Available online at https://journal.rescollacomm.com/index.php/ijbesd/index

International Journal of Business, Economics and Social Development

e-ISSN 2722-1156
p-ISSN 27722-1164

Vol. 2, No. 4, pp. 143-152, 2021

Strengthening Personal Data Protection, Cyber Security, and Improving Public Awareness in Indonesia: Progressive Legal Perspective

Abraham Ethan Martupa Sahat Marune*, Brandon Hartanto

Faculty of Law, Universitas Pelita Harapan, Tangerang, Indonesia

**Corresponding author email: index.abraham@gmail.com*

Abstract

The development of technology, communication, and the internet has positive and negative influences on all sectors of life in society. One of the negative impacts and problems is the alleged criminal act of buying and selling data and the absence of a special law (lex specialist) regarding the regulation of Indonesian personal data. The purpose of this research is to analyze in-depth the efforts to strengthen the protection of personal data, cyber security, and increase public awareness of the perspective of Progressive Law in Indonesia. This study uses a normative juridical method using secondary data, a statutory approach, a conceptual approach, and a case approach. This scientific paper concludes that the Synergy of Ministries and related institutions (Legislative, Executive, and Judiciary) is the key to protecting personal data and cyber resilience. Then, strengthening efforts should be made, namely immediately passing the Draft Law on Personal Data Protection (RUU PDP), forming an independent institution. However, if at this time a dispute occurs, it can be resolved by Article 30 of the ITE Law and the PMH Lawsuit (Tort), supported by a progressive legal approach and futuristic interpretation by the judge examining the quo case. The synergy of government agencies, the private sector, and other stakeholders is needed to increase public awareness by increasing education/dissemination of efforts to prevent misuse of personal data.

Keywords: Progressive Law, Personal Data, Cybersecurity.

1. Introduction

In today's era, the rapid development of Science and Technology coupled with the entry of Indonesia into the 4.0. Industrial Revolution Era and Cyberspace, also known as the internet world's rapid development, has made it part of the daily lives of so many Indonesians (Rasidin et al., 2020; Endarto et al., 2019; Hangabei et al., 2020). This has caused almost all human activities to interact online so that all mechanisms in all fields are switched through the online system. This of course has a positive impact where our access to doing things is easier and much faster, but in addition to the positive impact, of course, there is also a negative impact, namely the level of crime in cyberspace increases if there is no strong enough protection (Mohmmadi, 2021; Miró-Llinares and Moneva, 2019). The National Cyber Agency of Indonesia (BSSN) stated that there were around 888 million cyber-attacks in Indonesia recorded from January to August 2021 (BSSN, 2021).

This number will certainly continue to grow if not balanced with proper handling. One example of a sector that has a high risk of being attacked by cybercrimes is in the field of e-commerce (Apau et al., 2019; Choi et al., 2020). If we want to make transactions through e-commerce, then we must enter our data. To avoid misuse of our data by irresponsible parties, it is necessary to protect personal data. Based on research using Google Forms that were distributed to 226 respondents in terms of different ages, occupations, domiciles, latest education, 95% of respondents stated that personal data protection was very important, and 5% stated that personal data protection was important. In addition, the protection of personal data is also one of the determining factors for consumer online trust, which is an important thing in digital transactions. This is because if consumers do not feel safe, they will stop using e-commerce platforms due to privacy concerns.

Indonesia is one of the countries in Asia with an inadequate legal framework regarding the protection of personal data even though almost 74% of Indonesia's population are internet users. Indonesia's existing legal framework for personal data protection identifies challenges in providing a comprehensive legal framework and explores strategies for government, business, and civil society to comply with regulations (Inggarwati et al., 2020). In the development of

technology and information technology, personal information consisting of name, e-mail, and telephone number is very valuable data because it can gain economic value in the business world. This is what is called a digital file, which is a collection of personal data information that is owned by almost everyone by utilizing technology developed by private parties which seriously endangers the privacy of a person's data (Shivpuri, 2021).

The increasing need for information and communication technology causes various criminal acts to appear that can cause material and immaterial losses to a person. The increasing activity of the number of internet users makes the problem of protecting personal data a serious matter because its spread can be done easily and quickly through technology, which risks the leakage of someone's data (Widyaningrat and Dharmawan, 2014).

Protection of personal data is the mandate of Article 28 G of the 1945 Constitution of the Republic of Indonesia which regulates the right to protection of personal self, family, honor, dignity, and property under their control. The definition of personal data protection has not been explicitly regulated in the laws and regulations. However, several legal instruments regulate the protection of personal data, namely Law no. 11 of 2008 concerning Information and Electronic Transactions amended by Law no. 19 of 2016, Government Regulation of the Republic of Indonesia No. 71 of 2019 concerning the Implementation of Electronic Systems and Transactions (PP 71/2019), Indonesian Government Regulation No. 80 of 2019 concerning Trading Through Electronic Systems (PP 80/2019), and Minister of Communication and Information Technology Regulation No. 20 of 2016 concerning Protection of Personal Data in Electronic Systems.

