Annals of Justice and Humanity (AJH)
Vol 1, No 1, 2021, 29-37 https://doi.org/10.35912/ajh.v1i1.1383

Prevention of personal data privacy leakage in e-government, as the government's responsibility

Yayang Nuraini Zulfiani
Faculty of Law, UIN Sunan Gunung Djati Bandung, Indonesia
yayangnurainizulf@gmail.com

Article History
Received on 13 December 2022
1st Revision on 22 December 2022
2nd Revision on 25 December 2022
3rd Revision on 5 January 2023
Accepted on 9 December 2023

Abstract
Purpose: Data protection of Personal rights needs to be a priority in upholding human rights and the need for strong institutions to protect them. Personal data protection in Indonesia needs to renew the authority of institutions or by creating new institutions.
Research Methodology: the research was carried out using descriptive and normative qualitative research methods with library sources.
Results: the results which laws and state institutions overseeing the protection of privacy data in Indonesia need to be improved through the renewal of the legal basis and the renewal of the authority of certain institutions or can also refer to the formation of new institutions related to the security of public personal data to prevent bureaucratic pathologies related to personal data and prevent cyber-crime regarding personal data.
Limitations: E-Government and the laws of Personal data privacy
Contribution: This study discusses the legal basis for the importance of personal data protection and the importance of reforming central and regional institutions that are authorized to carry out personal data protection for the Indonesian people.
Keywords: *E-government, State Institutions, Public Service, Local Government*
How to Cite: Zulfiani, Y. N. (2021). Prevention of personal data privacy leakage in e-government, as the government's responsibility. *Annals of Justice and Humanity*, 1(1), 29-37.

1. Introduction

E-Government is a renewable way to develop public services in Indonesia so incumbents must be selective in choosing what methods to use to achieve well-implemented E-Government because this involves the existing system, then in what ways. And which one is considered the best to use in achieving E-Government, then regarding when the law related to E-Government needs to be changed or get an update, Considering legal politics is an effort to realize good regulations following the circumstances and situations at a time, is it a law that has been formed but has not overcome E-Government problems such as bureaucratic pathology, data security, inadequate infrastructure, errors or disturbances, E-Government systems that need renewal and need further development or just a few things that need to be updated following the movement of E-Government legal politics (no need for major/massive renewal) especially media, programs, channels, and even E-Government applications always changes every year. This is reinforced by the Harvard JFK School of Government statement, which has suggested that three elements of successful e-Government implementation must be owned and considered very seriously, namely: Support, Capacity, and Value (Indrajit, 2004). Renewal along with the times to eliminate pathologies in the government bureaucracy and provide the best in public services, lest the legal basis of E-Government cannot overcome the problems that arise in the implementation of E-Government because according to the Public Service Act if the Government cannot improve infrastructure related to public services immediately, the Government is considered negligent.

E-government affects all aspects of society, especially in public services. Still, the E-government in Indonesia has not been equipped with adequate regulations or institutions to protect people's data

contained in E-government itself, so this is very vulnerable to leakage of personal data and cybercrime. Personal Data Protection is part of Human Rights and is the spearhead of the development of revolution 4.0 (Muni, 2020). Bearing in mind the cases of Personal Data Leakage in the implementation of E-government, such as in the Digital Public Services in Bekasi and Bogor City, the protection of personal data needs to be a priority in upholding human rights and the need for strong institutions to oversee this because, through legal protection carried out by state institutions, a state can make a draft and plan for the development of a national law that is effective and following Pancasila and the 1945 Constitution, so that these 2 things become interrelated and result in cause and effect. As Riwukore et al. (2021) state, the Indonesian Central Bureau of Statistics needs to re-arrange the data security regulation. The protection of personal data in Indonesia needs to be examined by renewing the authority of certain institutions or creating new institutions so that they can trigger government policies regarding which points will be maintained, which will be replaced, which laws will be revised, and which E-government laws will be eliminated according to the needs of the industrial revolution 4.0 era. This research discusses the legal basis for the importance of protecting personal data and the importance of reforming institutions that are authorized to carry out personal data protection for Indonesian people, which oversees the protection of privacy data in Indonesia needs to be repaired and enhanced through updating the legal basis and renewing the authority of certain institutions, or it can also refer to the establishment of a new institution related to the security of people's data to prevent bureaucratic pathology related to personal data and prevent cyber-crime related to personal data.

