Available online at JDR Website: http://journal.unublitar.ac.id/jdr

Journal Of Development Research, 7 (1), May 2023, Pages 95-103

DOI: https://doi.org/10.28926/jdr.v7i1.278

Mechanism for Protecting Personal Data Against Crimes in Cyber-Space (Cyber Crime)

Siti Sumartiningsih[(1)], Susanto Santiago Pararuk[(2)], Ngestu Dwi Setyo Pambudi[(3)]

Universitas Airlangga, Indonesia

E-mail: : [(1)]siti.sumartiningsih-2022@fh.unair.ac.id, [(2)]susanto.santiago.pararuk-2022@fh.unair.ac.id, [(3)]ngestu.dwi.setyo-2022@fh.unair.ac.id

Received: 20 December 2022; Revised: 26 May 2023; Accepted: 28 May 2023

Abstract

Protection of personal data is one of the Human Rights (HAM) which is part of personal protection and all of its property needs to be given a legal basis to provide security for the personal data. Besides that, protection of personal data is needed to raise public awareness and guarantee recognition and respect for the importance of protecting personal data. Protection of personal data from hacking actions carried out by irresponsible people who can endanger themselves. By hacking personal data, hackers will be able to enter banking accounts, social media accounts, and others which can cause material losses to victims of hacking. There are so many negative impacts experienced by victims, that criminal law is needed in determining criminal responsibility for hackers because this is a serious crime that can be threatened with criminal sanctions. This type of legal research is a type of normative legal research. This study emphasizes that fundamental efforts are needed regarding literacy and education regarding the internet for the wider community, because the internet has become a vital necessity in this modern era. Even more It needs to be rearranged the harmonization of the imposition of criminal sanctions and the overall coordination of the Law Enforcement Apparatus (APH) against hacker who committed cybercrime as well as by theft of personal data.

Keywords: criminal liability, hacking, personal data protection

Introduction

Problems in the transportation sector are The rapid development of communication and information technology has created opportunities and challenges. Information technology allows humans to connect without knowing the boundaries of the country so that it is one of the driving factors of globalization. Various sectors of life have utilized information technology systems such as organizing electronic commerce (e-commerce) in the trade/business sector, electronic education (e-education) in the field of education, electronic health (e-health) in the health sector even up electronic government (e-government) in the field of government, as well as communication and information technology that is utilized in other fields. The use of such communication and information technology results in a person's personal data being very easy to collect and move from one party to another without the knowledge of the Personal Data Subject, thereby threatening the constitutional rights of the Personal Data Subject. So protection against it from crime and the threat of crime is absolutely necessary in this era of globalization.

Regulated in Article 28 G paragraph (1) Basic Law of the Republic of Indonesia of 1945 (UUDNRI 1945) which states that: "Everyone has the right to personal, family, honor, dignity protection, and property that is under his authority, and is entitled to a sense of security and protection from the threat of fear to do or not do something that is a human right ". Personal Data Protection Issues arise because of concerns about violations of personal data that can be experienced by people and / or legal entities. Such violations cause material losses and non material. The formulation of rules regarding the Protection of Personal Data can be understood because of the need to protect the rights of individuals in society in connection with the processing of personal data both carried out electronically and

non electronics uses data sports devices. Adequate protection of personal data will be able to give the public the trust to provide personal data for a greater range of community interests without being abused or violating his personal rights.

Personal data contains most of a person's circumstances. The state of a person who does not show a person to the public based on his own safety and comfort reasons. The concept of privacy was first sanctified by Samuel Warren and Brandheis in "The Right to Privacy" or the right not to be disturbed. There is development and technological progress, a public awareness arises that there is a awareness that there is a right of a person to enjoy life (Kusnadi & Wijaya, 2021:3). In line with this Article 1 number 22 jo Article 79 paragraph (1) Law Number 24 of 2013 Concerning Amendments to Law Number 23 of 2006 concerning Population Administration stipulates that personal data is certain individual data that is stored, maintained, and guarded the truth and protected by its collar by the state.

Furthermore Alan Westin (1967) defines the right to privacy as claims from individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others. The power of privacy coverage usually makes many arrangements regarding privacy in a country, both in type and level (Djafar, 2019).
This is similar to the concept offered by Arthur Miller (1971) which points to the concept of privacy on the ability of individuals to exercise control over the dissemination of information related to themselves. Another opinion from Julie Innes (1992) which defines privacy as a condition when someone has control over the realm of their private decisions, which include decisions on private access, private information and private action. While the private sector itself is explained as a product of love, joy and care for others (Djafar, 2019). In line with Solove's opinion (2008) which says that the private context includes: family, body, gender, home, and communication and personal information of a person.

