Journal of Cyber Law and Information Security
Volume 1, Number 2, 2022

Electronic System Operator Liability under Indonesia's GR 71/2019: A Comparison with Singapore's Cybersecurity Framework

Sufi Sundari[1*]

[1] Universitas Bhayangkara Jakarta Raya, Bekasi, Indonesia

Abstract

Article history:
Received: August 20, 2022
Revised: September 08, 2022
Accepted: October 29, 2022
Published: December 30, 2022

Keywords:
Cybersecurity, Electronic System Operators, Indonesia, Liability, Singapore.

Identifier:
Zera Open
Page: 136-156
https://zeraopen.com/journal/jclis

This article examines the effectiveness of Government Regulation No. 71 of 2019 in regulating the liability of Electronic System Operators in Indonesia, using Singapore's cybersecurity framework as a comparative benchmark. The discussion is situated within increasing cybersecurity risks, data breach incidents, and the growing dependence of public and private services on electronic systems. This study contributes to Indonesian cyber law scholarship by positioning Indonesia as the main object of analysis while using Singapore's Cybersecurity Act 2018 to identify lessons for regulatory improvement. Using a normative juridical approach and comparative legal method, the article analyzes statutory provisions, scholarly literature, and selected cyber incident reports. The findings show that GR 71/2019 provides an important foundation for operator responsibility by recognizing obligations related to system reliability, security, and accountability. However, compared with Singapore's framework, Indonesia's regulation remains limited in operationalizing liability through incident reporting, audits, risk assessments, supervisory coordination, and remedies. The article concludes that Indonesia needs a more precise, risk-based, and enforceable liability framework to strengthen cybersecurity governance and public trust

*Corresponding author:
(Sufi Sundari)

1. Introduction

The growth of digital services has made electronic system operators central actors in the governance of data, transactions, and cybersecurity. In Indonesia, electronic system operators do not merely provide technical infrastructure but also mediate access to personal data, financial transactions, communication services, public administration, and digital commerce. This position creates a legal expectation that operators must ensure the reliability, security, and accountability of the electronic systems they manage. Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions, commonly referred to as GR 71/2019, strengthens this expectation by regulating public and private electronic system operators, electronic system registration, system reliability, data governance, and responsibility for losses caused by electronic systems. However, the increasing frequency of data breaches and cyber incidents raises an important question about whether the regulation provides a sufficiently effective liability framework for operators in practice.

The issue became more visible after major cyber incidents involving Indonesian digital platforms and public-sector data. The Tokopedia breach, for instance, reportedly involved claims that millions of user records had been leaked, showing how private digital platforms may become high-risk sites for consumer data exposure (Potkin, 2020). A similar concern emerged in the alleged BPJS Kesehatan data leak, where the Ministry of Communication and Informatics summoned the state health insurer after samples of personal data were allegedly offered online (Reuters, 2021). These incidents illustrate that the legal problem is not limited to

unauthorized access itself, but also concerns post-incident responsibility, notification, supervision, sanctions, and remedies for affected users. Rosadi (2018) argues that Indonesia's personal data protection framework has long been fragmented across different laws and sectoral regulations, while Sinaga and Putri (2020) emphasize that legal reform is needed to respond to the risks of digital transformation and the increasing economic value of personal data.

GR 71/2019 provides an important regulatory basis because it places obligations on electronic system operators to operate systems in a reliable, secure, and responsible manner. It also recognizes the distinction between public-sector and private-sector operators, which is relevant because cyber risks now affect both government-managed systems and commercial digital platforms. Nevertheless, the effectiveness of this framework depends on whether legal obligations are sufficiently clear, enforceable, and supported by institutional supervision. Lesmana et al. (2021) note that personal data protection is closely connected to the constitutional right to privacy, meaning that weak enforcement may affect not only consumers but also citizens' fundamental rights. Similarly, Putri and Martha (2021) highlight the importance of legal responsibility in data leakage cases, particularly because victims often face difficulty proving harm and obtaining remedies.

A comparison with Singapore is useful because Singapore provides a benchmark for evaluating Indonesia's regulatory design rather than serving as an equal object of study. Singapore has developed a more specific cybersecurity governance model through the Cybersecurity Act 2018, which focuses on the protection of critical information infrastructure, regulatory oversight, incident

response, and obligations imposed on owners of essential systems. Gorian (2019) describes Singapore's framework as a calibrated model that combines state authority, private-sector cooperation, and legally defined duties for critical infrastructure protection. The significance of this model became evident after the SingHealth cyberattack, in which personal data of around 1.5 million patients was stolen, including information linked to Singapore's prime minister (Kim & Aravindan, 2018). Although Singapore's framework is not identical to Indonesia's, it offers a relevant comparison because both countries face the same regulatory challenge: how to transform cybersecurity responsibility from a general obligation into a concrete and enforceable legal duty.

