

# Legal and Cultural Implications for Personal Data Protection in the Era of Global Digitalization

**Mustafa Slamet**

Universitas Proklamasi 45 Yogyakarta

[mustafa@up45.ac.id](mailto:mustafa@up45.ac.id)

**Sarwo Edy**

Universitas Proklamasi 45 Yogyakarta

[slametsarwo@up45.ac.id](mailto:slametsarwo@up45.ac.id)

DOI: 10.23917/laj.v10i2.7088

Submission track:

Reviewed:

6 November 2024

Final Revision:

17 September 2025

Available Online:

31 Januari 2026

Corresponding  
Author:

Mustafa Slamet  
[mustafa@up45.ac.id](mailto:mustafa@up45.ac.id)

## ABSTRAK

Kemajuan pesat Teknologi Informasi dan Komunikasi (TIK), khususnya penyebaran luas internet dan Kecerdasan Buatan (Artificial Intelligence/AI), telah mengubah tatanan masyarakat global secara fundamental. Meskipun perkembangan ini menawarkan manfaat yang signifikan, hal tersebut juga menimbulkan tantangan yang kompleks terhadap hak atas privasi dan perlindungan data pribadi. Studi ini menggunakan metode penelitian hukum normatif untuk mengkaji kerangka hukum dan budaya yang mengatur privasi data di era digital. Penelitian ini menganalisis peraturan perundang-undangan dan bahan hukum yang ada untuk mendefinisikan serta mengklasifikasikan ruang lingkup hak privasi di tengah revolusi digital. Lebih lanjut, penelitian ini menelaah persinggungan antara regulasi hukum dan nilai-nilai budaya, dengan argumen bahwa digitalisasi global tidak hanya memerlukan mekanisme hukum yang tangguh, tetapi juga pemahaman yang mendalam mengenai implikasi budaya. Temuan penelitian menunjukkan bahwa kerangka hukum saat ini harus beradaptasi dengan evolusi AI yang cepat dan sifat ekonomi digital yang tanpa batas, sembari tetap menghormati beragam pendekatan budaya terhadap privasi.

**Kata Kunci:** Perlindungan Data Pribadi, Digitalisasi, Kecerdasan Buatan (AI)

## ABSTRACT

The rapid advancement of Information and Communication Technology (ICT), particularly the proliferation of the internet and Artificial Intelligence (AI), has fundamentally transformed global society. While these developments offer significant benefits, they pose complex challenges to the right to privacy and personal data protection. This study employs a normative legal research method to examine the legal and cultural frameworks governing data privacy in the digital era. It analyzes the existing legislation and legal materials to define and classify the scope of privacy rights amidst the digital revolution. Furthermore, this research investigates the intersection between legal regulations and cultural values, arguing that global digitalization requires not only robust legal

---

mechanisms but also a profound understanding of cultural implications. The findings suggest that current legal frameworks must adapt to the swift evolution of AI and the borderless nature of the digital economy while respecting diverse cultural approaches to privacy

---

**Keywords:** Personal Data Protection, Digitalization, Artificial Intelligence (AI)

---

## INTRODUCTION

Along with global technological developments, all aspects of life have been affected, including economics, politics, culture, art, and education. Technological progress is inevitable in this life, as it goes hand in hand with scientific progress. Every innovation must provide positive benefits for humanity. Ease and new ways of doing human activities, particularly in the field of information technology, have brought numerous benefits through discoveries in the last decade (Jacob, 2016). Technology is becoming increasingly complex with innovations such as artificial intelligence (AI), robotics, the Internet of Things (IoT), and renewable energy (Dewi, 2015). These developments will continue to shape the future technology landscape, driving efficiency and convenience, but also requiring appropriate regulation and ethics to ensure maximum benefits for society (Wardiana, 2002).

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 does not just ignore it, if someone's personal data is not used by irresponsible people? (harm others), by taking advantage of today's technology (Gie, 1996).

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 (Saad, 2022). Collecting large amounts of information about a person's personal data using digital technology which started in the early 1970s using computers until now using the internet. One of the developments in information technology is a revolution in the field of computer technology that can store large amounts of private personal data, which is called cloud computing, which is a combination of the use of computer technology ('computing') and internet-based development ('cloud'). 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."

Protection of information privacy regarding personal data in Indonesia is still very weak, because no one guarantees that someone's privacy data will 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 Law Number 27 of 2022 concerning Personal Data Protection, it provides legal protection for personal data which must be protected because it is part of human rights.

This law provides a clear legal basis for personal data controllers to process personal data in accordance with the principles of personal data protection. Personal data protection must be carried out in accordance with the principles of personal data protection, namely the principles of clarity, certainty, openness, limited use, compliance, collection, approval for the use of personal data, processing of personal data, security of personal data, deletion or destruction of personal data, and accountability of data controllers. personal.