There is a need to review legal politics related to the protection of personal data, both regulations, how state institutions, both central and regional institutions, to implement these regulations and where the protection of personal data will go in Indonesia, especially in the unification of national and multidisciplinary regulations, and there is no mechanism or system that can detect pathology, starting at this time, it is necessary to make changes to the legal values above in order to protect the rights of citizens, if this is allowed to go unpunished then the Government is considered negligent in providing protection of personal data and does not pay attention to general principles of governance (AUPB), besides that by improving the legal basis for personal data protection which is adapted to the needs of the times, it is hoped that this will trigger improvements in personal data protection facilities and infrastructure so that cyber problems can be prevented and the quality of public services can be improved so that in accordance with Pancasila, the 1945 Constitution and technological advances in the industrial revolution 4.0 and even 5.0 in the future.

2. Literature Review

In terms of legal politics, personal data protection is something that needs to be regulated by the Indonesian State, which is facing the Industrial Revolution 4.0. Padmo Wahjono has an argument which states that:
“Legal politics is a basic policy that determines the direction, form, and content of the law to be formed” (Norris, 2017).

While Satjipto Rahardjo (1991) defines legal politics are:
The activity of choosing and the method to be used to achieve a social goal with certain laws in a society whose scope includes answers to several basic questions, including what goals are to be achieved through the existing system, what methods and which ones are considered the best to be used in achieving these goals, at what time and through how the law needs to be changed, can a standard and established pattern be formulated to assist in deciding the process of selecting goals and ways to achieve these goals properly”(Indrajit, 2004).

On the other hand, Soedarto reiterated that:
“Legal politics is an effort to realize good regulations according to the circumstances and situations at a time” (Soedarto, 1986).

So that according to the understanding of the legal experts above, legal politics is very influential in all aspects of society, especially in the 4.0 revolution era, where data exchange between the world is very easily carried out by various parties and is very prone to cyber actions that harm the security of personal data, a lot of parties - parties who will interact with each other and the community, at all times and this does not only revolve around everything related to diplomacy but is more in-depth, and this is carried out to facilitate and facilitate cooperation between people in the world and cooperation between state entities such as society, industry, and companies, So that in terms of carrying out significant tasks and collaborating on all trade administrations, political systems, social and cultural interaction mechanisms, as well as other pressing issues, This only seeks to enhance the productivity and welfare of the entire Indonesian population. The direction of legal politics related to this needs to be tightened because the existing regulations have not been able to overcome bureaucratic pathologies, personal data leakage, and misuse of personal data, which even existing Indonesian laws have not been able to overcome. In this case, the direction of legal politics needs massive reform because it involves the benefit of living together, which Global Human Rights guarantee, not only by one country; then to implement these regulations, it is necessary to expand the authority of state institutions both central and regional to carry out Personal protection data in the E-Government of this authority can also refer to the task force in the local Government to ensure that the local government E-Government is carried out following the law and protects the personal data of the people contained therein.

Based on the statement above, it is necessary to know more about Privacy; Samuel Warren and Louis Brandeis wrote “The Right to Privacy” which stated that:
“The legal conception of the right to privacy refers to the 'right to be let alone' with two main principles related to personal honor and values such as individual dignity, autonomy, and personal independence” (Bloustein, 1964).