Accordingly, the research gap addressed in this article lies in the limited examination of Electronic System Operator liability under Indonesia's GR 71/2019 through a structured comparative benchmark. Existing studies on Indonesian cyber law often discuss personal data protection, privacy, or electronic transactions more broadly, while fewer studies place operator liability at the center of analysis. This article therefore positions Indonesia as the main object of study and uses Singapore's cybersecurity framework as a benchmark to evaluate whether Indonesia's liability framework has sufficiently defined operator obligations, incident-response duties, supervisory mechanisms, sanctions, and remedies for affected users. Based on this gap, the first research question is: How effective is Government Regulation No. 71 of 2019 in regulating the liability of Electronic System Operators in Indonesia when evaluated against Singapore's cybersecurity framework? The second research question is: Why is evaluating Indonesia's Electronic System Operator liability

framework necessary in response to increasing cybersecurity risks and comparative lessons from Singapore?

2. Research Methods

This study employs a normative juridical approach using a comparative legal method to examine the liability framework of Electronic System Operators under Indonesia's Government Regulation No. 71 of 2019. The normative approach is used because the main object of analysis is legal norms, particularly the provisions governing operator obligations, system reliability, cybersecurity responsibility, user protection, administrative supervision, and sanctions. Through this approach, the article evaluates whether GR 71/2019 provides a sufficient legal basis for holding Electronic System Operators accountable when electronic systems fail to protect users, personal data, or public trust in digital services.

The comparative element is used to position Singapore's cybersecurity framework as a benchmark for evaluating Indonesia's regulatory design. Singapore is not treated as an equal object of study, but as a comparator that helps identify possible strengths, weaknesses, and improvement points in Indonesia's framework. The comparison focuses mainly on Singapore's Cybersecurity Act 2018 and its approach to critical information infrastructure protection, incident-response obligations, regulatory supervision, and duties imposed on relevant system owners. This comparison is relevant because both Indonesia and Singapore face similar cybersecurity risks, while Singapore has developed a more specific legal structure for cybersecurity governance.

The legal materials used in this article consist of primary, secondary, and supporting materials. Primary legal materials include Government Regulation No. 71 of 2019, the Indonesian Electronic Information and Transactions Law and its amendments, and Singapore's Cybersecurity Act 2018. Secondary legal materials include peer-reviewed journal articles, scholarly books, and indexed legal studies discussing cyber law, personal data protection, electronic system governance, cybersecurity regulation, and liability. Supporting materials include reports and reputable news sources used only to illustrate relevant cyber incidents, such as data breach cases involving digital platforms or public-sector systems.

The analysis is conducted through statutory, conceptual, and comparative approaches. The statutory approach is used to interpret the obligations and liability provisions imposed on Electronic System Operators under Indonesian law. The conceptual approach is used to clarify the meaning of liability, accountability, cybersecurity responsibility, and user protection in electronic systems. The comparative approach is then applied to evaluate whether Indonesia's framework has sufficiently defined operator obligations, incident-response duties, supervisory mechanisms, sanctions, and remedies when assessed against Singapore's cybersecurity framework. Through this method, the article aims to formulate a legal assessment of the effectiveness and necessity of strengthening Indonesia's Electronic System Operator liability framework.

3. Results and Discussion

3.1. How effective is Government Regulation No. 71 of 2019 in regulating the liability of Electronic System Operators in Indonesia when evaluated against Singapore's cybersecurity framework?

Government Regulation No. 71 of 2019 provides an important foundation for regulating Electronic System Operator liability in Indonesia because it places electronic system governance within a framework of reliability, security, responsibility, and legal accountability. Under this regulation, Electronic System Operators are not understood merely as technical service providers. They are legal subjects that manage electronic systems used for public administration, private services, communication, transactions, data processing, and digital platforms. This broad regulatory scope is important because cybersecurity risks in Indonesia arise not only from private digital companies but also from public-sector systems that store and process large amounts of citizen data. In this respect, GR 71/2019 is effective as an entry point for establishing that operators have legal duties when they operate electronic systems.