The beginning of the actual computer was formed by a British mathematics Professor, Charles Babbage (1791-1871). In 1812, Babbage paid attention to the natural suitability between mechanical and mathematical machinery. Mechanical machines are very good at doing the same task of repeatedly without errors; whereas mathematics requires simple reps of a certain step. The problem then develops to place the mechanical machine as a tool to answer mechanical needs. The development of communication and information technology today causes in the course of life to be inseparable from an electronic device in the form of a computer, handheld telephone (the handphone), and so on. As the computer develops which was originally used as a counter tool (calculator), then the computer can be paired with a communication and information technology called the Internet to increasingly complement the function of the computer as a communication and information tool. The word Internet itself has 2 (two) meanings as follows (Sudirman & Wahono, 2023) :

1. Internet network (letter "i" small as initial letter) is a communication network in which connected computers can communicate even though hardware (hardware) and the software (software) different. This is referred to as an internet network (internet-working);
2. Internet networks (letters "I" large as initial letters) are networks of a network of millions of computers that can communicate with each other using a computer network communication rule (protocol) same one. The protocol used is Transmission Control Protocol / Internet Protocol (TCP/IP*)*.(Chandra, 1995).

Crime can also encroach through computer media and its networks (Internet), crime using the internet is known as "cybercrime". Edmon Makarim refers to encyclopedia of Knowledge define cybercrime as "is a term formula used to describe an interdisciplinary approach to the study of control and communication in animals, humans, machine and organization. The Word." (Makarim, 2003) *Crime* in this case it has the meaning of crime which is an anti-social act that causes harm, disobedience in social life, which causes anxiety and irregularities in society. Andi Hamzah further classifies computer crime based on tasks that are charged with fraud in the computer field viz (Hamzah, 1990: 23):

1. Crimes against computer systems, include :
   a) In input (*input*), with removal, addition of input materials;
   b) In data processing, with changes, destruction;
   c) On computer programs, by theft and sale, program destruction, insert fraudulent instructions; and
   d) At output (*output*) with forgery

2. Crimes against computer equipment; actions that can be included here such as fraud in the purchase of computer equipment (hardware) with the aim of destroying the achievements and reputation of the opposing party.

Andi Hamzah's opinion is as good as what is listed in The Encyclopedia of Crime and Justice: "it has two main categories. In the First, the computer is a tool of a crime, such as fraud, emblezzement, and theft of property; or is used to plan manage a crime. In a second, the computer is a object of a crime, such as sabotage, theft or alteration of storage data, or theft of it service ."(Dressler, 2011).

Regarding cybercrime in the International world itself is regulated in The Council of Europe Convention on Cybercrime signed in Budapest, Hungary on November 23, 2001. Cybercrime is an international crime that can harm losses to victims across countries. Edwin's opinion. H. Sutherland in his book is titled "*Principle of Criminology*" define international crime namely: "*an international crime is act that is defined as criminal under international law. In most instances, this will be done through international agreements, but customary international law also plays a role. Normally, an act will initially be defined as a crime by an international agreement and the, after the agreement has been ratified by a large number of states and generally accepted even by those states who do not becomes parties, the act may be regarded as a crime under customary international law. If an act is defined as an international crime under customary*".

The law of personal data protection develops as true as the development of technology itself, especially communication and information technology. As explained earlier, data protection regimes were born in Europe as a result of the absence of a clear definition of privacy and personal life, which is regulated under Article 8 of the European Convention. The right to data protection itself aims to protect individuals in the era of information society. The country that first passed the Data Protection Act was Germany (1970), which was then followed by Britain in the same year, and then a number of other European countries like Sweden, France, Switzerland and Austria follow. Initially these developments surfaced in the United States in the presence of a fair credit reporting law in 1970 which also contained elements of data protection.