Furthermore, Arthur Miller stated:
“Protection of personal data rests on the decision of an individual to exercise any control over the dissemination of information regarding himself” (Kitchin, 2014).
Julie Innes strengthens Arthur Miller's statement, which suggests that:
“Personal data protection gives full control over the realm of private decisions to itself then this includes 3 important actions on private access, private information and private action” (Kalyvas & Overly, 2014).

So, according to the author, it is necessary to protect the right to Privacy, especially on ethical and moral grounds. Still, the protection of personal data has not been regulated in an independent law, only contained in several articles or other regulations under the law, so the government Government still regulates the legal politics “half-measures” or considered “one-sided” with the bill on personal data protection not being ratified yet, even though if you look deeper, there is a lot of misuse of personal data that is not following positive Indonesian law, so it is better in terms of personal data protection it is necessary looking at the arrangements that have been made by every other country and matched with the sociological conditions of the Indonesian people, here are examples of points in the regulation of personal data based on the OECD, APEC and GDPR:

OECD (2013)	APEC (2015)	GDPR (2016)
1. Collection limitation 2. Data quality 3. Purpose specification 4. Use limitation 5. Security safeguards 6. Openness 7. Individual participation 8. Accountability	1. Preventing harm 2. Notice 3. Collection limitation 4. Uses of personal information 5. Choice 6. Integrity of personal information 7. Security safeguards 8. Access and correction 9. Accountability	1. Lawfulness, fairness and transparency 2. Purpose limitation 3. Data minimization 4. Accuracy 5. Storage limitation 6. Integrity and confidentiality 7. Accountability

Figure 1. Examples of points in the regulation of personal data based on the OECD, APEC and GDPR

Protection of personal data, when studied further, of course, needs to be firmly guided by real practices for a human right guaranteed by the State, comprehensive protection, and rules binding on various parties to protect information and personal data. Then guarantee that the data or information remains under control to enable each owner of the data to be safe, to be able to share some information or not, to know exactly who has access, at what time and for whatever reason, then the owner of the personal data can update information more easily.

On the other hand, the EU GDPR states that:
"In any information relating to personal data ('data subject') that can identify or can be identified; identify directly or indirectly by that person, especially by referring to an identification data such as name, identity number, location data, online identification data or related to any important data regarding physical identity, psychological, genetic, mental, economic, or social status of the owner of the data"(Ross, 2016; Schwab, 2017).

Meanwhile, positive Indonesian law discusses that General Personal Data consists of:
a) Name
b) Address
c) Email address
d) Location data
e) IP addresses
f) web cookies

So far, the rules regarding personal data are bound in the Indonesian Constitution, especially in Chapter XA—Article 28 A-J; more complete rules relating to each protection of personal data are contained in the 1945 Constitution in Article 28G paragraph (1), which reads:
"Every person has the right to protection for personal, family, honor, dignity and property under his control, and has the right to feel safe and protected from threats of fear to do or not do something that is a human right" (Pradana, 2022; Supriyono et al., 2022).

Indonesia has internationally ratified several international agreements, namely the International Covenant on Civil and Political Rights (ICCPR), which was ratified through Law Number 12 of 2005, which prioritizes the authority of the State to protect every privacy right of its citizens without exception, so that matters This remains in line with Law Number 39 of 1999 concerning Human Rights which explicitly guarantees the right to privacy data to be safeguarded by the State, this is contained in Article 14 (2), Article 29 (1) and Article 31.

Article 29, paragraph (1) expresses the acknowledgment of every personal data protection as follows:
a) Personal self
b) Family
c) Honour
d) Dignity
e) His property.

Then it is reaffirmed in Article 14 paragraph (2), which reads
"One of the rights to self-development is the right to seek, obtain, store, process, and convey information using all available means."
This is in line with Article 32 of the Human Rights Act
"Independence and secrecy in correspondence relations, including communication relations by electronic means, must not be disturbed, except on the order of a judge or other lawful authorities following the provisions of the legislation."

