not yet existence comprehensive and specific regulations, system law criminal law in Indonesia is still left behind in give optimal protection against society in the increasingly digital era prone to to threat cybercrime.

2. Limitations Law Enforcement and Capacity Apparatus

Limitations in enforcement law and capacity apparatus be one of challenge main in handle cybercrime and personal data protection in Indonesia. The authorities enforcer law, such as police and prosecutors, still face constraint in matter source Power human beings who have skill specializing in the field digital forensics and investigation cybercrime.crime cyber own different characteristics from crime conventional, where the perpetrator often use technology advanced for disguise identity and location them, so that demand skills as well as deep understanding to

system security cyber. However, the limitations amount power expert who has competence in the field This hinder the process of identification, tracking, and disclosure case cybercrime in a way effective. As a result, many case cybercrime that is not revealed or the solution need a very long time, so reduce effectiveness enforcement law.

Apart from the limitations source Power human, infrastructure investigations that are still minimal also become constraint big in Handling cybercrime. Many officers enforcer law Not yet own access to technology and devices soft competent digital forensics for analyze proof electronic in a way fast and accurate. In addition, the work the same between institution enforcer law with party private and providers internet service in obtain the necessary data for the investigation is still ongoing not optimal. Lack of facilities and procedures standard in Handling goods digital evidence leads to the process of proof in court often not Enough strong for to ensnare perpetrator cybercrime. With condition this, cybercrime Keep going develop with more speed tall compared to with ability apparatus in overcome it, so that cause risk big for security of personal data and digital transactions in Indonesia.

3. Weakness Coordination inter- institutional

Weakness coordination between institution be one of constraint main in handle cybercrime and personal data protection in Indonesia. Crime cases cyber often of a nature complex and cross sector, so that need Work the same close between various agencies, such as police, Ministry of Communication and Information, Financial Services Authority, Bank Indonesia, and sector banking and telecommunications. However, until moment this, coordination between institution the Still not optimal. The absence of system integrated for share digital forensic information and data causes each agency Work in a way separated with different mechanisms. As a result, the response to incident cybercrime, such as hacking, theft identity, or personal data leaks, often running slow and not effective, so that perpetrator can with easy remove footsteps or continue the action is elsewhere.

In addition, the lack of harmonization regulations and procedures between the competent authorities also complicate things enforcement law to cybercrime. In some case, overlap overlap authority between agency government cause confusion in determine who is responsible answer in handle a case. This is resulting in the process of investigation and action become obstructed, while victims of cybercrime No quick get protection or recovery right them. Lack of coordination also has an impact on efforts prevention, where not yet There is system warning integrated early between institution for detect and address potential attack cyber in a way fast. With situation this, effort for increase personal data protection and mitigation cybercrime Still face challenge big, especially in build strong synergy between stakeholders interest.

4. Insufficient Punishment Deterrent effect

One of weakness in system law Indonesian criminal law in handle cybercrime is less punishment give effect deterrent for the perpetrators. Although Constitution Personal Data Protection and the Law Electronic Information and Transactions have arrange sanctions for offender, the punishment given often considered No comparable with the impacts caused. For example, the fines imposed to perpetrator cybercrime

often more small compared to the benefits they get get from his actions. As a result, the perpetrators still motivated For do action similar Because existing sanctions No Enough scary or harm for them. In addition, the punishment the criminal penalties applied are also still limited in to ensnare actor the intellectual behind cybercrime, especially for those who operate in network organized.

Not only that, in a number of case big impact wide to society, the punishment given to perpetrator cybercrime tend light and not comparable with losses experienced by the victim. For example, in case personal data leaks that include millions users, often the sanctions given only in the form of fine administrative without There is punishment heavy for responsible party answer. This is cause distrust public to system existing laws and show that regulation moment This Still own gap that can exploited by the perpetrator crime. Weakness sanctions also contribute to increasing amount case cybercrime Because No existence consequence sufficient law For press number violation. Therefore that, effectiveness law in give protection regarding personal data and addressing cybercrime Still become challenge big need fixed.

5. Challenge Jurisdiction in International Cases

Challenge jurisdiction in case cybercrime international be one of obstacle big in enforcement law in Indonesia. Many crimes cyber carried out by the perpetrators who operate from abroad, good in a way individual and in group organized. This is make legal process become more complicated Because every country has different regulations related cybercrime and personal data protection. In addition, no all countries have policy extradition or agreement Work The same with Indonesia in handle act crime cross- border. As a result, many perpetrator cybercrime is hard tracked and prosecuted in a way law Because constrained by jurisdictional boundaries national.