The regulation is also significant because it recognizes the need to distinguish between public and private Electronic System Operators. This distinction matters because different operators may control different types of data, infrastructure, and public interests. Public-sector operators may process population, health, licensing, social security, or administrative data, while private-sector operators may process consumer, financial, communication, or platform-based transaction data. The Tokopedia breach illustrates the vulnerability of private digital platforms, as reports

suggested that large numbers of user records were exposed and offered online (Potkin, 2020). Meanwhile, the alleged BPJS Kesehatan data leak demonstrates that public or state-related electronic systems may also become sources of serious data-security concern (Reuters, 2021). These cases show that Electronic System Operator liability must apply across both sectors because the potential harm is not limited to ordinary contractual loss but may affect privacy, identity security, and public trust.

From a normative perspective, GR 71/2019 is effective in creating a general obligation for operators to maintain secure and reliable systems. It supports the principle that those who control electronic infrastructure must also bear responsibility for preventing system misuse, maintaining system integrity, and protecting users from avoidable harm. This position is consistent with Rosadi's (2018) argument that Indonesia's digital legal framework has gradually moved toward recognizing privacy and personal data protection as important legal concerns. Sinaga and Putri (2020) also emphasize that the rise of digital transformation requires stronger legal instruments because personal data has become economically valuable and vulnerable to misuse. Therefore, GR 71/2019 contributes to the broader development of Indonesian cyber law by placing operator responsibility within electronic-system governance.

However, the effectiveness of GR 71/2019 remains limited because many of its obligations are formulated in general terms. The regulation requires operators to ensure system reliability and security, but it does not always provide detailed and measurable standards for assessing whether an operator has fulfilled its duty of care. This creates difficulty when a cyber incident occurs. In data breach cases, the main

question is not only whether an operator had a general duty to protect the system, but whether the operator failed to meet specific security obligations before, during, and after the incident. Such obligations may include risk assessment, access-control management, encryption, audit trails, incident detection, breach notification, system recovery, cooperation with regulators, and remedies for affected users. If these duties are not clearly operationalized, liability may become difficult to enforce.

This limitation becomes clearer when Indonesia's framework is evaluated against Singapore's cybersecurity framework. Singapore's Cybersecurity Act 2018 provides a more specific model for imposing cybersecurity duties, especially on owners of Critical Information Infrastructure. The Act does not only state that operators should maintain secure systems. It also provides more concrete obligations related to incident reporting, compliance with codes of practice, cybersecurity audits, risk assessments, and participation in cybersecurity exercises. Gorian (2019) describes Singapore's Cybersecurity Act as a new-generation standard for critical information infrastructure protection because it links cybersecurity governance with legally defined duties and regulatory oversight. This structure shows a stronger movement from broad legal responsibility toward operational compliance duties.

Singapore's framework is useful as a benchmark because it shows how cybersecurity responsibility can be made more enforceable. In Singapore, the legal framework identifies high-risk infrastructure and imposes heightened duties on the owners of such systems. Simmons and Simmons (2018) note that Singapore's Cybersecurity Act establishes a regulatory framework for monitoring and protecting critical information infrastructure, while also giving cybersecurity authorities powers

to respond to threats and incidents. This model strengthens accountability because system owners know the specific duties expected from them, and regulators have clearer tools to assess compliance. By contrast, Indonesia's GR 71/2019 is broader in coverage but less detailed in specifying the practical standards that operators must meet.

This does not mean that Indonesia should directly copy Singapore's framework. Indonesia has a different legal structure, larger population, wider platform ecosystem, and more complex decentralization of public services. However, Singapore offers a useful comparison because it demonstrates how liability can be supported by preventive and procedural duties. In Indonesia, the weakness is not the total absence of regulation, but the gap between general legal obligations and concrete enforcement mechanisms. GR 71/2019 establishes that Electronic System Operators must be responsible, but the framework still needs stronger detail on how responsibility is measured, how breaches must be reported, how compliance is audited, and how affected users may obtain remedies.

The issue of remedies is particularly important. Putri and Martha (2021) argue that legal responsibility in data leakage cases is necessary because victims often face uncertainty in identifying the responsible party, proving harm, and seeking legal recovery. This problem is intensified by the technical nature of cybersecurity incidents. Operators usually control the evidence needed to determine whether adequate security measures were implemented. Users often do not have access to internal logs, audit reports, system architecture, or incident-response records. As a result, even when harm occurs, affected users may struggle to prove negligence or

obtain compensation. In this context, a liability framework must not only declare operator responsibility but also create procedural mechanisms that reduce the evidentiary burden on victims.