There are several reasons regarding privacy rights that must be protected namely: First, in fostering relationships with others, one must cover part of his peer life so that he can maintain his position at a certain level. Second, someone in his life needs time to be alone so that privacy is needed by someone. Third, privacy is an independent right and does not depend on other rights but this right will be lost if the person publishes matters that are private to the public. Fourth, privacy also includes a person's right to have domestic relations including how someone fosters a marriage, fosters his family and others must not know the personal relationship. Fifth, other reasons why privacy deserves legal protection because the losses suffered are difficult to assess. The loss is felt far greater than the physical loss, because it has disrupted his personal life, so that if there is a loss suffered the victim is obliged to get compensation (Kusnadi & Wijaya, 2021: 4). At present the Protection of Personal Data in Indonesia is regulated in Law Number 27 of 2022 concerning the Protection of Personal Data. This is a state effort in protecting the personal data of its citizens in this modern era where privacy is a rare item in life.

It has been reported on the background of cybercrime in relation to Personal Data Protection (PDP) above, then in this legal study 2 (two) formulations of the issues to be discussed as follows: (1) How to link cybercrime in breaking down personal data that causes harm to the victim?; and (2) Is the form of legal protection in the context of Personal Data Protection carried out by the State?.

Materials and Method

This type of legal research is a type of normative legal research, which aims to review the provisions of positive law in this case criminal law as a source of law. Moris L Cohen expressed the opinion of Peter Mahmud Marzuki who stated "Legal Research is the process of wall the law that governs activities in human society" (Marzuki, 2017). Legal research on its nature starts with the desire for human fortitude expressed in the form of problems or questions, where every problem and legal question is needed answers and the deed gets new knowledge that is considered correct. In addition, this legal research is Doctrinal Research which provides or produces a systematic explanation of the norms or the legal tongues governing a particular category (Rijadi, 2017).

Results and Discussion

Linkage of Crime in cybercrime with Personal Data Protection (PDP).

Necessity today, almost in every activity in this modern era using the internet. It is worth knowing the language when we use the internet, so all the activities we do have been recorded in the deep form of digital data. Therefore, protection of the security of personal data must be regulated in such a way by the State in the context of securing the activities of citizens who can endanger the citizens themselves unnoticed. Cybercrime problem this is included in the group extra ordinary crime (extraordinary crime) is even felt as serious crime (serious crime) and transnational crime (trans-state crime) which always threatens the lives of citizens, nations and sovereign states. This crime or crime is the worst side of modern life from the information society due to the rapid advancement of technology with the increasing events of computer crime, pornography, digital terrorism, rubbish information war, information bias, hacker, cracker etc (Hartono, 2014). One of the cybercrime according to Convention on Cybercrime is Illegal Access; encompass the basic violation of the dangerous threat – threat from attacks on data security and computer systems. Protection against violations illegal access this is a picture of the interests of organizations and groups and people who want to regulate, run and control their systems without interference and obstacles; as an example of this crime is: hacking, cracking, and computer trespassing. This type of crime gives the offender access to important data (including password or system information) and secrets that might be used to buy goods using someone else's credit card information or encourage the offender to commit a form of violation regarding a more dangerous computer such as counterfeiting or fraud with a computer. Personal data assistance is regulated under Article 4 paragraph (1) Law Number 27 of 2022 concerning Protection of Personal Data to 2 (two) form is: Specific Personal Data; and general personal data which includes based on Table 1.

Table 1. Personal data assistance

Specific Personal Data	General Personal Data
a) Health data and information; b) Biometric data; c) Genetic data; d) Crime record; e) Child data; f) Personal financial data; and/or g) Other data in accordance with statutory provisions.	a) Full name; b) Gender; c) Nationality; d) Religion; e) Marital status; and/ or f) Personal data combined to identify someone

It has been explained before about illegal access as stated that hacker enter part or all of the victim's computer system by attacking the data stored on the installed system, the data traffic regarding the contents. Deep illegal access the offender commits an offense committed by entering into another person's computer system without the permission of the owner of the computer system. This crime is directed against someone's information which is a very personal and confidential matter. This crime is usually directed against the personal information of someone stored on a personal data form that is stored in a stored manner computerized, if someone else knows, it can harm the victim both materially and immaterilally (Hartono, 2014).