Unfortunately, these regulations are still sectoral in nature and do not have specific legal instruments so that they are not sufficient to encourage the development of the digital economy in Indonesia. This benefits from the many people who experience telemarketing activities that fall into the direct marketing category, which directly offers products such as insurance and credit without collateral damage. Recently, the leakage of personal data and buying and selling of data has become more and more common. As an illustration of the increasingly widespread problems of personal data leakage and data buying and selling, there have been a number of cases that occurred in the last 1 year, including (a) May 2020, as many as 91 million user data and 7 million sellers at Tokopedia were suspected of being leaked; as many as 1.2 million Bhinneka.com user data allegedly leaked and traded on the dark web; as many as 2.3 million personal data of Indonesian citizens from the 2014 election lists were allegedly successfully harvested from the KPU website; (b) August 2020, data on about 890,000 customers of the financial technology company (fintech) Kreditplus was allegedly leaked and sold at the Raid Forum; (c) September 2020, the personal data of approximately 5.8 million users of the Red Door application in Indonesia was sold; (d) April 2021, the personal data of about 130,000 Facebook users in Indonesia was allegedly leaked and disseminated on an amateur hacker site; (e) May 2021, data on hundreds of millions of BPJS Kesehatan members were allegedly hacked and sold at the Raid Forum at a price of around IDR. 84 million.

With the rise of sales data such as the cases above, we will discuss "How to strengthen personal data protection, cyber security, and increase public awareness of the perspective of Progressive Law in Indonesia?" which aims to find ways to strengthen the protection of Personal Data, Cybersecurity, and increase public awareness of cyberspace from the Progressive Law perspective in Indonesia from the Progressive Law perspective to achieve maximum personal data protection in Indonesia.

2. Methodology

The research method used is the normative juridical method. Normative legal research, which is another name for doctrinal legal research, is also known as library research or document study because this research is carried out or aimed only at written regulations or other legal materials (Taekama, 2018). The author uses a statutory approach, a conceptual approach, and a case approach. A regulatory approach is an approach taken by examining all laws and regulations related to the legal issues being handled. An approach is an approach taken by examining cases related to issues faced in courts that have permanent legal force (Banakar and Travers, 2005).

3. Results

3.1 Optimizing Indonesia's Cyber Security and Resilience: Digitizing Indonesia and the Economy

Indonesia is currently the country with the fourth largest growth in internet users in the world. Research conducted by Deloitte shows that digital technology (Digital Economy) can increase Indonesia's annual economic growth by 2% because it supports the growth of Small and Medium Enterprises (SMEs) (Budiyanti et al., 2021). There were 202.6 million internet users in Indonesia in January 2021. The number of internet users in Indonesia increased by 27 million (+16%) between 2020 and 2021. Internet penetration in Indonesia stood at 73.7% in January 2021. McKinsey believes that by embracing and developing digital technology, Indonesia can increase the economy to US$150 billion growth, or equivalent to 10% of Gross Domestic Product (GDP), by 2025. This number is an increase of 13% compared to the previous year. this growth is the fourth largest growth in the world after India, China, and the United States (Saeed et al., 2017). Certainly, the growth of the digital economy in Indonesia will increasingly have a very large role in national economic growth in the future. The Covid-19 pandemic also has a big impact on why the digitalization of the

current economy continues to grow. Therefore, the importance of cyber security in Indonesia at this time must be increased because the stakeholders who depend on this security are predicted to be even greater.

3.2 Current Regulations on Cyber Security

However, due to the not yet optimal cybersecurity system in Indonesia, Indonesia often experiences cyber-attacks. The National Cyber Agency of Indonesia (BSSN) stated that there were around 888 million cyber-attacks in Indonesia recorded from January to August 2021 (BSSN, 2021). These cyber-attacks were mainly hacking cases targeting government and corporate websites. The hackers targeted several government agencies, including the General Election Commission (KPU) and the Ministry of Defense (Detiknews, 2013). Hackers also targeted corporations; the cellular telecommunications operator Telkomsel was hacked in 2017 (Kompas, 2017). The cyber-attacks above show that the cyber security systems in place in the government may be ineffective. The laws and regulations related to network security are currently only the Law on Information and Electronic Transactions (UU ITE) and the Government Regulation on the Implementation of Electronic Systems and Transactions (PP PSTE). However, these laws and regulations do not cover the handling of interception practices in cyberspace or e-commerce governance. These regulations also do not regulate the government's role in the cyber security system so that its use for cyber security is still limited. This condition can be interpreted as a legal vacuum in the protection of people's personal data. As a result of the legal vacuum, there can be legal uncertainty (rechtsonzekerheid), or furthermore it will result in legal chaos (rechtsverwarring). To fill this gap, the government needs to push for the ratification of a cybersecurity bill (RUU) in the House of Representatives (DPR). This bill is very important to help the government distinguish between cyber defense and cybercrime attacks. Attacks on cyber defenses are aimed at our national security. Most of these attackers were terrorists or enemy states. While cybercrime refers to any criminal offense in cyberspace. Currently, the government does not seem to distinguish between those two. We need to realize that adequate regulations regarding cyber security in Indonesia by enacting a law, will have a major impact on our economic growth and of course increase the resilience and security of the state in cyberspace.