Institutional supervision is another area where GR 71/2019 needs strengthening. The regulation recognizes government oversight, but cybersecurity supervision in Indonesia may involve several institutions, including communication and informatics authorities, sectoral regulators, cybersecurity bodies, and law-enforcement agencies. This multi-institutional structure may create coordination problems if the distribution of authority is unclear. Doly (2021) argues that the protection of personal data requires a strong supervisory institution because enforcement depends not only on legal norms but also on the institutional capacity to monitor and sanction violations. Although Doly's discussion focuses on personal data protection, the argument is also relevant to Electronic System Operator liability because cybersecurity responsibility requires clear supervision and enforcement.

Therefore, GR 71/2019 can be considered partially effective. It is effective as a foundational regulation because it recognizes Electronic System Operators as responsible legal actors and imposes general duties regarding reliability, security, and accountability. It is also important because it applies to both public and private operators. However, compared with Singapore's cybersecurity framework, GR 71/2019 remains less effective in three main respects: the specificity of operator obligations, the clarity of incident-response duties, and the strength of supervisory and remedial mechanisms. The central gap is not whether Indonesia has a legal basis

for operator liability, but whether that legal basis is sufficiently detailed and enforceable in real cybersecurity incidents.

3.2. Why is evaluating Indonesia's Electronic System Operator liability framework necessary in response to increasing cybersecurity risks and comparative lessons from Singapore?

Evaluating Indonesia's Electronic System Operator liability framework is necessary because cybersecurity risks have become more frequent, complex, and socially significant. Digital systems now support economic activity, public administration, financial transactions, health services, education, and communication. As a result, a failure in electronic-system security can create consequences beyond individual inconvenience. It can affect public trust, institutional credibility, business continuity, consumer protection, and citizens' rights. In this setting, operator liability is not only a private-law concern. It is also part of the broader legal infrastructure needed to support a secure and trusted digital society.

The increasing scale of cyber incidents shows why general obligations are no longer sufficient. The Tokopedia and BPJS Kesehatan cases indicate that both private platforms and public-sector systems may become targets or sources of data exposure (Potkin, 2020; Reuters, 2021). These incidents show that cyber harm may involve millions of users and may include personal, financial, transactional, or health-related information. The legal response must therefore address prevention, mitigation, notification, investigation, sanctions, and remedies. If the law only provides broad responsibility without specific duties, affected users may not receive

adequate protection, and operators may not have strong incentives to maintain higher cybersecurity standards.

The nature of cyber harm also makes evaluation necessary. In many data breach cases, the harm is not always immediate or easily measurable. Users may suffer from increased risk of identity theft, fraud, phishing, reputational damage, profiling, or misuse of personal information. These harms may occur gradually and may be difficult to prove in court. Marune and Hartanto (2021) argue that strengthening personal data protection and cybersecurity in Indonesia requires a progressive legal perspective because digital risks cannot be addressed only through conventional legal categories. This argument supports the need to evaluate GR 71/2019 because operator liability must be adapted to the specific features of digital harm.

Another reason evaluation is necessary is the imbalance between operators and users. Electronic System Operators control the system infrastructure, security policies, internal documents, breach-detection mechanisms, and technical evidence. Users generally do not know whether an operator used adequate security measures or whether the breach resulted from negligence, weak governance, or unavoidable external attack. This evidentiary imbalance can make liability difficult to enforce. Therefore, Indonesia's framework should not rely solely on users proving fault after harm occurs. It should require operators, especially high-risk operators, to maintain records of compliance, conduct periodic risk assessments, and report incidents transparently to regulators and affected users.

Singapore's framework offers an important comparative lesson in this regard. Its Cybersecurity Act emphasizes preparedness and compliance, not only post-incident punishment. Duties such as cybersecurity audits, risk assessments, and incident reporting help create a documentary basis for evaluating whether system owners have acted responsibly. This is important because liability becomes more enforceable when legal duties generate records, standards, and procedures. Indonesia can learn from this model by strengthening the operational content of GR 71/2019 through technical standards, mandatory reporting duties, and clearer audit obligations for operators managing sensitive or high-risk systems.

Evaluation is also necessary because Indonesian cyber law has historically been fragmented. Before a more comprehensive personal data protection framework developed, personal data and cybersecurity issues were regulated through several instruments, including the ITE Law, GR 71/2019, ministerial regulations, and sector-specific rules. Rosadi (2018) explains that this fragmentation has long been one of the challenges in Indonesia's personal data protection framework. Darmanto and Zaini (2020), in their study of the implementation of Minister of Communication and Informatics Regulation No. 20 of 2016 in several civil registry offices, also show that the implementation of personal data protection obligations depends heavily on institutional readiness and administrative practice. This supports the argument that formal regulation alone is insufficient if implementation mechanisms remain weak.