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. Therefore, the challenge as a digital platform user is to be able to protect your data ourselves and 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.

Our society loves to share and interact, so sometimes we forget that there are people who use our personal data." Weak legal protection of data privacy in Indonesia has resulted in widespread data leaks. This is proven by the frequent occurrence of cybercrime cases, such as hacking and social media cracking, which lead to the breach of personal data, 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) (Kurnia, 2021).

## RESEARCH METHODOLOGY

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 (Ibrahim, 2013). 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 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. -invite. In this normative legal research, the method used in collecting legal materials is literature study or document study (Waluyo, 2002).

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.

## DISCUSSION

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, 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. Personal data must be protected and kept confidential, so that citizens' constitutional rights can be said to be guaranteed.

Personal data is information related to a person's identity, for example, Family Card (KK), Population Identification Number (NIK), and so on. However, 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 cases of data leakage. The rise in these cases reflects that the security and regulatory system in Indonesia is not strong enough. Data misuse vulnerabilities a person's personal property is a consequence of this problem. Irresponsible parties will use this data to carry out criminal acts, for example: using it for fraud, piracy, illegal access, manipulation of election data (Priscyllia, 2019).

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.

No	Province Name	Number of Cyber Attacks
01	Jakarta	100,98 million
02	Riau	72,93 million
03	Jawa Tengah	72,93 million
amount		246,84 million attack

Source: <https://widyasecurity.com/2024/02/02/data-nomor-serangan-cyber-di-indonesia-tahun-2023/>

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. Cybercrime is as follows:

global and transnational in nature, does not cause easily visible chaos, universal perpetrators of all ages, the use of technology is difficult to understand, and material and non-material losses (Buletin APJII, 2021).

According to the UK's National Criminal Intelligence Service (NCIS), manifestations of cyber crime appear in various types or variants as follows (Situmeang, 2021).

a. Unauthorized Access

This crime occurs when someone enters or infiltrates a computer network system without the permission or knowledge of the owner. Examples of these crimes include probing and port scanning, for example; Scanning results can show that the target server is running the Apache web server program, Sendmail mail server (Unknown, 2018).

b. Illegal Contents

One of the IT-related crime groups. Illegal Content can be interpreted as a crime by entering data or information on the internet about something that is incorrect, unethical and can be considered to violate the law or disturb public order. In simple terms, Illegal Content is disseminating activities such as uploading and writing things that are wrong or prohibited. which can harm other people (Arief, 2006).

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 ITE 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 (Supanto, 2016).

d. Data Forgery

Data Forgery is a crime involving falsifying data on important documents stored as scriptless documents via the Internet. This crime is usually aimed at e-commerce documents 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, stored information networks with the aim of intimidating the government or its people. Such attacks result in violence against individuals, groups or government property and create danger and fear. 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 (MacDonald, 2004).

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 heavens, 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 or 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 themselves. 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.

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

o. Froud.

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.

p. Pornography and pedophilia.

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

q. Cyber Espionage

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

r. Infringements of Privacy

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

or sensitive medical information.

s. Offense against Intellectual Property

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

The security system from cyber crime 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 the use of any personal data 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 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:

"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 contents of the Information and Electronic Transactions Law above, it can be concluded that every individual has the right to privacy protection regarding personal data that has been used or misused by others. Where misuse of privacy regarding personal data is a form of legal/constitutional violation. In the Personal Data Protection Law (UU PDP), it is stated that using other people's personal data can be subject to sanctions resulting in a maximum penalty of 4 years in prison and a maximum fine of IDR 4 billion. It is also stated in Article 27 in 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 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 (Anggraeni, 2018):

- a. Lack of awareness and understanding of law enforcers regarding data privacy policies and how to act on the law that should apply therein.
- b. Lack of public literacy or understanding in improving and maintaining the security of their privacy 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 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 telling 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 (Delpiero et al., 2021).
- d. The government is more responsive and enforces laws related to cyber crime.
- e. Social media platforms further strengthen their security systems and are not easily accessed by just anyone.

Implementation of the right to privacy requires a level of protection of fundamental rights and freedoms that is essentially equivalent to that in the international community. This is based on the premise that data protection is now a fundamental right in the legal order that cannot be circumvented by the transfer of personal data to third countries. 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 (Amendments to Law Number 11 of 2008 Concerning Electronic Information and Transactions, 2016).

Regarding 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 business actors are not providing correct, clear and honest information regarding consumer rights relating to privacy of their personal data (Djafar, 2019).

In terms of legal substance and culture, the most dominant factors in legal violations committed by business actors are not providing correct, clear and honest information regarding consumer rights relating to privacy of their personal data.