3.3 Cybersecurity Institutions

The Ministry of Defense and the National Police are two of the two agencies that maintain the country's cybersecurity system. In 2017, the government established the National Cyber and Crypto Agency (BSSN) for coordination between various institutions in maintaining cyber security. The Ministry of Defense, which is responsible for handling cyber-defense attacks, has established a cyber-defense center to carry out cyber-defense governance. At the same time, the National Army under the Ministry of Defense has formed a cyber work unit (Satsiber) to carry out cyber defense activities and operations. At the same time, the National Police are dealing with cybercrimes by establishing the Cybercrime Directorate. In addition, the Ministry of Foreign Affairs of the Republic of Indonesia has begun to play a role with cyber diplomacy, namely using diplomacy methods to find solutions to cyberspace problems. For example, Indonesia has played an active role in discussing cyber regulation and crime issues at the United Nations Cybersecurity Groups of Governmental Experts (UN GGE) and the United Nations Office on Drugs and Crime (UNODC) (Lim, 2002). Finally, in response to cyber-attacks, the Ministry of Communication and Information has formed a team called ID-SIRTII / CC (Indonesia Security Incident Response Team on Internet Infrastructure/Coordination Center), to ensure cyber security in Indonesia. Because BSSN has only been established for two years, coordination between these agencies is still in the early stages. In addition, BSSN has not yet built a solid infrastructure and has not appointed a responsible agency in each department.

The PDP Supervisory Agency will actually be an institution that specifically oversees the protection of personal data in Indonesia, as other independent institutions have emerged in Indonesia due to the urgency for solving new problems. With this urgency, it is indeed necessary for an institution that does have a vision and mission to carry out this supervision because this supervision of personal data cannot be carried out partially or in the sense that it is not supervised specifically or focused. The implementation of its performance as a public service must also pay attention to and fulfill the AAUPB as regulated in Law 30/2014 concerning Government Administration so that in practice it can still realize an implementation of public services by upholding protection and legal certainty for the entire community.

Non-independent institutions under the Ministry of Communication and Informatics will not be able to realize citizen data sovereignty. Because, Kominfo is part of the government which is also the controller of citizens' personal data. Because if the data controller is also the supervisor or the judge, the potential conflict of interest is very large. Moreover, the data managed by the government is very large and much of it is sensitive data. While neutrality is very necessary for a supervisory agency. For example, if there is a leakage of personal data of citizens in one of the ministries which is suspected to be carried out by the minister, an institution under the Ministry of Communication and Informatics at the level of the Directorate General will be reluctant to examine higher-ranking state officials. So if

the PDP supervisory agency is independent and reports directly to the president, then the agency will be more flexible in carrying out its duties and all parties can be investigated by an independent institution if it is suspected that there is a leak of citizens' personal data.

The independent supervisory agency PDP in Indonesia should adopt the independent concept in the General Data Protection Regulation. In the GDPR, the PDP's independent supervisory bodies are called Independent Supervisory Authorities. Its definition in Art. 4 The GDPR is a public independent authority established by member states. The level of independence from Independent Supervisory Authorities is specifically regulated in article 52 of the GDPR which consists of 6 paragraphs. In the GDPR formulation, this institution has the task of supervising and has the authority to carry out investigations and corrections/remedies, and also has the task of providing input on data protection issues and is the party that handles reports related to violations of the GDPR.

The existence of an independent authority will ensure the protection of personal data of citizens abroad, because the principle of independence is an international standard. If there is a company in Indonesia that manages citizens' personal data, but the data is then leaked by a foreign company, from a European Union country for example, an independent PDP authority in Indonesia can cooperate with an independent authority in the European Union to investigate the foreign company. However, if the Indonesian data management supervisory agency is not independent, then the inter-state investigation cooperation is not possible. Because the European Union through the GDPR requires independent authorities as a condition to cooperate in investigations.

Therefore, the existence of an independent institution is an absolute requirement to adequately supervise the protection of the personal data of all citizens. Without independence, these institutions will not be able to realize the common goal of upholding the sovereignty of citizens' data both at the national and international levels.

3.4 Digital Infrastructure

To build a reliable security system, the government must ensure the security of its infrastructure. Indonesia is still in the early stages of developing secure digital infrastructure. A 2014 study found that less than 3% of government agencies are secure. At the same time, developments in machine-to-machine (M2M) technology, the Internet of Things (IoT), and cloud computing continue to make these institutions more vulnerable to various cyber-attacks (Trautman 2015; Kuncoro et al., 2020; Mobayen et al., 2019). The government should develop a local cybersecurity industry. Indonesia's cybersecurity industry is still growing. The market is dominated by foreign hardware and software products. Only Industry consults fast-growing local services, providing services such as forensics and digital security (Detiknews, 2015). The BSSN must coordinate with various agencies to draw up a roadmap for industrial development. This goal requires long-term research and planning and requires substantial funding.