Cybercrime has developed so that understanding of new terms for the perpetrators. Those who like “play” internet, browsing other people's websites called “Hacker” and the act is called “Hacking”. If is Hecker the intruder and smuggler to the other person's site and the destructive is referred to as “cracker”. Hacker which explores various sites and peers data, but does not damage the computer system, the sites of other people or institutions are called “Hektivism”. Lately it can be said that money motivation is the most prominent, namely by using other people's credit card data to shop through the internet. The way they are referred to as “carder” obtaining credit card data is to cate data from conventional transactions, for example payments at hotels, tour bureaus, restaurants, shops and others (Hartono, 2014). There are 4 (four) type cybercrime carding as follows:

1. Misuse of card data; in the form of credit card abuse that is not presented, is an event where the credit card user is not aware of the card being used by another party until he receives the bill;
2. Wiretapping; done by tapping credit card transactions through a communication network. This crime can cause great harm to the victim;
3. Counterfeiting; type of crime with a credit card forgery mode. Usually they use fake cards that are made so similar to real cards. Carding this type is usually carried out by personal to credit card counterfeit syndicates that have certain expertise;

4. Phissing; done through messages email fraud from a legitimate company. For example: universities, internet service providers, banks, etc. Order in email this usually directs someone to the site website fake or make someone leak personal information. Hacker use personal information to commit identity theft. The identity will be used for crimes that harm the owner (Widayanti, n.d.).

The modus operandi that is commonly used hacker in attacking the victim's personal data is Social Engineering. The matter is in the form of psychological manipulation of someone in determining action or taking up a confidential information. Social Engineering generally done by telephone or internet. Social Engineering is one of the methods used by hacker to obtain information about the target, by requesting that information directly to the victim or other party who has the information. This mode is the most frequent way for fraudsters to trick their victims. The perpetrators will confess Customer Service or Support Staff from banks, credit cards, insurance and other financial institutions. The mode starts from a telephone received by a potential victim who is not aware that the fraud is trying to extract his personal data.

The first method is the most basic method in Social Engineering, can complete the task hacker quickly. Hacker just asking for what he wants like: password, access to networks, network maps, system configurations, or room keys. The second way is to create a false situation where a person is part of the situation. The attacker can make reasons that concern the interests of other parties or other parts of a company, this requires effort hacker in seeking more information and usually also having to gather additional information about the target. Next way hacker the most popular now is through email, by sending email who asks for a target to open attachment which is certainly inserted worm or Trojan Horse to make backdoor in the system.

Nowadays a lot platform be it within the scope of business, banking, education, government, communication, etc. which requires the provision of personal data to be given digitally by side does make all of its activities more effective and efficient. Imagine that now someone can create an account at a bank without having to go directly to the bank, all directed through digitization. Even to communicate at this time when activating the phone card (SIM CARD) must attach a Resident Identity Card (KTP) and/ or the Family Card (KK) which ironically again requirements like this are ordered by the State through a policy.Thus the State must also be responsible for the personal data of the requested citizens.

In terms of the concept of personal autonomy and the rationale regarding the concept of individualism, that each individual has a uniqueness, basic rebates, and values as a human being. To protect personal autonomy and individuality, one must be given a personal space that is free from outside influences. Privacy policy is to protect border lines that protect individuals from the curious views of third parties. An important aspect of human dignity is the right to individual freedom (Ananthia Ayu D, Dkk, Perlindungan Hak Privasi Atas Diri Di Era Ekonomi Digital, Penelitian Kepaniteraan Dan Sekretariat Jenderal Mahkamah Konstitusi, Pusat Penelitian Dan Pengkajian Perkara Dan Pengelolaan Perpustakaan Mahkamah Konstitusi, 2019). This is what should be prioritized by the State in the context of protecting its people.

Through Law Number 27 of 2022 concerning the Protection of Personal Data, the state provides protection by regulating the criminal sanctions in its depth as follows:

Article 67 paragraph (1);

"Any person who intentionally and unlawfully obtains or collects personal data that does not belong to him with a view to benefiting himself or others that could result in loss of the Personal Data Subject as referred to in Article 65 paragraph (1) convicted with a prison criminal of at most 5 (lima) year and / or a fine of at most Rp. 5,000,000,000,- (five billion rupiah)."

Article 67 paragraph (2):

"Any person who intentionally and unlawfully discloses Personal Data that does not belong to him as referred to in Article 65 paragraph (2) is sentenced to a prison crime of at most 4 (four) year and/or criminal fines at most Rp. 4,000,000,000,- (four billion rupiah)".

Article 67 paragraph (3):

"Any person who intentionally and unlawfully uses Personal Data that does not belong to him as referred to in Article 65 paragraph (3) is sentenced to a prison criminal of at most 5 (lima) year and/or criminal fines at most Rp. 5,000,000,000,- (five billion rupiah)."