The fragmentation problem is closely related to Electronic System Operator liability. Cyber incidents often involve multiple legal issues at once: electronic

transactions, consumer protection, personal data protection, public administration, criminal law, and sectoral regulation. If obligations are scattered across different rules without clear coordination, operators may face uncertainty, regulators may overlap, and victims may not know which mechanism to use. A clearer liability framework under GR 71/2019 would help define who is responsible, which authority supervises compliance, what steps must be taken after an incident, and what remedies are available to users.

The Singapore comparison also shows the importance of a risk-based approach. Singapore imposes specific obligations on owners of Critical Information Infrastructure because such systems are essential to national security, public welfare, and economic stability. Indonesia may not need to adopt the same categories exactly, but it can use the same logic. Operators that manage high-risk data or essential services should face stronger obligations than operators with limited risk. For example, electronic systems involving health data, financial data, population records, public services, or large-scale consumer platforms may require mandatory security audits, breach notification, risk assessments, and stronger sanctions for non-compliance. This would make Indonesia's framework more proportionate and more responsive to actual cybersecurity risks.

Such evaluation is also necessary to strengthen public trust in Indonesia's digital economy. Digital transformation depends not only on innovation and platform growth but also on legal assurance. Users are more likely to trust digital services when they know that operators are legally required to protect their data and can be held accountable when preventable failures occur. Sinaga and Putri (2020)

emphasize that personal data has growing economic value in the digital era, which increases the need for legal protection against misuse and exploitation. In this context, Electronic System Operator liability is not a narrow technical issue. It is part of the legal foundation for consumer confidence, digital governance, and rights protection.

The comparative lesson from Singapore is therefore not that Indonesia has no cybersecurity law, but that Indonesia needs stronger regulatory precision. GR 71/2019 already establishes an important foundation, yet its effectiveness depends on how far its broad obligations can be translated into measurable and enforceable duties. Indonesia can improve its framework by clarifying incident-response obligations, introducing stronger reporting duties, requiring audits and risk assessments for high-risk operators, strengthening coordination among supervisory institutions, and providing clearer remedies for affected users. These improvements would not change the basic orientation of GR 71/2019, but would make it more practical and enforceable.

Accordingly, evaluating Indonesia's Electronic System Operator liability framework is necessary because cybersecurity risks demand legal rules that are preventive, enforceable, and user-oriented. GR 71/2019 is important because it recognizes operator responsibility, but comparison with Singapore shows that Indonesia still needs more detailed obligations and stronger accountability mechanisms. Singapore's framework provides a useful benchmark because it demonstrates how cybersecurity duties can be operationalized through incident reporting, audits, risk assessments, regulatory supervision, and preparedness

obligations. For Indonesia, the main lesson is to strengthen its own framework so that operator liability does not remain a general principle, but becomes a clear legal mechanism for preventing harm, responding to incidents, and protecting affected users.

4. Conclusion

This article concludes that Government Regulation No. 71 of 2019 has provided an important legal foundation for regulating the liability of Electronic System Operators in Indonesia. The regulation is significant because it recognizes Electronic System Operators as legal actors that must ensure the reliability, security, and accountability of electronic systems. It also covers both public and private operators, which is essential because cybersecurity risks may arise from digital platforms, state-managed systems, public-service databases, and private-sector infrastructures. In this sense, GR 71/2019 is effective as a general normative framework because it establishes that operators cannot be treated merely as technical intermediaries. They carry legal responsibility when the electronic systems they manage affect users, personal data, transactions, and public trust.

However, the effectiveness of GR 71/2019 remains limited when evaluated against Singapore's cybersecurity framework. The main weakness is not the absence of regulation, but the lack of more specific and measurable obligations. GR 71/2019 already requires operators to maintain secure and reliable systems, yet it does not fully operationalize these obligations into clear standards on incident reporting, cybersecurity audits, risk assessments, breach notification, supervisory coordination,

and user remedies. Singapore's Cybersecurity Act 2018 provides a useful benchmark because it demonstrates how cybersecurity duties can be translated into concrete compliance mechanisms, especially for critical information infrastructure. The comparison shows that Indonesia's framework needs stronger regulatory precision, particularly for operators that manage high-risk data, essential public services, financial systems, health information, or large-scale consumer platforms. Therefore, Singapore is not used as a model to be copied entirely, but as a comparator that helps identify areas where Indonesia's Electronic System Operator liability framework can be strengthened.