3.5 Strengthening Personal Data Protection in Indonesia

Based on Article 1 paragraph 1 of the Bill on Protection of Personal Data, Personal Data is any data about a person either which and/or can be identified separately or in combination with other information either directly or indirectly through electronic and/or non-electronic systems. Based on Article 3 of the Personal Data Protection Bill, personal data consists of Personal Data of a general nature; and Personal Data of a specific nature. General Personal Data consists of the full name; gender; citizenship; religion; and/or Personal Data combined to identify a person. Meanwhile, specific Personal Data includes health data and information; biometric data; data; sexual orientation; political views; crime records; child data; personal financial data; and/or other data by the provisions of the legislation. Previously, some laws regulate the Protection of Personal Data as stated in the background of this paper, one example is Law 14/2008 on Public Information Disclosure. In the Act, it is stated in article 17 letter (h), that personal data includes the history and condition of family members; history, condition and treatment, treatment of a person's physical and psychological health; a person's financial condition, assets, income, and bank accounts; evaluation results concerning one's capabilities, intellect, and recommendation of abilities; and/or personal records relating to the activities of formal education units and non-formal education units. Recently, the leakage of personal data and buying and selling of data has become more and more common. As an illustration of the increasingly widespread problems of personal data leakage and data buying and selling, there have been a number of cases that occurred in the last 1 year, including (a) May 2020, as many as 91 million user data and 7 million sellers at Tokopedia were suspected of being leaked; as many as 1.2 million Bhinneka.com user data allegedly leaked and traded on the dark web; as many as 2.3 million personal data of Indonesian citizens from the 2014 election lists were allegedly successfully harvested from the KPU website; (b) August 2020, data on about 890,000 customers of the financial technology company (fintech) Kreditplus was allegedly leaked and sold at the Raid Forum; (c) September 2020, the personal data of approximately 5.8 million users of the Red Doorz application in Indonesia was sold; (d) April 2021, the personal data of about 130,000 Facebook users in Indonesia was allegedly leaked and disseminated on an amateur hacker site; (e) May 2021, data on hundreds of millions of BPJS Kesehatan members were allegedly hacked and sold

at the Raid Forum at a price of around IDR 84 million. Then, the case of Tokopedia shareholders and company structure documents in 2018 were leaked to the public by KrAsia, a media-based in China, and that KrAsia obtained the data from BKPM RI. Case of selling 91 million Tokopedia personal data for US$5,000 (IDR 74.3 million) on a dark web trading site. Several cases are in the process of reporting in the form of cases related to buying and selling data, illegal data access. There are also cases of opening personal data such as e-KTP numbers and KK numbers so that they can be accessed by the public. It was stated that the perpetrator of the case had been sentenced to 8 months in prison plus a fine. Some perpetrators are threatened with a maximum sentence of 9 years and/or a maximum fine of three billion rupiahs.

However, Indonesia's policies or regulations regarding the protection of personal data in special The regulations currently in force regarding this matter are separate and are scattered in several laws and only reflect aspects of personal data protection in general, Law Number 39 of 1999 on Human Rights, and Law Number 23 of 2006 concerning Population Administration as amended by Law Number 24 of 2013. Specifically related to telecommunications and media, there is already a Telecommunication Law, ITE Law, and Public Information Openness Law. But at least in ministerial level regulations, Kominfo has issued Regulation Number 20 of 2016 concerning the Protection of Personal Data in Electronic System Operator. Contains provisions regarding the rights of the owner of personal data, obligations of users of personal data, obligations of electronic system administrators, and dispute resolution. Kominfo Regulation Number 20 of 2016 establishes consent as the core of data privacy protection under Indonesian data privacy laws, and all laws can only be implemented after obtaining the consent of the personal data owner. Kominfo Regulation Number 20 of 2016 stipulates that the presentation, delivery, delivery, or opening of access to personal data in an electronic system can only be carried out based on the consent of the owner of the data, whose consent must be accurate and by the purpose. obtain and collect the data. The term 'consent' is defined in Kominfo Regulation Number 20 of 2016 which requires that it be given in writing, either manually or electronically.

In the process, the electronic system operator must first obtain the consent of the owner of the personal data after the electronic system operator has provided complete information or explanation regarding the implementation of the Process.

Furthermore, the electronic system operator will also have precautions in place to avoid personal data protection failures. Finally, the Government clarified the scope of personal data protection by issuing Government Regulation Number 40 of 2019 concerning the Implementation of Law Number 23 of 2006 as amended by Law Number 24 of 2013 concerning Population Administration. Meanwhile, the ITE Law does not contain special rules to protect personal data. However, in its provisions, there are Article 26 paragraph (1) and an explanation of Law 19/2016 which reads, "Unless specified by laws and regulations, the use of all information through electronic media regarding a person's data must be done with the consent of the person concerned." explained in Article 26 of the ITE Law, in the use of Information Technology, the protection of personal data is one part of personal rights. If someone's data is used without the person's permission, then the person whose rights have been violated can file a lawsuit for the loss caused. It should be noted that the personal data of these residents must be stored and protected by the state.

Furthermore, the practice of buying and selling personal data so far can be said to be included in Article 30 paragraph (3) of the ITE Law which reads, "Everyone intentionally and without rights or against the law accesses computers and/or electronics system in any way with interference, bypassing the system. "For his actions, people who violate can be sentenced to imprisonment of up to 8 years and/or a maximum fine of IDR 800 million. The procedure guidelines for the Electronic Information Law are contained in Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions, which previously governed Government Regulation Number 82 of 2012 concerning the Implementation of Electronic Systems and Transactions. The Electronic Information Act stipulates that, unless otherwise provided, the use of any information relating to a person's data through electronic media requires the consent of that person. The elucidation of the Electronic Information Law stipulates that the protection of personal data is part of the right to privacy and defines the right to privacy which includes the following, the right to enjoy a private life, to be free from any interference, the right to communicate with others without espionage, and the right to unify access information about a person's life and personal data. The reason for the issuance of Government Regulation no. 71 of 2019, which in addition to being following the existing concept of personal data protection summarized in the current Indonesian data protection regulations, contains several previously unrecognized additions to electronic system operators' obligations related to protection. personal data previously stipulated in PP 82/2012. First, PP 71/2019 explicitly recognizes and distinguishes 'personal data owner' and 'personal data controller', although it does not provide any definition of the terms. Second, PP 71/2019 recognizes the right to delete and the right to delete records. Third, PP 71/2019 includes several legal grounds for viewing personal data other than consent, namely, processing personal data to fulfill obligations or to fulfill requests from the owner of the data when making an agreement, fulfilling legal obligations to control personal data with applicable laws. , protect the interests of the owner of personal data, carry out the legal obligations of the personal data

controller, carry out the control of personal data in the service for personal interests, and take care of other valid interests of the personal data or personal data owner.