Apart from the obstacles in take action perpetrators who are abroad, investigation cybercrime cross- country also faces various obstacle technical and administrative. The process of collecting digital evidence often requires access against servers or data located outside the jurisdiction of Indonesia, while Work The same between countries in share information digital forensics still limited. The lack of bilateral or multilateral agreements in handle cybercrime make Indonesia difficult in do effective investigation. As a result, many case attack cyber or personal data theft that results in without settlement clear law, so that give gap for perpetrator For Keep going operate his action without Afraid will consequence real law.

4. CONCLUSION

In an increasingly digital era progress, cybercrime develop with level high complexity, threatening security of individual, corporate and even global data security national. Various form attack such as phishing, malware, ransomware, DDoS, carding, and typosquatting show that threat cyber No only impact on aspects financial, but also damaging reputation and operations a entity. With an increasingly sophisticated modus operandi sophisticated, the perpetrators cybercrime utilise gap security and manipulation psychological For steal information valuable as well as

bother digital system. Criminal law in Indonesia in protect data security from threat cybercrime Still face various challenges, especially related regulations that are spread across many constitution sectoral. Law Information and Electronic Transactions Law Number 11 of 2008 in conjunction with Constitution Number 19 of 2016 regulates use of personal data in transaction electronics, but not yet give comprehensive protection. Article 26 in Constitution the obligatory agreement data owner in its use, while Articles 30 and 32 regulate sanctions for access illegal as well as deletion or data destruction. However, the law This more focused on security system compared to personal data protection in a way specifically for overcome emptiness law This, Indonesia ratified Constitution Number 27 of 2022 concerning Personal Data Protection, which provides framework law more clear in personal data management, requires protection strict by the organizer system electronics, as well as ensure right individual on his personal data. The system law Indonesian criminal law still face various weakness in handle cybercrime and personal data protection, including absence comprehensive regulation, limitations capacity apparatus enforcer law, weakness coordination between institutions, less punishment give effect deterrent, and challenge jurisdiction in case international. Existing regulations Still fragmented and not yet capable accommodate complexity cybercrime, while apparatus enforcer law Still lack source power and expertise in investigation digital forensics. Lack of coordination effective between institution cause slowness response to incident cybercrime, while light sanctions No Enough press number violations. In addition, the challenges jurisdiction in case cross country hamper enforcement law to the perpetrators who operate from overseas.

REFERENCES

Aini, N., & Lubis, F. (2024). Tantangan Pembuktian Dalam Kasus Kejahatan Siber. *Judge: Jurnal Hukum*, *5*(02), 55-63.

Annan, A. (2024). Tinjauan Yuridis Perlindungan Data Pribadi Pada Sektor Kesehatan Berdasarkan Undang-Undang No. 27 Tahun 2022. *Synergy: Jurnal Ilmiah Multidisiplin*, *1*(04), 247-254.

Arrasuli, B. K., & Fahmi, K. (2023). Perlindungan hukum positif Indonesia terhadap kejahatan penyalahgunaan data pribadi. *UNES Journal of Swara Justisia*, *7*(2), 369-392.

Astomo, P. (2021). Politik Hukum Penyelenggaraan Sistem Pendidikan Nasional Yang Responsif Di Era Globalisasi. *Masalah-Masalah Hukum*, *50*(2), 172-183.

Balaka, K. I., Hakim, A. R., & Sulistyany, F. D. (2024). Pencurian Informasi Nasabah Di Sektor Perbankan: Ancaman Serius Di Era Digital. *Yustitiabelen*, *10*(2), 105-130.

Disemadi, H. S., & Kang, C. (2021). Tantangan Penegakan Hukum Hak Kekayaan Intelektual dalam Pengembangan Ekonomi Kreatif di Era Revolusi Industri 4.0. *Jurnal Komunikasi Hukum (JKH)*, *7*(1), 54-71.

Djanggih, H., & Qamar, N. (2018). Penerapan teori-teori kriminologi dalam penanggulangan kejahatan siber (cyber crime). *Pandecta Research Law Journal*, *13*(1), 10-23.

