LEGAL AND CULTURAL IMPLICATIONS OF PERSONAL DATA PROTECTION IN THE ERA OF GLOBAL DIGITAL SOCIETY

Mustafa
Slamet Sarwo Edy
Faculty of Law, Universitas Proklamasi 45
mustafa@up45.ac.id

Abstract

The Indonesian government must safeguard, guarantee, and protect people's personal data from being hacked by irresponsible parties. This research examines laws regarding legal protection efforts for the right to personal data privacy from hacking crimes. However, this is not enough to guarantee protection against hacking of people's personal data in cyberspace, which is increasingly common nowadays, very broad, covering analysis of legal frameworks, comparison of international regulations, socio-cultural impacts, and challenges of cross-border implementation. The results of the research conclude that law enforcement regarding the protection of the right to privacy of personal data is not yet fully optimal, judging from the number of cases that have occurred recently. The legal pillars already exist, and our collective hope is that law enforcement can be carried out optimally, so that there are no more cases of hacking into someone's data, which could cause losses in the future. Apart from that, there is legal uncertainty regarding the protection of personal data, because Indonesia currently does not have legal instruments and technology that can detect data theft in the digital era. The author's view is that legal instruments for protecting privacy and personal data in the era of global digitalization must at least meet 3 criteria: (1) protecting privacy and personal data as a human right, (2) it is an element that binds individuals and society in all fields, including law, economics, and politics. and (3) international in nature.

Keywords: Personal Data; Legal Protection; Era of Digital Technology.

Abstrak

Pemerintah Indonesia harus menjaga, menjamin, dan melindungi data pribadi masyarakat dari peretasan oleh pihak-pihak yang tidak bertanggung jawab. Penelitian ini mengkaji peraturan perundang-undangan terkait upaya perlindungan hukum atas hak privasi data pribadi dari tindak kejahatan peretasan. Namun, hal ini belum cukup untuk menjamin perlindungan terhadap peretasan data pribadi masyarakat di dunia maya, yang saat ini semakin marak terjadi; penelitian ini mencakup analisis kerangka hukum, perbandingan regulasi internasional, dampak sosio-budaya, serta tantangan implementasi lintas batas. Hasil penelitian menyimpulkan bahwa penegakan hukum terkait perlindungan hak privasi data pribadi belum sepenuhnya optimal, dilihat dari jumlah kasus yang terjadi belakangan ini. Pilar-pilar hukum sudah ada, dan harapan kita bersama adalah penegakan hukum dapat dilakukan secara optimal, sehingga tidak ada lagi kasus peretasan data seseorang, yang dapat menimbulkan kerugian di masa depan. Selain itu, terdapat ketidakpastian hukum terkait perlindungan data pribadi, karena Indonesia saat ini belum memiliki instrumen hukum dan teknologi yang dapat mendeteksi pencurian data di era digital. Menurut pandangan penulis, instrumen hukum untuk melindungi privasi dan data pribadi di era digitalisasi global setidaknya harus memenuhi tiga kriteria: (1) melindungi privasi dan data pribadi sebagai hak asasi manusia, (2) merupakan unsur yang mengikat individu dan masyarakat di semua bidang, termasuk hukum, ekonomi, dan politik, serta (3) bersifat internasional.

***Kata kunci**: Data Pribadi; Perlindungan Hukum; Era Teknologi Digital.*

A. Background

The increasingly rapid development of science and information technology in developed countries today has positive and negative impacts and is a challenge that must be faced by developing countries. Changes in law and culture in society are the implications of advances in science and technology. In information technology, the anxiety generated by this change often results in financial worries for society.[1] Thus, one of the things that influences the development of digital information technology is the interaction between individuals and public institutions that serve the public in the global digital era.[2] Various sectors of life have utilized science and information technology, including data collection, data storage, data processing, production, and delivery, from industry to society's culture, quickly and effectively. The scope of information systems includes e-commerce, e-transportation, e-industry, e-tourist, e-government, e-payment, e-education, e-medicine, e-laboratory, and others.[3]

The growth of science and information technology today is very rapid, and its impact is also very large on legal and cultural events in everyone's lives. So it can be said that now every aspect and stage of a person's life is touched by the progress of science and the development of science and technology. Science and technology are not simple entities because they are related to the essential drives and creative instincts in humans. What is the relationship between changes in law, culture, and technology, which are closely related, interdependent, and influence each other in the social and cultural life of society, so that with these developments, society cannot just ignore them, when another individual's personal data is used by an irresponsible person? (harm others), by taking advantage of today's technology.[4]

Information has given birth to a global legal and cultural norm, meaning that every person who has information naturally has the instinct to always distribute it to other people, without using other people's data.[5] Collecting large amounts of information about a person's personal data using digital technology, which started in the early 1970s using computers until now expanded to the internet. The development of digital information technology is a

[1] T. Jacob, *Manusia Ilmu dan Teknologi: Pergumulan Abadi Dalam Perang dan Damai* (Yogyakarta: Tiara Wacana 1988), 19-20.
[2] Sinta Dewi Rosadi, "Konsep Perlindungan Hukum atas Privasi dan Data Pribadi Dikaitkan dengan Penggunaan Cloud Computing di Indonesia," *Yustisia* 5, no. 1 (2016): 22, https://doi.org/10.20961/yustisia.v5i1.8712.
[3] Wawan Wardiana, "Perkembangan Teknologi Informasi di Indonesia," paper presented at *Seminar dan Pameran Teknologi Informasi 2002*, Fakultas Teknik, Universitas Komputer Indonesia (UNIKOM), Jurusan Teknik Informatika, Bandung, July 9 (2002): 1, http://eprints.rclis.org/6534/1/WAWAN_PERKEMBANGAN_TI.pdf.
[4] The Liang Gie, *Pengantar Filsafat Teknologi* (Yogyakarta: Andi, 1996), 78.
[5] Abdul Raman Saad, *Personal Data & Privacy Protection* (Selangor, Malaysia: Puddingburn Publishing, 2005), 1-2.

revolution in the field of computer technology that can store large amounts of personal data. The development of computer technology is a combination of internet-based cloud computing. Meanwhile, this progress is contrary to the Right to Personality in Indonesia, which guarantees its protection in the Indonesian Constitution, especially as confirmed in Article 28 G paragraph (1) of the 1945 Constitution, which states:

"Everyone has the right to protect themselves, their family, honor, dignity, and property under their control, and has the right to a sense of security and protection from the threat of fear of doing or not doing something, which is a human right."