Unfortunately, many of these regulations have become ineffective, causing the regulation of personal data protection in Indonesia to be still partial, which has not been able to accommodate all losses incurred in the event of personal data. Therefore, a comprehensive legal umbrella is needed, namely the Personal Data Protection Bill which is being drafted by the DPR. The presence of the Personal Data Protection Bill is one concrete step towards strengthening the protection of personal data in Indonesia. With the completion of this PDP Bill, Indonesia will become the fifth country in ASEAN to enforce regulations on Personal Data Protection. For existing Personal Data Controllers, there will be a period of two years before the PDP Bill is fully effective and meets full compliance (Kumalaratri, 2021).

Steps to support Data Protection in Indonesia do not stop with the existence of a comprehensive Personal Data Protection Law. However, there is also a need for a supervisory agency that is expected to monitor the performance of personal data managers, including personal data controllers. In the Personal Protection Bill, Article 21 states that in conducting a Personal Data experiment, the Personal Data Controller is obliged to maintain the confidentiality of the Personal Data. However, more supervision is needed to monitor their performance. Although many institutions are mandated, such as in the Law on Public Information Openness, namely the Information Commission, this new supervisory agency has a different focus, task, function, and authority from the Information Commission. this independent supervisory agency to focus more on personal data protection. In addition, this formation is because this matter cannot be resolved by government institutions. After all, the duties and authorities are broad, namely, they must supervise the implementation of this law, resolve all problems in the event of a dispute, negotiate with other countries regarding data transfer, sanctions, conduct socialization to the public regarding the Protection of Personal Data. Then regarding the applied sanctions, in the Personal Data Protection Bill, there are already administrative and criminal sanctions arrangements. we compare with the provisions in the GDPR in force in the European Union, it is said that this regulation is subject to a penalty of 20 million Euros (approximately IDR. For lesser cases of data leakage, a fine of 10 million Euros or two percent of global company revenue will be imposed (Article 83 GDPR). The Director-General of Informatics Applications at the Ministry of Communication and Informatics, Samuel Abrijani Pangerapan at the Cyberfest 2019 event said that the application of sanctions in the PDP Law follows the General Data Protection Regulation (GDPR) applicable in the European Union. However, unlike the GDPR, which stipulates fines on a percentage basis, which is 4% of total global income, the PDP Law will set a minimum and maximum fine. He again explained that the policy did not want to bankrupt Indonesian companies so that the 4% GDPR rule was not followed.

Therefore, in the PDP Bill the sanctions applied in terms of personal data protection in Indonesia, especially in the case of buying and selling personal data, have been stated in article 64 paragraph (2) of the Personal Data Protection Bill, which reads “Everyone who intentionally sells or buys data Personal as referred to in Article 54 paragraph (2) shall be sentenced to a maximum imprisonment of 5 years or a maximum fine of IDR. 50,000,000,000.00 (fifty billion rupiah). Unfortunately, the need for comprehensive personal data protection rules has not been accompanied by growing public awareness in protecting personal data. To increase public awareness, it is necessary to socialize the wider community regarding the importance of protecting personal data currently. With this socialization, it is hoped that the public will increase awareness of the importance of protecting their data and can take preventive measures to avoid becoming victims of personal data breaches.

3.6. The Application of Progressive Law to Strengthen Personal Data Protection in Efforts to Enforce the Sale and Purchase of Personal Data in Indonesia.

According to Rahardjo (2009), progressive law enforcement is carrying out the law not just black-and-white words from regulations (according to the letter), but according to the spirit and deeper meaning (to very meaning) of the law. Law enforcement is carried out with determination, empathy, dedication, commitment to solving legal issues and accompanied by the courage to find other ways than what is usually done (Rahardjo, 2009). This means that Progressive Law is very concerned about truth, humanity, and justice because considering the purpose of the law is not only limited to achieving legal certainty but also about benefiting and achieving true justice for the welfare of the people.

We can see the application of progressive law in the sale and purchase of personal data in Indonesia in the case of Denny Siregar's data burglary by an outsourcing employee of Telkomsel in Surabaya with a revenge motive due to being bullied by a Denny Siregar supporting account. Because there have been reports from consumers/victims, the suspect is guilty and charged with Article 46 or 48 of Law number 11 of 2008 concerning ITE, or article 50 of Law number 36 of 1999 concerning telecommunications, and Article 362 of the Criminal Code or Article 95 of Law number 24 of 2013 concerning Population Administration a maximum of 10 years in prison or a fine of IDR. 10 billion. In addition to the guilty party (suspect), sanctions can also be applied due to company negligence resulting in