From a legal and political point of view, the DPR has prepared a Personal Data Protection Bill that takes into account the international values of the EU GDPR. In this case, it contains 15 chapters and 74 articles consisting of:
a) General Provisions,
b) Type of Personal Data,
c) Rights of Personal Data Owners,
d) Processing of Personal Data,
e) Obligations of Personal Data Controllers and Processors in the Processing of Personal Data,
f) Transfer of Personal Data,
g) Prohibition on the Use of Personal Data,
h) Formation of Personal Data Controller Code of Conduct,
i) Exceptions to Personal Data Protection,
j) Dispute Resolution,
k) International Cooperation,
l) Community Role,
m) Criminal Provisions,
n) Transitional Provisions,
o) Closing Provisions

3. Research Methodology

In research related to the Prevention Of Personal Data Privacy Leakage In E-Government As The Government Responsibility, the type of research that the author uses is normative legal research, namely legal research carried out by conducting a literature study with various library sources such as laws and regulations, laws, other supporting literature and institutional surveys (Efendi & Ibrahim, 2016). The study was conducted using qualitative methods to analyze and identify difficulties concerning the subject available (Chirozva & Damba, 2021; Rahman-Khan & Sultana, 2021). This study was analyzed qualitatively descriptively of when policies related to E-Government need to be changed or updated and what values need to be rebuilt, considering that E-Government is a basic policy that is highly favored in public services so that the protection of personal data contained in E-Government needs to be protected to prevent cyber-crime, besides that the protection of personal data in E-Government needs to follow positive Indonesian law and be adapted to the circumstances and situations at the time of the industrial revolution 4.0.

4. Results and discussion

There is a need for limitations and mechanisms in the implementation of the Law on Personal Data Protection and it is necessary to consider what kind of institution that functions as a regulator, supervisor and controller (independent regulatory), or a commission (a task force can also be formed) tasked with implementing the implementation of data protection in more depth whether the authority is still given to the Government according to the boundaries of their respective sectors then coordinates to the Minister of Communication and Informatics or gives authority to each Regional Government that has E-Government then returns to refer to the technicalities of how to enforce the protection of personal data whether it remains through complaints, deliberation, and courts as Permenkominfo Number 20 of 2016 concerning Protection of Personal Data in Electronic Systems or there are new technicalities that are fully authorized to institutions/task forces in Regional Governments which have their own E-Government. Regarding the authority of the Regional Government in implementing the protection of personal data contained in E-Government, the legal politics is still unclear and will overlap if it is not regulated more fully. A special task force that handles the protection of personal data in E-Government is a vital part that carries out the implementation of the protection of people's data in more depth.

Leakage of personal data in the implementation of E-government in the Digital Public Services in Bekasi and Bogor Cities

The Government's carelessness and negligence in protecting personal data are embodied in the case of hacking the servers of several civil registration offices such as Bogor and Bekasi so that data sets containing millions of personal information are sold from the servers, and then the personal information

is purchased by marketing companies that specialize in campaigns so that certain times intentionally purchase the data before the election to reach the public via text messages on behalf of the candidate. There were 47 cases of E-Government data theft in 2017, then increased to 88 cases in 2018 and then to 143 cases in 2019 (Djafar, 2019).

Of course, this has violated Arthur Miller's conception of personal data, which states that:
The protection of personal data rests on an individual's decision to exercise any control over the dissemination of information concerning himself or herself (Kitchin, 2014).
And Julie Innes stated:
"Protection of personal data gives complete control over the realm of private decisions to himself then this includes 3 important actions on private access, private information and private actions" (Kalyvas & Overly, 2014).