The protection of information privacy regarding personal data in Indonesia is still very weak, because no one guarantees that someone's private data will not be compromised. This is suspected by the fact that there is still a lot of misuse of people's personal data, including for business and political interests. There are still many companies that buy and sell personal data without the permission of the data subject. When someone fills in their personal data in a credit card application form, for example, there are several banks that sell this data to other companies for certain purposes. Even though it is protected by Indonesia has a legal basis for protecting personal data, namely Law Number 27 of 2022 concerning Personal Data Protection, which provides legal protection for a person's personal data, because personal data is the essence of human rights inherent in it.

The aforementioned laws and regulations on personal data protection provide a strong legal basis for those providing legal protection to the public in the digital technology era. Legal protection for the public is a key principle in law enforcement, ensuring legal certainty, benefit, justice, and accountability to the public, and ensuring the public feels secure about their personal data. In this global digital era, there are many crimes that utilize a person's personal data, for business or political purposes, so it needs to be protected by the state by providing very severe punishments for the perpetrators as a form of deterrent effect for their actions. So many people don't understand that personal data is prone to misuse by irresponsible parties.[6] Therefore, the challenge as a digital platform user is to be able to protect our data ourselves and that of others. There is increasing concern over the emergence of generative AI as it relates to cybersecurity. The emergence of DevenceGP T is another possible cyber threat because GenAI can help create business email compromises on a large scale.

[6] Muhammad Yudistira, & Ramadani, "Tinjauan Yuridis Terhadap Efektivitas Penanganan Kejahatan Siber Terkait Pencurian Data Pribadi Menurut Undang-Undang No. 27 Tahun 2022 Oleh Kominfo," *Unes Law Review* 5, no. 4 (2023): 3804, https://doi.org/10.31933/unesrev.v5i4.

Our society loves to share and interact, so sometimes we forget that there are people who use our personal data." Personal data leaks in Indonesia are currently widespread and causing public concern. This demonstrates that cybercrime has become a hot topic, as mass data leaks have become a ticking time bomb for Indonesians in the current digital technology era, with blackmail and online fraud. "In the current context, personal data is the new oil. Sometimes we provide full name and telephone number data. Other times, we provide home address data and e-mail. This combination of data can be misused by irresponsible parties, for example, for banking purposes (scam).[7]

B. Research Methods

This research includes normative legal research, or what is often called doctrinal research, with research objects or targets in the form of regulations, legislation, and other legal materials.[8] Normative research generally involves researching library materials or secondary materials covering primary, secondary, and tertiary legal materials. This research focuses on the legal protection of the right to privacy and personal data in the digital era, including how to define, classify, and scope the right to privacy and personal data itself. For this reason, this research is based on statutory regulations to see how the state provides protection and guarantees for Indonesian citizens regarding the right to privacy and personal data based on Law Number 27 of 2022, as well as analytical and comparative research to find out how the Indonesian state guarantees Personal personal data is used as a comparison because Indonesia is a country that is still developing, so the flow of globalization is very easy to accept, without considering the legal risks and changes in its culture, because the regulations regarding the right to privacy and personal data of its citizens are protected by law. In this normative legal research, the method used in collecting legal material is literature study or document study. The comparative analysis in this research aims to reveal two main approaches: a comprehensive model of individual rights protection (such as in the European Union) and a more fragmented or context-specific model (such as in the US and Indonesia), which is influenced by cultural differences and economic/political priorities.[9] This research uses a multidisciplinary approach that combines rigorous legal analysis with social and cultural perspectives to provide a comprehensive understanding of personal data protection

[7] Tri Meilani Ameliya, "Japelidi ajak masyarakat berempati saling lindungi data pribadi," Antaranews, 19 November 2021, https://www.antaranews.com/berita/2534125/japelidi-ajak-masyarakat-berempati-saling-lindungi-data-pribadi?
[8] Johnny Ibrahim, *Teori dan Metodologi Penelitian Hukum Normatif*, (Malang: Bayumedia, 2005), 302.
[9] Bambang Waluyo, *Penelitian Hukum dalam Praktek*, (Jakarta: Sinar Grafika, 2002), 18-19.

in the global digital era.

In order to ensure effective protection of personal data, there needs to be cooperation between the government, law enforcement, and the public in increasing awareness of the importance of protecting personal data and ensuring compliance with the provisions in Law Number 27 of 2022. There is also an insistence on the need for a number of regulations regarding the protection of personal data. recognized by the government. In fact, there are already a number of personal data protection regulations that have been established by the government, but so far, they are still general. Such as Minister of Communication and Information Regulation Number 20 of 2016 concerning Protection of Personal Data in Electronic Systems, which has been in effect since December 2016.

C. Results and Discussions

Today's advances in science and information technology have brought major changes to everyday life. However, the development of science and information technology poses threats and worries to human life while also having benefits. For example, artificial intelligence (AI), a technology that is currently widely used and developed in various scientific disciplines, is one of which is in the field of law. The existence of AI in the legal sector is now starting to show its positive influence. The following are some of the roles of AI in supporting law enforcement in various countries, including document processing, risk analysis, information retrieval, decision making, case management, and fraud prevention. Question? Is IA capable of handling cases of personal data leakage, considering that every year, data leaks in Indonesia are very large? This can be seen from data on cases of personal data leakage in Indonesia due to hacking. A person's personal data must be protected and kept confidential, because it is a public right guaranteed by the state.