Dm, M. Y., Addermi, A., & Lim, J. (2022). Kejahatan Phising dalam Dunia Cyber Crime dan Sistem Hukum di Indonesia. *Jurnal Pendidikan dan Konseling (JPDK)*, *4*(5), 8018-

8023.
Efendi, J., Ibrahim, J., & Rijadi, P. (2016). Metode Penelitian Hukum: Normatif dan Empiris.
Fauzy, E., & Shandy, N. A. R. (2022). Hak Atas Privasi dan Politik Hukum Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi. *Lex Renaissance*, *7*(3), 445-461.
Hisbulloh, M. H. (2021). Urgensi rancangan undang-undang (RUU) perlindungan data pribadi. *Jurnal Hukum*, *37*(2), 119-133.
Kurniawan, A. B., & Soeskandhi, H. (2022). Perlindungan Hukum Kepada Pengguna Elektronik Banking Atas Kejahatan Carding Ditinjau Dari Undang-Undang Informasi dan Transaksi Elektronik. *SUPREMASI: Jurnal Hukum*, *5*(1), 64-87.
Kurniawati, H., & Yunanto, Y. (2022). Perlindungan Hukum Terhadap Penyalahgunaan Data Pribadi Debitur Dalam Aktivitas Pinjaman Online. *Jurnal Ius Constituendum*, *7*(1), 102-114.
Maulana, M. A. (2022). Typosquatting: Ancaman dan Dampaknya dalam Kejahatan Teknologi Informasi. *Fairness and Justice: Jurnal Ilmiah Ilmu Hukum*, *20*(2), 104-113.
Najwa, F. R. (2024). Analisis Hukum Terhadap Tantangan Keamanan Siber: Studi Kasus Penegakan Hukum Siber di Indonesia. *AL-BAHTS: Jurnal Ilmu Sosial, Politik, dan Hukum*, *2*(1), 8-16.
Niffari, H. (2020). Perlindungan Data Pribadi Sebagai Bagian Dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi (Suatu Tinjauan Komparatif Dengan Peraturan Perundang-Undangan Di Negara Lain). *Jurnal Yuridis*, *7*(1), 105-119.
Parulian, S., Pratiwi, D. A., & Yustina, M. C. (2021). Studi tentang ancaman dan solusi serangan siber di indonesia. *Telecommunications, Networks, Electronics, and Computer Technologies (TELNECT)*, *1*(2), 85-92.
Putra, M. (2018). Hukum Dan Perubahan Sosial (Tinjauan Terhadap Modernisasi Dari Aspek Kemajuan Teknologi). *MORALITY: Jurnal Ilmu Hukum*, *4*(1), 47-59.
Rachmadie, D. T. (2020). Regulasi Penyimpangan Artificial Intelligence Pada Tindak Pidana Malware Berdasarkan Undang-Udang Republik Indonesia Nomor 19 Tahun 2016. *Recidive: Jurnal Hukum Pidana Dan Penanggulangan Kejahatan*, *9*(2), 128-156.
Raihana, R., Sari, T. E. K., & Fanny, F. (2023). Tindak Pidana Pencucian Uang Perspektif Hukum Pidana Dan Perkembangan Teknologi. *Seikat: Jurnal Ilmu Sosial, Politik Dan Hukum*, *2*(3), 347-355.
Ramadhan, G. (2023). Perlidungan Hukum Bagi Korban Ransomware Wannacry. *Das Sollen: Jurnal Kajian Kontemporer Hukum Dan Masyarakat*, *1*(02).
Rizal, M. S. (2019). Perbandingan Perlindungan Data Pribadi Indonesia dan Malaysia. *Jurnal Cakrawala Hukum*, *10*(2), 218-227.
Rosmayati, S. (2023). Tantangan Hukum Dan Peran Pemerintah Dalam Pembangunan E-Commerce. *Koaliansi: Cooperative Journal*, *3*(1), 9-24.
Situmeang, S. M. T. (2021). Penyalahgunaan data pribadi sebagai bentuk kejahatan sempurna dalam perspektif hukum siber. *Sasi*, *27*(1), 38-52.
Suwiknyo, F. B. (2021). Tindak Kejahatan Siber Di Sektor Jasa Keuangan Dan Perbankan. *Lex Privatum*, *9*(4).
Wahyudi, D. (2013). Perlindungan Hukum Terhadap Korban Kejahatan Cyber Crime

Di Indonesia. *Jurnal Ilmu Hukum Jambi*, *4*(1), 43295.
Yanova, M. H., Komarudin, P., & Hadi, H. (2023). Metode Penelitian Hukum: Analisis Problematika Hukum Dengan Metode Penelitian Normatif Dan Empiris. *Badamai Law Journal*, *8*(2), 394-408.
Yitawati, K., Purwati, Y., & Sukarjono, B. (2022). Implikasi dan Sosialisasi Undang-Undang Tentang Perlindungan Data Pribadi dalam Menjaga Kerahasiaan Data Pribadi Seseorang. *Jurnal Daya-Mas*, *7*(2), 90-95.

.