B. Criminal Sanctions for Hacking Actors (Hacking) in an account belonging to another person in the perspective of Personal Data Protection (PDP).

Criminal is a translation of the word "straf" in Dutch. In everyday life, people also use the term "punishment" as a translation of words straf. According to Sudarto there is a difference between the terms punishment and criminal. The term punishment contains a general understanding as a sanction that is deliberately imposed on someone who has violated the law, both criminal law and civil law, whereas the term criminal is a special understanding relating to criminal law. That is, in the event of a violation of the provisions of criminal law. Then the offender can be subject to criminal sanctions (Muladi & Arief, 2010). According to Barda Nawawi Arief, if the notion of funding is broadly interpreted as a process of giving or dropping a criminal by a judge, then it can be said that the funding system includes the entire statutory provisions governing how the criminal law is enforced or operationalized concretely so that someone is sanctioned.

After understanding the criminal understanding, then what is meant by (funding veroordering). Sudarto's opinion about idling is a synonym of the term punishment. The sentence comes from the basic word of law, so that it can be interpreted as "setting a sentence" or "deciding about the sentence ".Thus the convict can be interpreted as a criminal offense in law (Muladi & Arief, 2010),. Mid-funding is also interpreted as a result or consequence of an act of violating criminal provisions that have been carried out.

At present a new legal regime is born known as cyber law (cyberlaw) or telematics law. Cyber law or cyber law, internationally used for legal terms related to the use of information and communication technology. Likewise, telematics law is an embodiment of the convergence of telecommunications law, media law, and informatics law. Another term also used is information technology law (law of information technology) cyberspace law (virtual world law) and Cyber law. In this connection, the legal world has long expanded its interpretation of principles and norms when dealing with the issue of intangible lacy, for example in the case of electricity theft as a criminal offense. In reality cyber activities are no longer simple because their activities are no longer limited by the territory of a country, which is easily accessible whenever and wherever.

Here are some examples of crime cases in cyberspace (cybercrime) done by a person hacker in Indonesia (NAGAJOSTER.COM, 2022):

1. Info " strange " on the KPU site (2004); 2004 was the first moment Indonesia held direct elections. The IT Team of the Election Commission also launched the KPU site which is worth Rp. 152,000,000,000,- (one hundred fifty -two billion) and inflamed impossible to be hack, the statement unexpectedly challenged hacker named Xnuxer (Dani Firmansyah) to break into the site. Initially Xnuxer tried to hack by doing XSS (Cross Site Scripting), i.e. inject dangerous code into website KPU. Because it failed, Xnuxer tried spoofing , i.e. divert IP website so he can take control of the site. The Xnuxer attack was successful and allowed it to do SQL Injection (SQL query manipulation). As a result, hacker the origin of Yogyakarta can modify web pages and change information on the KPU site;
2. War hacker Indonesia vs Australia (2013); this case began when Edward Snowden, a former US intelligence, declared Australia tapping President Susilo Bambang Yudhoyono (SBY). It ignites anger hacker Indonesia so Anonymous was born Indonesia. This community also made a movement "Stop Saying Indonesia" by pounding website Australia has passed various ways. Ddos attacks, for example the Army Cyber Indonesia floods Australian sites with request fake until overload and website failed access. One of the victims is the Australian federal police site. Anonymous Indonesia also does deface against hundreds website random civilian property. This attack made lower-class business sites in Australia display warning words from Indonesia. Australia did not remain silent. They counterattack by making down various website important Indonesia like KPK, PLN, Garuda Indonesia, Indonesia Republican Police, Tempo and others.
3. PT. Global Network (Tiket.com) and Citilink were once dizzy by a tantrum hacker Indonesia led by adolescents 19 (nineteen) years from Tangerang. They do Illegal Access on the ticket application system that is connected to the citilink ticket sales system. They look for code booking flight ticket, then sell it through Facebook with a discount of 30%-40% so many people buy it. Ironically it takes 1 (one) more months for Ticket.com to realize there are intruders in the system. As a result, Ticket.com loses around Rp. 4 Billion, while Citilink loses Rp. 2 Billion rupiah.