Protection of personal data related to a person's identity, such as Family Card, Population Identification Number, and other data that must be protected by the state. Thus, it is very unfortunate that recently, suspected cases of personal data leakage have increasingly emerged; Indonesia is even ranked 3rd in the world, with the most data leaks. The increase in crimes against personal data security reflects that the legal system is not functioning properly. Data misuse vulnerabilities a person's personal property, which is a consequence of this problem. There are irresponsible parties who use someone's data to commit cyber crimes, for example, using it for fraud, piracy, illegal access, and manipulation of election

data.[10] Of the many cyber attacks that were hacked, the capital Jakarta, the center of Indonesia's economy, became the province with the most cyber attacks in 2023.

Table 1. Global Cyber Attacks on Indonesia in 2023

Province Name	Number of Cyber Attacks
Jakarta	100,98 million
Riau	72,93 million
Jawa Tengah	72,93 million
Total	**246,84 million**

Source: Muhammad Nur Firman, 2023.[11]

Looking at the case above, there are five (5) policies that must be taken by the Indonesian government to prevent leakage of the personal data of its citizens, which are guaranteed by the country's constitution as follows:

1. Legal Policy Regarding the Protection of Personal Data on Social Media

There are no legal policies regarding the protection of personal data in Indonesia that specifically regulate this matter. However, there are several regulations that can be legally enforced if there is misuse of personal data, namely, Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions, where electronic transactions via social media can also cause data leaks and cybercrime.[12] Cybercrime is as follows: global and transnational in nature, does not cause easily visible chaos, involves universal perpetrators of all ages, the use of technology is difficult to understand, and results in both material and non-material losses.[13] A person can be sued if they cause harm as a result of violating norms and their actions can be held accountable.[14]

According to the UK's National Criminal Intelligence Service (NCIS), manifestations of cybercrime appear in various types or variants as follows.

a. Unauthorized Access

[10] Fanny Priscyllia, "Perlindungan Privasi Data Pribadi Perspektif Perbandingan Hukum," *Jatiswara* 34, no. 3 (2019): 241, https://doi.org/10.29303/jtsw.v34i3.218.
[11] Muhammad Nur Firman, "Data Jumlah Serangan Cyber di Indonesia Tahun 2023," Widya Security, 2023, https://widyasecurity.com/2024/02/02/data-jumlah-serangan-cyber-di-indonesia-tahun-2023/?.
[12] Buletin APJII, https://apjii.or.id/assets/media/buletin_apjii_edisi_88_-_juni_2021_bulletin.pdf. (accessed 19 February 2024).
[13] *Ibid*.
[14] Sahat Maruli Tua Situmeang, "Penyalahgunaan Data Pribadi sebagai Bentuk Kejahatan Sempurna dalam Perspektif Hukum Siber," *SASI* 27, no. 1 (2021): 49, https://doi.org/10.47268/sasi.v27i1.394.

An attempt to use a system, network, data, or device without official authorization. This often involves hacking and security exploits, which can lead to data theft, financial loss, and reputational damage. Prevention includes the use of strong passwords, system updates, monitoring user activity, and public awareness training on cybersecurity.[15]

b. Illegal Contents

One of the IT-related crime groups. Illegal Content is a criminal offense related to illegal activity online. The Electronic Crime and Illegal Content Law is regulated under the Electronic Information and Transactions Law. Illegal Content involves inputting data or information into the internet in an unethical, fraudulent, unlawful, or disruptive manner, and is considered a cybercrime. In simple terms, Illegal Content is disseminating activities such as uploading and writing things that are wrong or prohibited. which can harm other people.[16]

c. Deliberate Spread of Viruses

The act of spreading computer viruses via sending e-mail is not specifically regulated. However, Article 30 paragraph (2) of the Electronic Transaction Information Law confirms that several actions are prohibited and punishable by criminal sanctions, including the prohibition against accessing other parties' computers and/or electronic systems unlawfully, so that the act of spreading computer viruses through sending e-mail (cyber spamming) can be considered a criminal offence.[17]

d. Data Forgery

Data falsification, often referred to as data forgery, is a falsification or criminal act involving unauthorized copying. According to Article 35, data falsification must be committed "intentionally" and/or "without authority" and/or "against the law." owned by institutions or institutions with database websites created as if there was a "typo" which in the end will benefit the perpetrator because the victim will enter personal data and credit card numbers which could be misused.

e. Cyber Terrorism

Cyber terrorism is an unlawful attack on computer networks. Information networks are attacked with the aim of intimidating governments or their citizens. Such attacks result

[15] Unknown, "Probing atau port scanning," https://pejuangkabupaten.blogspot.com/2018/07/probing-atau-port-scanning-satu-langkah.html. (accessed 19 February 2024).
[16] Barda Nawawi Arief, *Tindak Pidana Mayantara: Perkembangan Kajian Cyber Crime di Indonesia* (Jakarta: PT Raja Grafindo Persada, 2006), 42.
[17] Supanto, "Perkembangan Kejahatan Teknologi Informasi (Cyber Crime) dan Antisipasinya dengan Penal Policy," *Yustisia* 5, no. 1 (2016): 59, https://doi.org/10.20961/yustisia.v5i1.8718.

in violence against individuals, groups, or governments that are highly sensitive to the public. Satellite systems, telecommunications, banking, air traffic control, maritime navigation systems, telecommunications networks, electricity distribution, defense and security networks, including weapons of mass destruction (WMD) control systems, including nuclear bombs, health and other forms of public service facilities are targeted. terrorist crimes.[18]

f. Political Hacking

Crime Political activities or more popularly known as hacktivists destroy hundreds of websites to campaign for their programs, and often even use them to post messages to discredit their opponents. This effort was carried out actively and efficiently for the anti-Indonesian campaign on the East Timor issue spearheaded by Ramos Horta.

g. Gambling

Gambling in the global cyber world. This activity can be played back in countries that are tax havens, such as Cyman Island which is a paradise for money laundering, even Indonesia is often used as a destination country for money laundering.