The analysis, according to the author's opinion, is guaranteed in Law Number 14 of 2008 concerning Public Information Openness so that every protection of public data and information should be collected by public bodies as stipulated in Article 6 paragraph (3) letter (c) of the Law on Public Information Disclosure, so that does not provide public information relating to personal data. In its implementation, personal data protection rules related to the administration of electronic systems, including communication and informatics, were then formulated in PP Number 82 of 2012 and Permenkominfo Number 20 of 2016 concerning Protection of Personal Data in Electronic Systems, Permenkominfo Number 21 of 2017 concerning Registration Telecommunications Service Customers. Personal data protection (Manan & Harjianti, 2016), according to the PDPSE Minister of Communication and Informatics, includes protection contained in:
a) acquisition and collection;
b) processing and analysis;
c) storage;
d) appearance,
e) announcement,
f) delivery,
g) dissemination,
h) and access opening;
i) and destruction of personal data.

Personal data protection guaranteed in the Minister of Communication and Information Number 20 of 2016 concerning the Protection of Personal Data in Electronic Systems includes (Palguna, 2013):
a) All aspects and stages of personal data processing,
b) Rights of the owner of personal data (rights of subject data),
c) Obligations of users of personal data,
d) Obligations of the electronic system operator in all stages of processing
e) If a dispute occurs in the management of personal data or there is a failure in protecting the confidentiality of personal data, the Minister of Communication and Information provides a forum for complaints to the minister (Kominfo) so that a settlement of the problem is carried out by deliberation or other alternative dispute resolution, if there is no common ground then it is advisable to file a lawsuit civil law in court.
f) Electronic system operators' deadline (transition) is two years.

Indonesia's positive law certainly recognizes personal data as individual data that must be stored, cared for and guarded for truth and confidentiality protected by the State so that the leakage of personal data is a form of negligence by the central Government and local Government where the Indonesian people are greatly disadvantaged in this case, if the politics of protection law personal data in Indonesia is still gray, so the enforcement of human rights related to the protection of personal data is still difficult to implement "honestly" even in a gamling manner the State prioritizes complaints to the minister (Kominfo), so that problem resolution is carried out by deliberation or other alternative dispute

resolution channels courts that are more certain so that in order to reduce the accumulation of complaints to Kominfo, it is time to implement personal data protection, expand the authority of state institutions as well as task forces from central and regional state institutions to carry out protection of personal data contained in E-Government.

Leakage of data by government servers is a form of poor implementation of Law Number 24 of 2013 concerning Population Administration in Article 85, which reads:
"The state must store and provides protection for the personal data of these residents." (Law Number 24 of 2013 Concerning Population Administration, 2013)
Then Article 79 reads:
"Obligates the state to provide protection and appoints the minister as the person in charge of access rights to citizens' data."

The leaked personal data of residents included (Djafar, 2019):
a) Family Card Number (KK)
b) National Identity Number (NIK)
c) Date, month, or year of birth
d) Information about physical and mental disabilities
e) biological mother's NIK
f) father's NIK
g) Information about physical and mental disabilities
h) Fingerprints
i) iris of the eye
j) Signature

In the author's opinion, all of the data is politically legal and has been regulated by law so that it does not leak and needs protection from the Government through positive legal arrangements (Laws and State Institutions as implementers at both the central and regional levels, if any can also be opened to the public). Because of a very important urgency, it still does not disclose personal data so that the Indonesian Government can carry out enforcement in the perspective of human rights; its implementation needs to expand the authority of state institutions and task forces from central and regional state institutions to carry out the protection of personal data that contained in E-Government to support the Government in building and implementing various portfolios of information technology with the main aim of improving two-way interactions with the public that protect their data, especially in the G2C-type E-government application to bring users closer. The government with its people through programs, applications and certain channels that are interesting and diverse so that people can easily reach their Government in order to fulfill various service needs Which are needed continuously is the most common E-government application applied in Indonesia, especially in the context of conveying aspirations, licensing and other public services, but in this case, there needs to be an update in order to protect users' personal data, in the previous regulation there was not much discussion regarding this, only briefly that the Government will protect the public's personal data, but data leaks often occur until the use of data by irresponsible parties, legal politics related to E-government to Citizens (G2C) needs updating in order to protect personal data in digitization, Particularly websites, applications, channels, and programs need more information about this pathology that affects server security. Moreover, and this is really serious, there are still a lot of instances of personal data leakage in Indonesia. , even the President's data was leaked to the virtual world, namely in the case of the Presidential vaccine certificate which was leaked on the Internet, even though this is crucial because it contains a Population Identification Number, this shows the direction of legal politics related to E-government so far has not yet deeply protected people's personal data, so updates must be carried out massively, all E-government needs to implement this because people's personal data such as identification number, date of birth, home address and even data Families who enter government applications, websites, channels and programs are the Government's responsibility to protect them from misuse so as to reduce other cyber cases in the future, by updating the political direction of Indonesia's e-government law, it is hoped that this will increase data security—but also expected to be able to improve E-Government infrastructure to improve application systems, websites, channels, to