4. The Telkomsel website displays harsh words (2017); Indonesian public accessing website Telkomsel was once a stir because it encountered harsh words on the site page provider the name. It turns out there is a person protesting the high rate of Telkomsel by mehack. Hackers successfully do deface by changing the display website Telkomsel. Website is paralyzed so visitors cannot access information as usual. Fortunately Telkomsel customer data is separate from website server, so it's still safe. Telkomsel also managed to restore website - within 12 (twelve) hours after at hack;
5. Tokopedia sea turtle data leaked to Dark Web (2020); there are 91 (ninety one) million user data and more than 7 (seven) data merchant e-commerce this was leaked by hacker named ShinyHunters. Tokopedia user personal data (***email, name , address, date of birth, gender of telephone number***, and password encrypted) leaked to the public. Even this information is sold to cyberspace at a price of around Rp. 70 million. Surely this incident has the potential to bring harm to Tokopedia users. Because, hacker usually utilize for user profiles scam (fraud online) and phishing (take over the account or system). Send email fraud for example.

Activities through electronic system media are also called cyber space (cyber space), although virtual in nature can be categorized as real legal actions or deeds. Juridically the activities in the cyber space cannot be approached by the size and qualifications of conventional law alone because if this method is taken there will be too many difficulties and things that escape the enactment of the law. Activities in cyber space are virtual activities that have a very real impact even though the evidence is electronic. Criminal provisions that can be used in granting criminal sanctions for hacker can be seen in Article 30 paragraph (1), paragraph (2), and paragraph (3) jo Article 46 of Law Number 19 of 2016 Concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE Law) as follows:

Article 30 paragraph (1) ITE Law: "Everyone intentionally and without rights or against the law accesses someone else's computer and / or electronic system in any way";

Article 30 paragraph (2) ITE Law: "Everyone intentionally and without rights or against the law accesses computers and / or electronic systems in any way with the aim of obtaining electronic information and / or electronic documents";

Article 30 paragraph (3) ITE Law: "Everyone intentionally and without rights or against the law accesses computers and / or electronic systems in any way by violating, breaking through, going beyond or breaking into security systems".

For the form of sanctions that can be imposed seen according to Article 46 paragraph (1), paragraph (2), and paragraph (3) ITE Law as follows:

Article 46 paragraph (1) ITE Law: "Everyone who fulfills the elements referred to in Article 30 paragraph (1) is sentenced to a prison criminal of at most 6 (six) year and / or a fine of at most Rp. 600,000,000,- (six hundred million rupiah)";

Article 46 paragraph (2) ITE Law: "Everyone who fulfills the elements referred to in Article 30 paragraph (2) is sentenced to a prison crime of at most 7 (seven) year and / or a fine of at most Rp. 700,000,000,- (seven hundred million rupiah)";

Article 46 paragraph (3) ITE Law: "Everyone who fulfills the elements referred to in Article 30 paragraph (3) is sentenced to a prison criminal of at most 8 (eight) year and / or a fine of at most Rp. 800,000,000,- (eight hundred million rupiah)".

Cyber law as regulated in Article 2 of the ITE Law is universally included. ITE Law has a range of jurisdictions not solely for legal actions in force in Indonesia and / or carried out by Indonesian Citizens (WNI), but also applies to legal actions carried out outside the jurisdiction of Indonesia, both by WNI and foreign legal entities that have legal consequences in Indonesia, bearing in mind the use of electronic communication and information technology and electronic transactions can be cross-territorial or universal. Imposition of criminal sanctions to a person hacker need to be considered regarding the evidence. Considering that electronic information is not only not yet accommodated in the legal system of criminal events in Indonesia comprehensively, but also turns out to be very vulnerable to being changed, tapped, falsified, and sent to various corners of the world in seconds. Thus the impact it causes can be complex and complicated.

Although it is known that perpetrators of hacking through the internet can be subject to criminal sanctions, however has not really been said to be effective in handling cases that arise later on, the development of cybercrime (cybercrime) is getting more powerful. The perpetrators continue to try to renew the Piranti tool with a more sophisticated one so that it cannot be detected as much as possible. Also in his work hacker commit the crime neatly and silent. So great is cybercrime until it is regulated in international conventions, this crime can penetrate space and time and its victims can be from various circles around the world.