h. Denial of Service Attack

A denial of service attack, also known as "unprecedented" by the FBI (Federal Bureau of Investigation), aims to jam the system by disrupting access from legitimate users. The tactic used is to flood the website with unimportant data. The site owner will suffer a lot of losses because controlling or re-controlling the website takes a long time.

i. Insiders or internal hackers

This crime can be committed by people within the company itself. The method is to use employees who are disappointed or have problems with the company.

j. Viruses

Malicious programs that spread viruses today can be transmitted via internet applications. Previously, the pattern of virus transmission was only via floppy discs. Viruses can hide in files and be downloaded by users, and can even spread through file submissions.

k. Piracy

Software piracy is a trend these days. Software producers can lose because their work can be pirated by downloading it from the internet and copying it onto a CD-room

[18] Janet J. Prichard & Laurie E. MacDonald, "Cyber Terrorism: A Study of the Extent of Coverage in Computer Security Textbooks," *Journal of Information Technology Education* 3 (2004): 280, https://www.jite.org/documents/Vol3/v3p279-289-150.pdf.

which is then reproduced illegally without the permission of the owner (creator).

l. Fraud

A type of manipulation of financial information with the aim of extracting maximum profits. For example, share prices are misleading through rumors, fictitious auction sites, and so on.

m. Pornography and pedophilia

Apart from bringing various conveniences by overcoming space and time constraints, the cyber world has also brought the world of pornography.

n. Cyber Espionage

This crime involves hacking to obtain confidential information from another party, especially in the context of business competition.

o. Infringements of Privacy

Crimes involving the theft of someone's personal information, such as credit card numbers or sensitive medical information.

p. Offense against Intellectual Property

Crimes involving violations of intellectual property rights on the internet, such as website impersonation or theft of trade secret information.[19]

The security system against cybercrime is not only regulated in the law containing Electronic Information and Transactions (called the ITE Law), which discusses data protection from unauthorized use, protection carried out by electronic system operators, and protection against illegal access. However, an institution that is fully responsible is needed, so that personal data of national color is guaranteed from leaks. In the Information and Electronic Transactions Law Article 26 (ITE Law), it is required that any personal data stored in electronic media must first obtain approval from the owner of the data concerned.

Then anyone who violates these provisions can be subject to sanctions for the losses they have caused. Not only that, in the Information and Electronic Transactions Law, especially the article above, there is also a provision for the government to provide solutions when electronic system operators are found to have committed violations and not complied with the rules relating to personal data, and can file civil lawsuits with the court for violations that have been committed. done. Then, in Article 28G in paragraph (1) of the 1945 Constitution, it is stated:

[19] Arundati Swastika Waranggani, "Ini 3 Faktor yang Menjadi Penyebab Kejahatan Siber Mudah Terjadi," https://www.cloudcomputing.id/berita/3-faktor-penyebab-kejahatan-siber. (accessed 20 July 2024).

"Everyone has the right to protect themselves, their family, honor, dignity, and property under their control, and has the right to a sense of security and protection from the threat of fear of doing or not doing something which is a human right."

Based on the Electronic Information and Transactions Law, it can be concluded that every individual has the right to protection against personal data that has been used or misused by others. Misuse related to personal data is a form of legal/constitutional violation. Therefore, in the Personal Data Protection Law (PDP Law), it is stated that the use of another person's personal data can be subject to criminal sanctions of imprisonment of up to four (4) years and a maximum fine of IDR 4 billion. This is also stated in Article 27, paragraph (3) of the 1945 Constitution, namely:

"Every person intentionally and without right distributes and/or transmits and/or makes accessible Electronic Information and/or Electronic Documents which contain insulting and/or defamatory content."

If there is defamation due to the misuse of personal data, the perpetrator can be subject to Article 310 in paragraph 1 of the Criminal Code, which reads

"Any person who deliberately attacks someone's honor or good name by accusing them of something, with the clear intention of making it known to the public, is threatened for defamation with a maximum imprisonment of nine months or a maximum fine of four thousand five hundred rupiah."

2. Policies to Prevent Misuse of Personal Data

To ensure data privacy is protected, legal certainty is needed that strictly regulates and provides severe sanctions if violations are found, as mandated by the constitution or the highest legal document in the country. The principle of legality is important to guarantee these rights and must be recognized by all countries. Legal provisions can be used to guarantee the protection of personal data or information in the constitution. That is why the Indonesian government must immediately issue strict regulations regarding the protection of individual data or information and how to implement them.

There are so many cases of misuse of personal data when using social media nowadays, of course there are several factors that cause these violations, including:[20]

a. Lack of awareness and understanding of law enforcers regarding data privacy policies and how to act on the law that applies therein.

[20] Setyawati Fitri Anggraeni, "Polemik Pengaturan Kepemilikan Data Pribadi: Urgensi Untuk Harmonisasi dan Reformasi Hukum di Indonesia," *Jurnal Hukum & Pembangunan* 48, no. 4 (2018): 823, https://doi.org/10.21143/jhp.vol48.no4.1804.

b. Lack of public literacy or understanding in improving and maintaining the security of their personal data on social media.
c. There is the Fear of Missing Out (FOMO) phenomenon, which causes people to be carried away by using social media without paying attention to the policies for using social media.
d. There are system weaknesses in maintaining the security of users' personal data.

Based on this, it is necessary to know what policies should be implemented to protect and overcome the misuse of personal data.

a. Increase security on your social media by verifying and changing passwords regularly and checking where your accounts are linked.
b. Do not share personal information, such as passwords or changing accounts to other people.
c. The government is increasing education to the public regarding the security of the privacy of each individual's personal data.[21]
d. The government is more responsive and enforces laws related to cybercrime.
e. Social media platforms further strengthen their security systems and are not easily accessed by just anyone.

Implementation of the right to privacy requires that the level of protection of fundamental rights and freedoms be essentially equivalent to that of the international community. This can be seen in the premise that data protection is a fundamental right in the legal order that cannot be circumvented by the transfer of personal data to another country. Therefore, Transborder data flows are part of the task of protecting the fundamental rights of state institutions appointed by the state as fully responsible institutions, and a valid argument can be made to support the Information and Electronic Transactions law, including its implementation and data privacy security standards in Indonesia.