the leakage of Personal data. The application of progressive law in controlling the mode of buying and selling personal data can be applied in 3 law enforcement media, namely in Administrative Law, Civil Law, and Criminal Law. Law enforcement in the field of Administrative Law, as contained in article 31 letter h, which reads "Personal Data dispute resolution officials/agencies for failure the confidentiality of the protection of Personal Data who handles complaints can provide recommendations to the Minister for administrative decisions to Electronic System Operators even though complaints can or cannot be resolved by deliberation or other alternative settlements." states that administrative sanctions may be imposed on the Electronic System Operator even though it can or cannot be resolved by deliberation or other alternative settlements. Administrative sanctions in article 36 paragraph (1) Permenkominfo No. 20 of 2016, which can be done with a verbal warning, written warning, temporary suspension; and/or announcements on online websites. Administrative sanctions are given by the minister or the head of the relevant sector supervisory and regulatory agency. If the imposition of sanctions by the leadership of the supervisory and regulatory agencies of the relevant sector is carried out after coordinating with the Minister. Administrative sanctions are also regulated in Article 100 paragraph (2) of PP No. 71 of 2019, in the form of written warnings, administrative fines, temporary suspension, termination of access; and/or removal from the list. This form of sanctions does not eliminate criminal and civil liability. Specifically, the imposition of sanctions in the form of termination and termination of access is carried out in coordination with the leadership of the relevant Ministries or Institutions. In Article 23 of the Personal Data Protection Bill, it is stated that the Personal Data Controller is obliged to prevent the Personal Data from being accessed illegally, then in article 40 paragraphs (1) and (3) which reads, "In the event of a failure to protect the Personal Data, the Personal Data Controller must submit in writing within 3 x 24 hours to the Personal Data Owner; and the Minister." and In certain cases, the Personal Data Controller is obliged to the public regarding the failure to protect Personal Data. If there is a violation of this, an administrative sanction will be imposed by the minister based on article 50 paragraph (2) in the form of a written warning; temporary cessation of Personal Data activities; deletion or destruction of Personal Data; compensation; and/or administrative fines.

Law enforcement in the civil sector can be carried out by a lawsuit to the organizer of the electronic system by registering the lawsuit to the district court where the e-commerce company is located/in this case the operator of the electronic system is located (Thorleuchter and Van den Poel, 2012). The plaintiff/victim can demand compensation, either in the form of material that can be valued in money or immaterial, for example in the form of strengthening the security system, so that no personal data in the system is repeated. As in the case of the burglary of Denny Siregar's data, he demanded compensation of 1 trillion which is a claim for material losses based on psychological losses, and received prizes in the form of mental terror and Cash on Delivery (COD) delivery asking the house to pay since the damage occurred and the network for the attack.

In contrast to law enforcement in the criminal field, although no offense accommodates this act, it is appropriate to make the perpetrators of crimes, judges use progressive law with futuristic interpretations of Article 30 of the ITE Law and theft crime in Article 362 of Indonesian Criminal Code. So, the Principle of Legality vs. Progressive Law vs. the Principle of Benefit. However, if this PDP Bill has been ratified, then criminal sanctions will be accommodated which will deter the perpetrators, namely in the case of buying and selling personal data as regulated in article 64 paragraph (2), namely Anyone who intentionally sells or buys Personal Data as referred to in Article 64 paragraph (2). Article 54 paragraph (2) shall be sentenced to a maximum imprisonment of 5 years or a maximum fine of IDR. 50,000,000,000.00 (fifty billion rupiah). In addition, Article 65 states that the punishment as referred to in Article 61 to Article 64 can also be imposed with additional penalties in the form of confiscation of profits and/or assets obtained or proceeds from criminal acts and compensation for losses. If committed by the Corporation, the penalty can be applied to the management, control holder, order giver, beneficial owner, and/or the Corporation. The only punishment that can be applied to the Corporation is fine. The fine imposed on the Corporation is a maximum of 3 (three) times the maximum penalty imposed. In addition to being sentenced to criminal penalties, the Corporation may be subject to additional penalties in the form of confiscation of profits and/or assets obtained or proceeds from criminal acts; freezing or a large part of the Corporation's business; prohibition to perform certain actions; closing or most of the places of business and/or activities of the Corporation; carry out obligations that have been neglected; and compensation. Based on the explanation above, strengthening in terms of buying personal data will be more effective and profitable if it is implemented based on progressive law with a futuristic interpretation of Article 30 of the ITE Law while waiting for the ratification of the Personal Data Protection Bill and followed by the creation of an independent supervisory agency and outreach to the public.

3.7. Increasing Public Awareness of Cyberspace

The results of the We Are Social study stated that in 2021 there were 202.6 million internet users in Indonesia, meaning that two-thirds of Indonesia's population is connected to the internet. However, based on not directly proportional to the occurrence of crime in Indonesia, based on data from the State of the Internet report, Indonesia is second in terms of criminal cases in the world, with a figure of 36.6 million attacks. According to data from the Child

Protection Commission (KPAI), pornography and cybercrime during 2011-2019 became the 3rd rank child complaint report which shows that cybercrime for children has become a serious enough threat for every Indonesian child who has been able to access the internet.