## 1. Weaknesses of the Legal Structure

In terms of structure, the DPR, together with the government and related agencies as stakeholders, have 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 the use of a person's personal data is Bank Indonesia, however, according to its authority, Bank Indonesia has more of a supervisory function over banks than on representing the interests of consumers, while the institution needed is an institution that represents the interests of society in general.

## 2. 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 a person's personal data. Because in this era, information on a person's personal data has now 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, 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 (Sautunnida, 2018).

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 political format as to where this protection will lead (Shofie, 2008).

### **3. 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, so that many legal violations are committed by officials and the public, so that the legal culture that arises cannot be separated from the weak legal substance that provides pessimistic perception of legal protection efforts provided by law (Djafar, 2019).

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 (Niffari, 2020).

### **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 increasing, both among adults, teenagers and children, means that digital crimes 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 his 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:

- 1) Legislative Regulation Number 27 of 2022 concerning Personal Data Protection on October 17 2022, this regulation was ratified, considering that it is very 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 obtained if this type of violation continues to be committed, in article 67 it also discusses the criminal provisions of this act.
- 2) 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, which 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 received if the criminal act continues to occur (Herryani, 2022). 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 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.
- 3) 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 received 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 crime is a crime that does not discriminate. Even innocent people can become targets of criminal acts.

Therefore, it is necessary to have a real role from various parties so that legal pillars can be enforced as they should, for example:

1) 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.

2) 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.

3) 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 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.

4) 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 (Situmeang, 2021).

#### **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. 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 (Concerning the Implementation of Electronic Systems and Transformation, 2019). 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 (Anggraeni, 2018). 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 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:

1. We have to be smart in managing software, especially passwords;
2. Maximize personal data protection, for example separating e-mail for work and transactions;
3. Anticipate digital fraud, such as reading more on social media about new modes of digital fraud;
4. Put your digital track record first, such as not oversharing about your personal life; And

5. Harmony, namely working together to protect personal data, remaining 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:

1. Gender-related online bullying;
2. Prevent misuse of personal data by irresponsible parties;
3. Avoid potential fraud;
4. Avoid potential defamation; And
5. Right to control over personal data (Kominfo, 2021).

So, it can be concluded that law enforcement in Indonesia regarding the protection of privacy rights for personal data is not yet fully optimal, 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 of someone's data which could result in losses.

## CONCLUSION

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, therefore it can be concluded that 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

Amendments to Law Number 11 of 2008 Concerning Electronic Information and Transactions, Pub. L. No. 19 (2016).

Anggraeni, S. F. (2018). Polemic on Personal Data Ownership Regulations: The Urgency for Harmonization and Legal Reform in Indonesia. *Journal of Law & Development*, 48(4), 814–825.

Arief, B. N. (2006). *Mayantara Crime: Developments in Cyber Crime Studies in*. Mayantara Crime: Developments in Cyber Crime Studies in Indonesia.

Buletin APJII. (2021). Menelisik Dugaan Kasus Kebocoran Data BPJS Kesehatan. *Buletin APJII. Concerning the Implementation of Electronic Systems and Transformation*, 70 (2019).

Delpiero, M., Reynaldi, F. A., Ningdiah, I. U., & Muthmainnah, N. (2021). Juridical Analysis of Privacy Policy and Online Marketplace Liability in Protecting Users' Personal Data in Data Leak Cases. *Padjadjaran Law Review*, 9(1).

Dewi, S. (2015). The Concept of Legal Protection for Privacy and Personal Data Linked to the Use of Cloud Computing in Indonesia. *Justice*. Vol.5 No.1 January-April 2016. *Justice*, 5(1), 165. file:///C:/Users/hp/Downloads/8712-15812-1-PB.pdf.

Djafar, W. (2019). Personal data protection law in Indonesia: landscape, urgency and need for reform. In *Legal Seminar in the Era of Big Data Analysis, UGM Faculty of Law Postgraduate Program* (Vol. 26).

Gie. (1996). *Introduction to the Philosophy of Technology* (pp. 1–2).

Herryani, M. R. T. R. (2022). "Legal Protection Against Marketace Online Consumer Personal Data Leaks." *Legal Transparency*, 5(1), 110–33.

Ibrahim, J. (2013). *Theory and Methodology of Normative Legal Research*.

Jacob, T. (2016). *Humans, Science and Technology Eternal Struggle in War and Peace*.

Kominfo. (2021). *No Title*. <https://aptika.kominfo.go.id/2021/10/pentingnya-pelindungan-data-pribadi-di-era-digital>.

Kurnia, N. (2021). *As National Coordinator of the Digital Literacy Activist Network (JAPELIDI) at the Siberkreasi Talk event*. Friday.