Regarding the positive law regarding the protection of personal data in Indonesia, it provides an understanding that the regulations in positive law still have various weaknesses, which result in legal violations. These weaknesses in the legal system can be interpreted as weaknesses in terms of structure, substance, and legal culture. In terms of legal substance and culture, the most dominant factors in legal violations committed by

[21] Maichle Delpiero, *et. al.*, "Analisis Yuridis Kebijakan Privasi dan Pertanggungjawaban Online Marketplace Dalam Perlindungan Data Pribadi Pengguna Pada Kasus Kebocoran Data," *Padjadjaran Law Review* 9, no. 1 (2021): 1, https://jurnal.fh.unpad.ac.id/index.php/plr/article/view/509/378.

business actors are not providing correct, clear, and honest information regarding consumer rights relating to the privacy of their personal data.[22]

a. Weaknesses of the Legal Structure

In terms of structure, the DPR, together with the government and related agencies as stakeholders, has not been able to formulate a legal change that truly becomes a guideline for carrying out strict supervision and action against perpetrators of crimes, so as not to harm other people. Weak law enforcement in Indonesia provides ample opportunity and space for criminals and economic criminals to use people's personal data without that person's consent; of course, in this case, the interests of other people are greatly harmed. Another thing in Indonesia is that an agency has not yet been established to supervise or monitor the use of personal data, so that it is not easily used and/or hacked by irresponsible parties.

Currently, the only institution that has carried out a supervisory function over in using someone's personal data is Bank Indonesia; however, according to its authority, Bank Indonesia has more of a supervisory function over banks than in representing the interests of consumers, while the institution needed is an institution that represents the interests of society in general.

b. Weaknesses in Legal Substance

Structural weaknesses will basically have an impact on the substance, namely regarding the provisions in statutory regulations. The weaknesses in legal substance in positive law, which regulate the protection of a person's personal data in Indonesia, are: First, the current provisions regarding the protection of personal data are inadequate. Second, sanctions are still weak against criminals who are negligent or misuse someone's personal data.

Third, there are no provisions regarding a body specifically established to supervise the use of someone's personal data. In this era, information on a person's personal data has become a commodity that can be misused by irresponsible parties, which can harm society. Fourth, weaknesses related to law enforcement. Legal rules and instruments are available, but how law enforcement can be realized is of course a shared responsibility for both the government, Bank Indonesia, business actors,

[22] Wahyudi Djafar, "Hukum Perlindungan Data Pribadi di Indonesia: Lanskap, Urgensi dan Kebutuhan Pembaruan," paper presented at *Tantangan Hukum dalam Era Analisis Big Data*, Program Pascasarjana Fakultas Hukum Universitas Gadjah Mada (UGM), Yogyakarta, August 26, 2019, https://learning.hukumonline.com/wp-content/uploads/2022/09/Hukum-Perlindungan-Data-Pribadi-di-Indonesia-Wahyudi-Djafar.pdf.

consumers, and law enforcement officials, such as police, prosecutors, and judges, so that the law can be enforced properly and so that stability can be created. national.[23]

Since the enactment of the Consumer Protection Law until now, this law has been the most sought after by people, but perhaps the least implemented. Why? because the direction of law enforcement still seems sporadic and unsystematic. Meanwhile, violations of consumer rights are very visible. There is no clear legal or political format as to where this protection will lead.[24]

c. Weaknesses of Legal Culture

Weaknesses in legal culture currently need to receive serious attention from the legal system, because the legal culture that exists in society is weak, resulting in many legal violations being committed by officials and the public, so that the legal culture that arises cannot be separated from the weak legal substance that provides a pessimistic perception of legal protection efforts provided by law.[25]

The legal culture that creates weaknesses includes: First; Community legal awareness, which is meant by legal culture, is the attitude of the community and business actors towards the law and the legal system, regarding value beliefs, ideas, and expectations about the law, which are very weak. Laws, as legal products created to protect society, are only seen as rules without clear aims and objectives. Second, Legal Awareness of Business Actors, are minor violations of the application of legal rules that apply in banking. Small things like this are usually the beginning of problems that occur between banks as business actors and the public as consumers, and are also factors in legal weaknesses that allow legal violations to occur in producing and trading goods and/or services. In contrast to consumer legal awareness, in this case, business actors actually take advantage of existing legal products and the public's lack of legal awareness to take advantage.[26]

3. Legal arrangements regarding the protection of personal data that has been hacked

With advances in science and information technology, the number of internet users is increasing, both among adults, teenagers, and children, which means that digital crimes

[23] Lia Sautunnida, "Urgensi Undang-Undang Perlindungan Data Pribadi di Indonesia: Studi Perbandingan Hukum Inggris dan Malaysia," *Kanun Jurnal Ilmu Hukum* 20, no. 2 (2018): 381-382, https://doi.org/10.24815/kanun.v20i2.11159.
[24] Yusuf Shofie, *Kapita Selekta Hukum Perlindungan Konsumen di Indonesia* (Jakarta: Citra Aditya Bakti, 2008), 231.
[25] Wahyudi Djafar, *Loc.Cit*.
[26] Hanifan Niffari, "Perlindungan Data Pribadi Sebagai Bagian dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi Suatu Tinjauan Komparatif dengan Peraturan Perundang-Undangan di Negara Lain," *Selisik Jurnal Hukum dan Bisnis* 6, no. 1 (2020): 8, https://doi.org/10.35814/selisik.v6i1.1699.

are increasingly occurring. The government should be able to create a very strong legal umbrella because it is necessary to offset the crime of hacking personal data via the internet, so that it will create a sense of security and comfort for storing personal data in cyberspace. In international law itself, the right to privacy of personal data is regulated in "The General Declaration of Human Rights" in article 12, which states that every person has the right to legal protection of their personal data. Indonesia has ratified the UDCHR, and this means that the government must be committed to strictly and systematically enforcing the law regarding the right to privacy. Existing laws are expected to be able to bring benefits, legal certainty, protection, and justice to the entire community.