Police data on cybercrimes also shows that in 2018 there was an increase of up to 46.88 percent to reach 423 cases. These data indicate that preventing the threat of cybercrime and increasing awareness of cyberspace is very necessary, especially for children who are potential victims of cybercrime because children have become internet users with social developments that still need supervision. The importance of public awareness of cyberspace is because cyberspace has become the second world of humans to carry out activities of daily life so that various transactions, services, and permits are carried out using information and communication technology. The virtual world has given birth to various things that are all electronic, such as e-commerce, e-procurement, e-business, e-trade, e-service, e-life style, and others. Today, there are a lot of various electronic-based applications in various business communities, banking, government, ministries, campuses, and others. This shows that cyberspace has implications for the social participation of residents in providing active participation to be involved in activities in the community, and in making decisions. Referring to the explanation, the author sees the need for efforts to increase public awareness through socialization about cybercrime which is a criminal crime that has become a national and international issue, and most of them start from simple social problems in society and then shift to the virtual realm. The development of an increasingly advanced cyber world needs to be balanced with the dissemination of various understandings, especially aimed at the younger generation because the younger generation represents a group of internet users who are vulnerable to cybercrime where this group of users tends to spend a lot of time on internet usage. One of the institutions that need to broaden its focus in the public sphere is the EduCSIRT Pusdatin Kemendikbud. This institution plays an important role in providing services that include incident response in the form of incident triage; incident coordination; and incident resolution. The importance of socializing vital elements like this to realize cybercrime prevention and increase public awareness of cyberspace in Indonesia.

Socialization is broadly defined as a process in which an individual acquires attitudes, behaviors, and knowledge to participate in a society that involves various rules, roles, standards, and values covering personal, cognitive, and social aspects. Socialization takes place throughout the life course and can be achieved by socialization agents including parents, teachers, peers, and siblings, as well as by schools/daycares, the media, schools, the Internet, and other institutions.

3.7.1. Formal socialization

including socialization formed by the government and the community through institutions that have a special task in disseminating values, norms, and roles that must be learned by the community. In seeking public awareness of cyberspace, the authors suggest the application of an additional curriculum in basic education to increase awareness of cyberspace from an early age. By raising the awareness of today's children, we will move towards creating a culture of information safe in the future. Referring to the urgency, socialization needs to be done to prevent cybercrime, especially for elementary school-age children, because children's awareness today will create a culture of information without borders that are not safe. Therefore, education needs to be used as an educational medium for children to understand the dangers and threats of cybercrime. In addition, there is also a need for socialization through digital literacy with the use of languages that are different from people's conditions such as location and age level. In the government's role, it is necessary to appeal to application providers or creators to conduct socialization through public service advertisements that can increase public awareness of cyberspace. For example, an interactive Electronic Buying and Selling Application to prevent advertising errors from irresponsible sellers.

3.7.2. Informal socialization

including socialization contained in everyday relationships that are familial. Socialization to increase awareness of cyberspace and prevention of cybercrime in the community, especially children, should be carried out periodically and continuously considering the types of cybercrimes that continue to grow. In addition, the authors also suggest that the target of cyberspace socialization should be expanded not only to children but also to parents, teachers, and the wider community. Parents are the closest parties who first introduced their children to the internet. Therefore, parents must direct and direct their children to make the best use of the internet. Likewise, teachers and the community as parties can take part in providing understanding and supervision of children's behavior at school and in the community. Without the roles of these various parties, public awareness of cyberspace will be difficult to materialize, and cybercrime will be difficult to stop.

4. Conclusion

With an increasingly digitized economy, it is time for Indonesia to develop its capabilities in the cyber world. Because currently, cyber threats to Indonesia are very real. Not only a danger to 14 national securities, but also to the nation's economy which is supported by the internet. Adequate regulation-making as well as following and meeting existing needs has been made in detail and maturely by the House of Representatives and the Government. Good and efficient coordination between institutions by the main tasks and functions in maintaining and developing Indonesia's potential in a free virtual world is needed. All these things are of course important so that Indonesia can continue to grow and compete in an increasingly digitalized world. The strengthening of personal data protection can be done by passing the Personal Data Protection Bill which is expected to become a comprehensive law that can accommodate all forms of regulations regarding personal data protection to create law for the entire community. In addition, there is also a need for an independent supervisory agency that has the task of overseeing the control of personal data so that it can work effectively to realize personal data protection in Indonesia. While waiting for the ratification of the Personal Data Protection Bill, it will be effective and profitable if we apply a progressive law with a futuristic interpretation of Article 30 of the ITE Law to achieve public interest and justice. Synergy in increasing public awareness of cyberspace is a necessity and a necessity for Indonesia. All elements must play a role in their efforts. The government, parents, teachers, and the community must be able to become agents in providing understanding and supervision to form a cyber defense community that can ward off, detect, fend off, and prevent various potential cybercrimes.

For the Government and the House of Representatives to draft and pass the Cyber Security and Resilience Bill (RUU KKS), as well as the Personal Data Protection Bill (RUU PDP) to strengthen personal data protection early next year. Coordination between state institutions that are running well so that protection for the country from the threat of cyber-attacks is optimal, as well as the development of digital infrastructure in Indonesia so that it can continue to follow the needs of the community.

For judges, it is hoped that they will not reject cases or decide lightly on cases related to data security and privacy, also while waiting for the ratification of the Personal Data Protection Bill, judges can apply progressive law with futuristic interpretations of the current regulations so that the public interest and justice are achieved.

For the Central and Regional Governments, it is hoped that they will be able to take advantage of cyberspace to optimize public participation in accommodating aspirations, inputs, and increase awareness of cyberspace through this space.

References

Apau, R., Koranteng, F. N., & Adu, S. (2019). Cyber-crime and its effects on E-commerce technologies. *Journal of Information*, *5*(1), 39-59.

Banakar, R., & Travers, M. (Eds.). (2005). *Theory and method in socio-legal research*. London: Bloomsbury Publishing.