government media which previously had not operated properly (reducing bureaucratic pathology in the form of program errors). Furthermore, regarding E-government to Citizens (G2C), it is necessary to further regulate how to implement the follow-up of the aspirations conveyed by the community in government applications, media, or websites. Finally, choose the path of demonstrations or demonstrations to the Government, both the central Government and local governments.

5. Conclusion

5.1. Conclusion

E-government affects all aspects of society, especially in the Protection of Personal Data which is part of Human Rights which is the spearhead of the development of the 4.0 revolution, considering Indonesia's positive law regarding personal data contained in the 1945 Constitution, Law Number 24 2013 concerning Population Administration, Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning ITE, Law Number 36 of 1999 concerning Telecommunications and several Perkominfo have not been able to resolve the case of Sales of Personal Data in the case of Leakage of Personal Data in the implementation of E-government in the Case of Digital Public Services for the City of Bekasi and Bogor, the legal politics of protecting personal data needs to be a priority in upholding human rights because through legal politics a country can make a design and the plan for the development of a national law that is effective and in accordance with Pancasila and the 1945 Constitution, Due to different laws in regulations and the scope of specific situations, Indonesian legal politics have not taken this seriously, and the delay in the Personal Data Protection Bill's passing has led to a perception that theft of personal data is not a major issue, not nationally and multidisciplinary so that it has an impact on the enforcement of human rights related to the protection of personal data that is not good, despite the fact that in today's digital age, when cyber issues are common, human rights related to the protection of personal data are things that are definitely needed.

5.2. Limitation

The limitation of the problem in this study only focuses on the importance of personal data protection in Indonesian e-government both at the central and local levels, and then there is a gap between the situation in society and the expected State or commonly called das sein and das solln that e-government in Indonesia has not been able to prevent leakage. Personal data with 2 cases of leakage of e-government in local governments so that there is a need for a stronger and clearer legal umbrella and requires a special agency or task force to handle personal data protection (expansion of authority or new task force).

5.3. Suggestion

The Government need to review the legal politics related to the protection of personal data, both regulations, how state institutions, both central and regional institutions, in implementing these regulations, either through the expansion of the authority of the Communication and Information Technology or the establishment of a new task force in E-Government belonging to the Regional Government that specifically handles and protects Personal data entered in the E-Government, will then be taken to where the protection of personal data in Indonesia, especially in the unification of national and multidisciplinary regulations, and the absence of a mechanism or system that can detect pathology, starting at this time it is necessary to change the value The above legal values are in order to protect the rights of citizens, if this is left unchecked then the Government is considered negligent in providing personal data protection and does not pay attention to the general principles of good governance (AUPB), in addition to improving the legal basis for personal data protection If it is adapted to the needs of the times, it is hoped that it will be a trigger for improving personal data protection facilities and infrastructure so that they can prevent cyber problems and improve the quality of public services to be in accordance with Pancasila, the 1945 Constitution and technological advances in the industrial revolution 4.0 and even 5.0 in the future.

Acknowledgment

Thank you, Allah *subḥānahu wataʿālā*, family, and all the University parties who have helped me complete this research. I hope this research can benefit the wider community and bring good changes in e-government.