Currently, regulations for the protection of personal data have been made in statutory regulations, namely:

a. Legislative Regulation Number 27 of 2022 concerning Personal Data Protection. On October 17, 2022, this regulation was ratified, considering that it is very It is important for the government to make efforts to provide legal certainty to the public regarding their personal data. This law is also used as the main reference if there is a violation of personal data. Created to avoid overlapping regulations and guarantee protection for the community. In article 1, general provisions are explained regarding the protection of personal data, while in article 57, it explains the administrative sanctions that will be imposed if this type of violation continues to be committed, and in article 67, it also discusses the criminal provisions of this act.
b. Law Regulation Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions Regulations regarding the protection of personal data are also in the ITE Law. It is hoped that this regulation can become a legal tool that can coordinate all kinds of violations in the fields of information and technology. In this regulation, there are also general provisions regarding efforts to protect a person's right to privacy and what sanctions will be imposed if the criminal act continues to occur.[27] In article 26, paragraph (2), it is explained that: "Any person whose rights as intended in paragraph (1) have been violated may file a lawsuit for losses incurred based on this law." The provisions in the article above are an effort to protect personal data in every electronic transaction

[27] Mas Rara Tri Retno Herryani, & Harsono Njoto, "Perlindungan Hukum Terhadap Kebocoran Data Pribadi Konsumen Online Marketace," *Selisik Jurnal Hukum dan Bisnis* 5, no. 1 (2022): 118, https://doi.org/10.30737/transparansi.v5i1.3096.

activity. Even though there is a legal umbrella that covers it, we as data owners must be responsible and always be vigilant regarding our own personal data.

c. Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions. This PTSE PP also talks a lot about the protection of a person's personal data. Article 8 explains that PSE must guarantee the security and reliability of electronic transactions as appropriate. Article 14 also explains many of the principles and obligations for protecting personal data. Article 100 paragraph (2) also explains the administrative sanctions that will be imposed if this is still violated. The sanctions that will be received include: written warning, fine, temporary suspension, termination of access, and removal from the list.

4. Parties Who Play a Role in Enforcing Personal Data Protection Laws Due to Hacking Crimes

The rapid development of information technology today requires us to always be alert to digital crime, which is always in the shadows. Hacking is a crime that does not discriminate. Even innocent people can become targets of criminal acts.[28] Therefore, it is necessary to have a real role from various parties so that legal pillars can be enforced as they should, for example:

a. The government, as a leader, has two main responsibilities in terms of protecting information and personal data belonging to its citizens; First, create a legal framework that regulates personal data protection as a privacy right. Second, carry out supervision and enforcement of these regulations, when their duties and roles run optimally.

b. The controller or data processor in protecting everyone's data, one of the parties that must play an active role is the controller and data processor. Whatever obstacles occur, of course, they must be able to overcome them and must also be able to choose risk mitigation measures that are their fortress, if there is a data leak in the existing system, because this is their duty and responsibility as control holders. The government, through the National Cyber and Crypto Agency (BSSN) Regulation No. 8 of 2020 concerning Security Systems and the Implementation of Electronic Systems, requires certification based on risk, whether at the highest or lowest level.

c. The parties who own the data are figures who play an important role in maintaining the privacy of personal data. When using social media, we should really understand the

[28] Selfina Agustin, "Dampak Kemajuan Teknologi Informasi Era Digital Terhadap Keamanan Data Pribadi Tantangan Dan Penanggulangan Terhadap Kejahatan Cyber," *Jurnal Penelitian Multidisiplin Bangsa* 1, no. 6 (2024): 500, https://doi.org/10.59837/jpnmb.v1i6.93.

code of ethics and procedures for using it. We also have to know what we can do and what we can't do, so that undesirable things don't happen in the future. Don't let regulations and other parties fulfill their role, but the data owner doesn't comply with the regulations, or instead discloses personal data that is private.

d. Law enforcement officers. When we talk about law enforcement, it is always closely related to law enforcement officials, whether police, judges, prosecutors, or BSSN. Because this is their domain and responsibility, the correlation between these parties is one of the main keys to enforcing existing laws.[29]

5. Safeguarding Personal Data in Online Crime

Indonesia, as a legal country, does not yet have legal provisions that specifically protect personal data or information.[30] However, Article 28G of the 1945 Constitution regulates guarantees of privacy protection, which includes the protection of personal information. Although not explained separately, this article may contain provisions related to the self-protection of Indonesian citizens, including the protection of personal data or information. Even though the Indonesian government has taken precautionary measures to maintain the confidentiality of personal data, this policy is still regulated through separate regulations and is an important part of personal data protection in general, not specifically.

Some of these actions are regulated by the ITE Law, Telecommunications Law, Company Documents Law, Basic Archives Regulations Law, Medical Law, Banking Law, and Administration Law. In Article 52 of 2000 concerning Telecommunications Businesses, the Internet as a Multimedia Service is referred to as a Telecommunications Service Provider which provides information technology-based services. The Personal Data Protection Statement makes it clear that this is a shared responsibility of individuals, communities, legal entities, and even countries. Therefore, the government must be able to provide protection to Indonesian citizens, not just rely on common sense. Therefore, preventive and control measures must be taken. One example is the careful disclosure and monitoring of personal data. Consisting of two controlling groups: private industry and government. Private industry groups include content producers and online service providers, internet service providers, or internet infrastructure owners, who are usually

[29] Sahat Maruli Tua Situmeang, *Op.Cit*., 47-50.
[30] Predderics Hockop Simanjuntak, "Perlindungan Hukum Terhadap Data Pribadi pada Era Digital di Indonesia: Studi Undang-Undang Perlindungan Data Pribadi dan General Data Protection Regulation (GDPR)," *Jurnal Esensi Hukum* 6, no. 2 (2024): 106, https://doi.org/10.35586/esensihukum.v6i2.412.

focused on specific industry sectors. Meanwhile, the government controls it through existing laws and regulations.