BSSN RI. (2021). "Perkuat Ketahanan Siber, BSSN dan Pemprov Banten Luncurkan Tim Tanggap Insiden Siber BantenProv-CSIRT". https://bssn.go.id/perkuat-ketahanan-siber-bssn-dan-pemprov-banten-luncurkan-tim-tanggap-insiden-siber-bantenprov-csirt/

Budiyanti, E., Permana, S. H., & Rivani, E. (2021, January). Important Points for Developing SMEs E-Commerce Towards Indonesia 4.0. In *4th International Conference on Sustainable Innovation 2020-Accounting and Management (ICoSIAMS 2020)* (pp. 388-392). Atlantis Press.

Choi, K. S., Lee, C. S., & Louderback, E. R. (2020). Historical Evolutions of Cybercrime: From Computer Crime to Cybercrime. *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, 27-43.

Detiknews. (2013). "Situs Dirjen Kementerian Pertahanan RI di-hack". https://news.detik.com/berita/d-2243078/situs-dirjen-kementerian-pertahanan-ri-di-hack

Detiknews. (2015). "BSSN dan Peta Keamanan Siber Indonesia". https://inet.detik.com/cyberlife/d-3899799/bssn-dan-peta-keamanan-siber-indonesia

Endarto, B., Alam, A. S., & Abadi, S. (2019, July). Curriculum Development in the Field of Law: Facing the New Era of Industrial Revolution 4.0. In *Journal of Physics: Conference Series* (Vol. 1179, No. 1, p. 012079). IOP Publishing.

Hangabei, S. M., Dimyati, K., & Surbakti, N. (2020). Oversee Investment and Indonesia Economic Regulatory Reform in the Era of Globalization and Industrial Revolution 4.0. *International Journal of Advanced Science and Technology*, *29*(4), 5123-

5138.

Inggarwati, M. P., Celia, O., & Arthanti, B. D. (2020). Online Single Submission For Cyber Defense and Security in Indonesia. *Lex Scientia Law Review*, *4*(1), 83-95.

Kompas. (2017). "Situs Telkomsel diretas, berisi keluhan internet mahal". https://tekno.kompas.com/read/2017/04/28/08042477/situs.telkomsel.diretas.berisi.keluhan.internet.mahal

Kumalaratri, G. (2021). Urgency Of The Personal Data Protection Bill On Privacy Rights In Indonesia. *Jurnal Hukum*, *37*(1), 1-13.

Kuncoro, A. H., Mellyanawaty, M., Sambas, A., Maulana, D. S., & Mamat, M. (2020). Air Quality Monitoring System in the City of Tasikmalaya based on the Internet of Things (IoT). *Jour of Adv Research in Dynamical & Control Systems*, *12*(2), 2473-2479.

Lim, M. (2002). Cyber-civic space in Indonesia: From panopticon to pandemonium?. *International development planning review*, *24*(4), 383.

Miró-Llinares, F., & Moneva, A. (2019). What about cyberspace (and cybercrime alongside it)? A reply to Farrell and Birks "Did cybercrime cause the crime drop?". *Crime Science*, *8*(1), 1-5.

Mobayen, S., Vaidyanathan, S., Sambas, A., Kacar, S., & Çavuşoğlu, Ü. (2019). A novel chaotic system with boomerang-shaped equilibrium, its circuit implementation and application to sound encryption. *Iranian Journal of Science and Technology, Transactions of Electrical Engineering*, *43*(1), 1-12.

Mohmmadi, J. (2021). Barriers and Law Enforcement Measures to Prevent Pornographic Crimes in Cyberspace. *Journal of Social Order*, *12*(4), 141-168.

Rahardjo, S. (2009). *Penegakan Hukum Suatu Tinjauan Sosiologis.* Yogyakarta: Genta Publishing.

Rasidin, M., Sidqi, I., & Witro, D. (2020). Drop Shipping in Islamic Economic Law Perspective: E-Commerce Study Inter Marketplace Drop Ship in The Industrial Revolution Era 4.0. *Nurani: Jurnal Kajian Syari'ah dan Masyarakat*, *20*(1), 97-106.

Saeed, M., Tuomisto, V., & Salluzzi, E. (2017). Unlocking the potential of digital trade. In *International Trade Forum* (No. 2, p. 32). International Trade Centre.

Shivpuri, D. (2021). Cyber Crime: Are the Law Outdated for this Type of Crime. *International Journal of Research in Engineering, Science and Management*, *4*(7), 44-49.

Taekema, S. (2018). Theoretical and normative frameworks for legal research: Putting theory into practice. *Law and Method*, https://ssrn.com/abstract=3123667

Thorleuchter, D., & Van den Poel, D. (2012). Predicting e-commerce company success by mining the text of its publicly-accessible website. *Expert Systems with Applications*, *39*(17), 13026-13034.

Trautman, L. J. (2015). E-Commerce, cyber, and electronic payment system risks: lessons from PayPal. *UC Davis Bus. LJ*, *16*, 261.

Widyaningrat, I. A. W., & Dharmawan, N. K. S. (2014). Tanggung Jawab Hukum Operator Telepon Selular Bagi Pengguna Layanan Jasa Telekomunikasi Dalam Hal Pemotongan Pulsa Secara Sepihak Di Denpasar. Kertha Semaya: *Journal Ilmu Hukum*, *2*(5), 1-5.