Conclusion

1. Protection of Personal Data by the state is absolutely necessary, because it is a privacy right that has to do with Human Rights (HAM). Protection of Personal Data is currently regulated in Law Number 27 of 2022 concerning Protection of Personal Data. The state in this case has an obligation to protect the personal data of its citizens by including criminal sanctions for the perpetrators of the leakage of personal data. Other dispensed acquisition of personal data carried out unlawfully (crime) in using the internet is also classified as cybercrime. Personal data is something that is very vulnerable to being hacked by hacker and used for the benefit hacker itself, the most of this concerns economic factors by accessing the victim's banking account;
2. Theft of personal data and fraud committed to obtain personal data or access to other people's property online clearly prohibited. Through Law Number 19 of 2016 Concerning Amendments to Law Number 11 of 2008 Regarding Information and Electronic Transactions (ITE Law), the state can also impose criminal sanctions against hacker who try to attack other people's vital accounts unlawfully. Companion is hacking behavior carried out by a person hacker who get deep access website belonging to a person or Government is done by not stealing personal data is also prohibited because it can disturb stability and cause unrest in society

Suggestion

1. Fundamental efforts are needed regarding literacy and education regarding the internet for the wider community, because the internet has become a vital necessity in this modern era. The community needs to be made aware of the language, not all aspects of life must be shared (share) via the internet for others to know. Furthermore, what needs to be corrected is the imposition of criminal sanctions in the PDP Law must be regulated even harder considering the maximum prison criminal threat is only 5 (five) years and is not regulated regarding the minimum limit for violators. This causes injustice for victims of theft and burglary of personal data, because crime practices such as this cause unrest or not a small amount of loss. Countries also need to have one data savings (one big data) which is really protected and can be used in all government access. So that the community in his life does not have to always include his personal data to third parties.
2. It needs to be rearranged the harmonization of the imposition of criminal sanctions and the overall coordination of the Law Enforcement Apparatus (APH) against hacker who committed cybercrime as well as by theft of personal data. Do not let action hacker it instead takes refuge in the PDP Law which establishes criminal sanctions that are smaller than the ITE Law. Then it needs to be strengthened again the role of state intelligence agencies and authorities in the regulation of communication and information technology considering that all this time these agencies only function as intermediaries public relation countries to citizens.

References

Ananthia Ayu D, dkk. (2019). Perlindungan Hak Privasi atas Diri di Era Ekonomi Digital, Penelitian Kepaniteraan dan Sekretariat Jenderal Mahkamah Konstitusi, Pusat Penelitian dan Pengkajian Perkara dan Pengelolaan Perpustakaan Mahkamah Konstitusi.

Chandra, F. H. (1995). Internet: Information Superhighway, Makalah Penataran Kualitas Dosen di Bidang Pengolahan Data dan Penyusunan Presentasi Melalui Media Komputer Bagi Dosen PTS, Kopertis Wilayah VI, Semarang, 1995, h.2.

Djafar, W. (2019). Hukum Perlindungan Data Pribadi di Indonesia: Lanskap, Urgensi dan Kebutuhan Pembaruan. Makalah Kuliah Umum “Tantangan Hukum Dalam Era Analisis Big Data, Pasca Sarjana Universitas Gajah Mada, Yogyakarta.

Dressler, J. (2011). The Encylopedia of Crime and Justice. Macmillian References.

Hamzah, A. (1990). Andi Hamzah, Aspek-Aspek Pidana di Bidang Komputer. Sinar Grafika.

Hartono, B. (2014). Hacker Dalam Perspektif Hukum Indonesia. Jurnal MMH, 43(1).

Kusnadi, S. A., & Wijaya, A. U. (2021). Perlindungan Hukum Data Pribadi Sebagai Hak Privasi. Jurnal Ilmu Hukum AL WA-SATH, 2(1).

Makarim, E. (2003). Kompilasi Hukum Telematika. Raja Grafindo.

Marzuki, P. M. (2017). Penelitian Hukum: Edisi Revisi. Prenada Media.

Muladi, & Arief, B. N. (2010). Teori-Teori dan Kebijakan Pidana. Alumni.

NAGAJOSTER.COM. (2022). 7+ Kasus Hacking yang Menggemparkan Indonesia dan Penyebabnya. https://www.niagahoster.co.id/blog/kasus-hacking-indonesia/

Rijadi, P. (2017). Memahami Metode Penelitian Hukum Dalam Konteks Penulisan Skripsi/ Tesis. AL Maktabah.

Sudirman, I., & Wahono, R. S. (2023). Sejarah Komputer, Kuliah Pengantar Ilmu Komputer. In Makalah.

Widayanti, P. W. (n.d.). Tindak Pidana Pencurian Data Nasabah Dalam Bidang Perbankan Sebagai Cyber Crime. Jurnal Legacy: Jurnal Hukum Dan Perundang-Undangan, 2(2) .