To ensure data privacy is protected, legal certainty is needed, which is regulated in the constitution, or the highest legal document in the country. The principle of legality is important to guarantee these rights and must be recognized by all countries. Legal provisions can be used to guarantee the protection of personal data or information in the constitution. That is why the Indonesian government must immediately issue strict regulations regarding the protection of individual data or information and how to implement them, as well as state institutions that can control all parties.

From the explanation of several of the laws mentioned above, there is not a single law and/or regulation that specifically regulates and institutions that guarantee hacking of someone's personal data. Thus, society is required to take personal care through; He also explained a number of ways to protect personal data, namely:

a. We have to be smart in managing software, especially passwords.
b. Maximize personal data protection, for example, by separating email for work and transactions.
c. Anticipate digital fraud, such as reading more on social media about new modes of digital fraud.
d. Put your digital track record first, such as not oversharing about your personal life, and
e. Harmony, namely working together to protect personal data, remains vigilant in an era like today, where the lifespan of digital traces may be longer than our lifespan.

According to Samuel A. Pangerapan, citing a statement from the Director General of Information Applications, there are five main reasons for protecting personal data, namely:

a. Gender-related online bullying
b. Prevent misuse of personal data by irresponsible parties;
c. Avoid potential fraud.
d. Avoid potential defamation; and
e. Right to control over personal data.[31]

This research also demonstrates that integrating international data protection theoretical frameworks, such as the GDPR and the OECD Privacy Guidelines, can strengthen the validity of comparative analysis between countries. By benchmarking

[31] Komdigi RI, "5 Alasan Mengapa Data Pribadi Perlu Dilindungi," https://www.komdigi.go.id/berita/sorotan-media/detail/5-alasan-mengapa-data-pribadi-perlu-dilindungi. (accessed 21 July 2024).

principles such as transparency, purpose limitation, and enforcement mechanisms, personal data protection policies in ASEAN can be directed toward a more inclusive, accountable, and adaptive model to global technological developments. Therefore, an approach that combines local dimensions with global normative references is a crucial strategy in formulating fair and effective personal data governance. So it can be concluded that law enforcement in Indonesia regarding the protection of privacy rights for personal data is not yet fully optimal, as seen from the many cases that have occurred recently. The legal pillars already exist, and our shared hope is that law enforcement can be carried out optimally, so that there are no more cases of hacking someone's data, which could result in losses.

D. Conclusions and Recommendations

In the current era, it is increasingly worrying because the use of the internet is increasingly disturbing, but it also provides enormous benefits for the progress of the nation, so that it is able to compete with other countries. It can be concluded that the protection of the right to privacy regarding private data is very necessary. because it concerns a person's identity and human rights. When this identity is hacked by irresponsible people, various other crimes will arise, such as fraud, piracy, manipulation of votes in elections, and so on. When this criminal act occurs, various parties will suffer losses (material and immaterial).

In Indonesia itself, there are already legal pillars that will serve as guidelines for Indonesian citizens together in following up on this case, namely: Law Number 27 of 2022 concerning Personal Data Protection, Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions, Government Regulation Number 71 of 2019 concerning Implementation of Electronic Systems and Transactions. With this regulation, all citizens are expected to be able to correlate between various parties such as the government, data processors, law enforcement officials, and, what is no less important, namely the data owners themselves, so that the objectives of this protection can be achieved as they should.

However, from the data obtained, it is very unfortunate that these regulations do not appear to have been implemented optimally, as can be seen from the many cases of hacking and misuse of personal data. Even in 2023, Indonesia will be ranked 3rd with the most hacking cases at 138.25 million in the world, and DKI Jakarta Province is the largest in all of Indonesia, with 100.98 million hacks.

References

Journal Articles

Agustin, Selfina. "Dampak Kemajuan Teknologi Informasi Era Digital Terhadap Keamanan Data Pribadi Tantangan Dan Penanggulangan Terhadap Kejahatan Cyber." *Jurnal Penelitian Multidisiplin Bangsa* 1, no. 6 (2024): 500-504. https://doi.org/10.59837/jpnmb.v1i6.93.

Anggraeni, Setyawati Fitri. "Polemic on Personal Data Ownership Regulations: The Urgency for Harmonization and Legal Reform in Indonesia." *Jurnal Hukum & Pembangunan* 48, no. 4 (2018): 814–825. https://doi.org/10.21143/jhp.vol48.no4.1804.

Delpiero, Maichle et. al. "Analisis Yuridis Kebijakan Privasi dan Pertanggungjawaban Online Marketplace Dalam Perlindungan Data Pribadi Pengguna Pada Kasus Kebocoran Data." *Padjadjaran Law Review* 9, no. 1 (2021): 1-11. https://jurnal.fh.unpad.ac.id/index.php/plr/article/view/509/378.

Herryani, Mas Rara Tri Retno, & Harsono Njoto. "Perlindungan Hukum Terhadap Kebocoran Data Pribadi Konsumen Online Marketace." *Selisik Jurnal Hukum dan Bisnis* 5, no. 1 (2022): 110-135. https://doi.org/10.30737/transparansi.v5i1.3096.

Niffari, Hanifan. "Perlindungan Data Pribadi Sebagai Bagian dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi Suatu Tinjauan Komparatif dengan Peraturan Perundang-Undangan di Negara Lain." *Selisik Jurnal Hukum dan Bisnis* 6, no. 1 (2020): 1-14. https://doi.org/10.35814/selisik.v6i1.1699.

Prichard, Janet J., & Laurie E. MacDonald. "Cyber Terrorism: A Study of the Extent of Coverage in Computer Security Textbooks." *Journal of Information Technology Education* 3 (2004): 279–289. https://www.jite.org/documents/Vol3/v3p279-289-150.pdf.