Evaluating Indonesia's liability framework is necessary because cyber incidents increasingly produce complex legal harms that are difficult for users to prove and remedy. Data breaches may expose individuals to identity theft, fraud, privacy violations, reputational harm, and long-term misuse of personal information. Since operators control most technical evidence, users often face an unequal position in proving negligence or demanding compensation. For this reason, Indonesia should strengthen GR 71/2019 through clearer implementing rules, risk-based obligations, mandatory incident-response procedures, stronger supervisory authority, and accessible remedies for affected users. A more effective framework should clarify who is responsible, what duties must be fulfilled, how compliance is assessed, which sanctions apply, and how victims can obtain protection after cybersecurity failures. By strengthening these elements, Indonesia can transform Electronic System Operator liability from a broad legal principle into a practical

accountability mechanism that supports cybersecurity, protects rights, and reinforces trust in the national digital ecosystem.

References

Darmanto, N., & Zaini, N. (2020). Implementation of Regulation of the Minister of Kominfo Number 20 2016 in Disdukcapil Sleman, Temanggung, and Gianyar District. *Jurnal Penelitian Komunikasi dan Opini Publik, 24*(1), 85–97.

Doly, D. (2021). Pembentukan lembaga pengawas pelindungan data pribadi dalam perspektif pembentukan lembaga negara baru. *Negara Hukum, 12*(2), 223–244.

Gorian, E. (2019). Singapore's Cybersecurity Act 2018: A new generation standard for critical information infrastructure protection. In *Smart technologies and innovations in design for control of technological processes and objects: Economy and production: Proceedings of the International Science and Technology Conference "FarEastCon-2018"* (Vol. 1, pp. 1–9). Springer.

Kim, J. & Aravindan, A. (2018, July 20). Singapore's worst cyberattack steals personal data of 1.5 million, including PM. *Reuters.* Retrieved May 28, 2022 from https://www.reuters.com/article/world/uk/singapores-worst-cyberattack-steals-personal-data-of-15-million-including-pm-idUSKBN1KA14A/

Lesmana, C. S. A. T., Elis, E., & Hamimah, S. (2021). Urgensi Undang-Undang Perlindungan Data Pribadi dalam menjamin keamanan data pribadi sebagai pemenuhan hak atas privasi masyarakat Indonesia. *Jurnal Rechten: Riset Hukum dan Hak Asasi Manusia, 3*(2), 1–6.

Marune, A. E. M. S., & Hartanto, B. (2021). Strengthening personal data protection, cyber security, and improving public awareness in Indonesia: Progressive legal perspective. *International Journal of Business, Economics and Social Development, 2*(4), 143–152.

Potkin, F. (2020, May 2). Indonesia's Tokopedia probes alleged data leak of 91 million users. *Reuters*. Retrieved May 28, 2022 from https://www.reuters.com/article/technology/indonesias-tokopedia-probes-alleged-data-leak-of-91-million-users-idUSKBN22E0P9/

Putri, E. P., & Martha, A. E. (2021). The importance of enacting Indonesian data protection law as a legal responsibility for data leakage. *Varia Justicia, 17*(3), 287–303.

Republic of Indonesia. (2019). Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions.

Reuters. (2021, May 21). Indonesia summons state health insurer over alleged data leak. *Reuters*. Retrieved May 17, 2022 from https://www.reuters.com/technology/indonesia-summons-state-health-insurer-over-alleged-data-leak-2021-05-21/

Rosadi, S. D. (2018). Protecting privacy on personal data in digital economic era: Legal framework in Indonesia. *Brawijaya Law Journal, 5*(1), 143–157.

Simmons & Simmons. (2018, April 27). *The Singapore Cybersecurity Act 2018*. Retrieved May 15, 2022 from https://www.simmons-simmons.com/publications/ck0d8kb0hudys0b33hi2c9gys/270418-the-singapore-cybersecurity-act-2018

Sinaga, E. M. C., & Putri, M. C. (2020). Formulasi legislasi perlindungan data pribadi dalam Revolusi Industri 4.0. *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional, 9*(2), 237–256.

Singapore. (2018). *Cybersecurity Act 2018*. Singapore Statutes Online. Retrieved May 28, 2022 from https://sso.agc.gov.sg/Act/CA2018