References

Bloustein, E. J. (1964). *Privacy as an Aspect of Human Dignity : An Answer to Dean Prosser Philosophical Dimensions of Privacy: An Anthology*. Cambridge University Press.

Chirozva, L., & Damba, R. (2021). The law of treaties in Africa: Exploring the Southern African development community mutual defence pact. *Annals of Justice and Humanity*, 1(1), 11–20. https://doi.org/10.35912/ajh.v1i1.781

Djafar, W. (2019). *Hukum Perlindungan Data Pribadi di Indonesia: Lanskap, Urgensi dan Kebutuhan Pembaruan*. https://law.ugm.ac.id/wp-content/uploads/sites/1043/2019/08/Hukum-Perlindungan-Data-Pribadi-di-Indonesia-Wahyudi-Djafar.pdf

Efendi, J., & Ibrahim, J. (2016). *Metode Penelitian Hukum: Normatif dan Emppiris*. Prenadamedia Group.

Indrajit, R. E. (2004). *Electronic Government : Strategi Pembangunan dan Pengembangan Sistem Pelayanan Publik berbasis Teknologi Digital*. Penerbit Andi.

Kalyvas, J. R., & Overly, M. R. (2014). *Big Data: A Business and Legal Guide* (1st Editio). Auerbach Publications. https://doi.org/10.1201/b17406

Kitchin, R. (2014). Big Data, new epistemologies and paradigm shifts. *Big Data & Society*, 1(1), 1–12. https://doi.org/10.1177/2053951714528481

Manan, B., & Harjianti, S. D. (2016). Konstitusi dan Hak Asasi Manusia. *Jurnal Ilmu Hukum Universitas Padjajaran*, 3(3).

Muni, A. (2020). Hak Asasi Manusia dalam Konstitusi Indonesia. *Al'adalah*, 23(1), 65–78. https://doi.org/10.35719/aladalah.v23i1.27

Norris, D. F. (2017). *Current Issues and Trends in Research*. Cybertech Publishing.

Palguna, I. D. G. (2013). *Pengaduan Konstitusional (Constitutional Complaint)*. Sinar Grafika.

Pradana, Y. (2022). Implementasi Prinsip "Kepentingan Terbaik bagi Anak" dalam proses persidangan Anak secara elektronik pada masa pandemi di Kota Jakarta Barat. *Jurnal Ilmiah Hukum dan Hak Asasi Manusia*, 1(2), 43–53. https://doi.org/10.35912/jihham.v1i2.1022

Rahardjo, S. (1991). *Ilmu hukum*. Citra Aditya Bakti.

Rahman-Khan, M. M. R., & Sultana, R. (2021). Shift in the role of criminology in criminal law: Reflecting the doctrinal change. *Annals of Justice and Humanity*, 1(1), 1–10. https://doi.org/10.35912/ajh.v1i1.708

Riwukore, J. R., Marnisah, L., Habaora, F. H. F., & Yustini, T. (2021). Implementation of One Indonesian Data by the Central Statistics Agency of East Nusa Tenggara Province. *Jurnal Studi Ilmu Sosial dan Politik*, 1(2), 117–128. https://doi.org/10.35912/jasispol.v1i2.1194

Ross, A. (2016). *The Industries of the Future*. Simon & Schuster.

Schwab, K. (2017). *The Fourth Industrial Revolution*. Penguin Books Limited.

Soedarto. (1986). *Hukum Dan Hukum Pidana*. Alumni.

Supriyono, S., Sholichah, V., & Irawan, A. D. (2022). Urgensi Pemenuhan Hak-Hak Konstitusional Warga Negara Era Pandemi Covid-19 di Indonesia. *Jurnal Ilmiah Hukum dan Hak Asasi Manusia*, 1(2), 55–66. https://doi.org/10.35912/jihham.v1i2.909