Priscyllia, Fanny. "Perlindungan Privasi Data Pribadi Perspektif Perbandingan Hukum." *Jatiswara* 34, no. 3 (2019): 239-249. https://doi.org/10.29303/jtsw.v34i3.218.

Rosadi, Sinta Dewi. "Konsep Perlindungan Hukum atas Privasi dan Data Pribadi Dikaitkan dengan Penggunaan Cloud Computing di Indonesia." *Yustisia* 5, no. 1 (2016): 22-30. https://doi.org/10.20961/yustisia.v5i1.8712.

Sautunnida, Lia. "Urgensi Undang-Undang Perlindungan Data Pribadi di Indonesia: Studi Perbandingan Hukum Inggris dan Malaysia." *Kanun Jurnal Ilmu Hukum* 20, no. 2 (2018): 369-384. https://doi.org/10.24815/kanun.v20i2.11159.

Simanjuntak, Predderics Hockop. "Perlindungan Hukum Terhadap Data Pribadi pada Era Digital di Indonesia: Studi Undang-Undang Perlindungan Data Pribadi dan General Data Protection Regulation (GDPR)." *Jurnal Esensi Hukum* 6, no. 2 (2024): 105-124. https://doi.org/10.35586/esensihukum.v6i2.412.

Situmeang, Sahat Maruli Tua. "Penyalahgunaan Data Pribadi sebagai Bentuk Kejahatan Sempurna dalam Perspektif Hukum Siber." *SASI* 27, no. 1 (2021): 38-52. https://doi.org/10.47268/sasi.v27i1.394.

Supanto. "Perkembangan Kejahatan Teknologi Informasi (Cyber Crime) dan Antisipasinya dengan Penal Policy." *Yustisia* 5, no. 1 (2016): 52-70. https://doi.org/10.20961/yustisia.v5i1.8718.

Wardiana, Wawan. "Perkembangan Teknologi Informasi di Indonesia." Paper presented at *Seminar dan Pameran Teknologi Informasi 2002*, Fakultas Teknik, Universitas Komputer Indonesia (UNIKOM), Jurusan Teknik Informatika, Bandung, July 9 (2002): 1-6. http://eprints.rclis.org/6534/1/WAWAN_PERKEMBANGAN_TI.pdf.

Yudistira, Muhammad, & Ramadani. "Tinjauan Yuridis Terhadap Efektivitas Penanganan Kejahatan Siber Terkait Pencurian Data Pribadi Menurut Undang-Undang No. 27 Tahun 2022 Oleh Kominfo." *Unes Law Review* 5, no. 4 (2023): 3802-3815. https://doi.org/10.31933/unesrev.v5i4.

Books

Arief, Barda Nawawi. *Tindak Pidana Mayantara: Perkembangan Kajian Cyber Crime di Indonesia*. Jakarta: PT Raja Grafindo Persada, 2006.

Gie, The Liang. *Pengantar Filsafat Teknologi*. Yogyakarta: Andi, 1996.

Ibrahim, Johnny. *Teori dan Metodologi Penelitian Hukum Normatif*. Malang: Bayumedia, 2005.

Jacob, T. *Manusia Ilmu dan Teknologi: Pergumulan Abadi Dalam Perang dan Damai*. Yogyakarta: Tiara Wacana 1988.

Saad, Abdul Raman. *Personal Data & Privacy Protection*. Selangor, Malaysia: Puddingburn Publishing, 2005.

Shofie, Yusuf. *Kapita Selekta Hukum Perlindungan Konsumen di Indonesia*. Jakarta: Citra Aditya Bakti, 2008.

Waluyo, Bambang. *Penelitian Hukum dalam Praktek*. Jakarta: Sinar Grafika, 2002.

Dissertation/Thesis/Working Papers

Djafar, Wahyudi. "Hukum Perlindungan Data Pribadi di Indonesia: Lanskap, Urgensi dan Kebutuhan Pembaruan." Paper presented at *Tantangan Hukum dalam Era Analisis Big Data*, Program Pascasarjana Fakultas Hukum Universitas Gadjah Mada (UGM), Yogyakarta, August 26, 2019. https://learning.hukumonline.com/wp-content/uploads/2022/09/Hukum-Perlindungan-Data-Pribadi-di-Indonesia-Wahyudi-Djafar.pdf.

Internet

Ameliya, Tri Meilani. "Japelidi ajak masyarakat berempati saling lindungi data pribadi." Antaranews. 19 November 2021. https://www.antaranews.com/berita/2534125/japelidi-ajak-masyarakat-berempati-saling-lindungi-data-pribadi? (accessed 19 February 2026).

Buletin APJII. https://apjii.or.id/assets/media/buletin_apjii_edisi_88_-_juni_2021_bulletin.pdf. (accessed 19 February 2026).

Firman, Muhammad Nur. "Data Jumlah Serangan Cyber di Indonesia Tahun 2023." Widya Security. 2023. https://widyasecurity.com/2024/02/02/data-jumlah-serangan-cyber-di-indonesia-tahun-2023/? (accessed 19 February 2026).

KeamananSiber. "'Satu Klik' Menuju Kebangkrutan, Dampak Ekonomi Serangan Siber." https://www.keamanansiber.com/2024/03/satu-klik-menuju-kebangkrutan-dampak.html? (accessed 13 Februari 2026).

Komdigi RI. "5 Alasan Mengapa Data Pribadi Perlu Dilindungi." https://www.komdigi.go.id/berita/sorotan-media/detail/5-alasan-mengapa-data-pribadi-perlu-dilindungi (accessed 21 July 2024).

Unknown. "Probing atau port scanning." https://pejuangkabupaten.blogspot.com/2018/07/probing-atau-port-scanning-satu-langkah.html. (accessed 19 February 2024).

Waranggani, Arundati Swastika. "Ini 3 Faktor yang Menjadi Penyebab Kejahatan Siber Mudah

Terjadi." https://www.cloudcomputing.id/berita/3-faktor-penyebab-kejahatan-siber. (accessed 20 July 2024).