MacDonald, J. J. P. L. E. (2004). Cyber Terrorism: A study of the extent of coverage in computer security textbooks. *Journal of Information Technology Education*, 3. 200, 280.

Niffari, H. (2020). "Personal Data Protection as Part of the Human Right to Personal Protection, a Comparative Review with Legislation in Other Countries." *Journal of Law and Business (Investigation*, 6(1), 1–14.

Priscyllia, F. (2019). "Personal Data Privacy Protection in a Comparative Legal Perspective." *Jatiswara*, 34(3), 1–5.

Saad, A. R. (2022). *Personal Data & Privacy Protection*. Puddingburn Publishing.

Sautunnida, L. (2018). The Urgency of Personal Data Protection Laws in Indonesia: A Comparative Study of British and Malaysian Laws. *Kanun Journal of Legal Studies*, 20(2), 369–384.

Shofie, Y. (2008). *Capita Selecta Consumer Protection Law*. PT Citra Aditya Bakti.

Situmeang, S. M. T. (2021). Misuse of Personal Data as a Perfect Form of Crime from a Cyber Law Perspective. *Sasi*, 27(1), 38–52.

Supanto. (2016). *Development of Information Technology Crime (Cyber Crime) and its Anticipation*

with *Penal Policy*, *Jurnal Yustisia* (p. 59).

Unknown. (2018). *Probing atau Port Scanning*.  
<https://pejuangkabupaten.blogspot.com/2018/07/probing-atau-port-scanning-satu.html>

Waluyo, B. (2002). *Legal Research in Practice*. Sinar Graphics.

Wardiana, W. (2002). *Development of Information Technology in Indonesia*. Indonesian Computer University.

[https://www-pwc-com.translate.goog/bm/en/press-releases/pwc-2024-global-digital-trust-insights.html?\\_x\\_tr\\_sl=en&\\_x\\_tr\\_tl=id&\\_x\\_tr\\_hl=id&\\_x\\_tr\\_pto=sc](https://www-pwc-com.translate.goog/bm/en/press-releases/pwc-2024-global-digital-trust-insights.html?_x_tr_sl=en&_x_tr_tl=id&_x_tr_hl=id&_x_tr_pto=sc). Diakses pada tanggal 19/07/2024. jam 13.00

[https://www.google.com/search?q=Peraturan Menteri Kominfo Nomor 20 Tahun 2016 mengenai Perlindungan Data Pribadi dalam Sistem Elektronik yang berlaku sejak Desember 2016.&oq=Peraturan+Menteri+Kominfo+Nomor+20+Tahun+2016+mengenai+Perlindungan+Data+Pribadi+dalam+Sistem+Elektronik+yang+berlaku+sejak+Desember+2016.&gslcrp=EgZjaHJvbWUyBggAEEUYOdIBCDExNjlqMGo3qAIAsAIA&sourceid=chrome&ie=UTF-8](https://www.google.com/search?q=Peraturan+Menteri+Kominfo+Nomor+20+Tahun+2016+mengenai+Perlindungan+Data+Pribadi+dalam+Sistem+Elektronik+yang+berlaku+sejak+Desember+2016.&oq=Peraturan+Menteri+Kominfo+Nomor+20+Tahun+2016+mengenai+Perlindungan+Data+Pribadi+dalam+Sistem+Elektronik+yang+berlaku+sejak+Desember+2016.&gslcrp=EgZjaHJvbWUyBggAEEUYOdIBCDExNjlqMGo3qAIAsAIA&sourceid=chrome&ie=UTF-8). Diakses pada tanggal 19-07-2024. jam 13.00

<https://widyasecurity.com/2024/02/02/data-jumlah-serangan-cyber-di-indonesia-tahun-2023/>

[https://apjii.or.id/assets/media/buletin\\_apjii\\_edisi\\_88\\_-\\_juni\\_2021\\_bulletin.pdf](https://apjii.or.id/assets/media/buletin_apjii_edisi_88_-_juni_2021_bulletin.pdf). Diakses pada tanggal 19-07-2024. jam 21.00

<https://pejuangkabupaten.blogspot.com/2018/07/probing-atau-port-scanning-satu-langkah.html>. Diakses pada tanggal 20-07-2024.jam.22

<http://kelompokeptik18.blogspot.co.id/2016/04/contoh-kasus-data-forgery.html>. Diakses pada tanggal 20-07-20240. Jam 23.00

<https://www.cloudcomputing.id/berita/3-faktor-penyebab-kejahatan-siber>. Diakses pada tanggal 20.07.2024. jam 7.30

<https://aptika.kominfo.go.id/2021/10/pentingnya-pelindungan-data-pribadi-di-era-digital>. Diakses pada tanggl 21/07/2024. jam 12.00