The Concept of Cyber Insurance as a Loss Guarantee on Data Protection Hacking in Indonesia

Submitted: 18 July 2022
Reviewed: 3 November 2022
Revised: 2 December 2022
Accepted: 3 December 2022

Article submitted to blind peer review

Jufryanto Puluhulawa[*]
https://orcid.org/0000-0001-7090-9699
Mohamad Hidayat Muhtar[**]
https://orcid.org/0000-0002-1728-683X
Mellisa Towadi[***]
https://orcid.org/0000-0002-9237-5250
Vifi Swarianata[****]
https://orcid.org/0000-0003-2257-9677
Apripari[*****]
https://orcid.org/0000-0001-5508-2136

DOI: https://doi.org/10.26512/lstr.v15i2.44206

Abstract

[Purpose] This research departs from the legal vacuum regarding data protection insurance in Indonesia. In terms of regulation, Law Number 40 of 2014 concerning Insurance has not regulated all about cyber insurance, and Indonesia still needs to have a law that regulates data protection.

[Methodology/Approach/Design] This research is categorized into the normative legal research type based on the issues and themes raised as a research topic. The research approach used is the conceptual approach, philosophical approach, and analytical approach. The research focuses on analyzing the concept of cyber insurance in protecting data and a study of the urgency of regulating cyber insurance in Indonesia to minimize the impact of losses due to data hacking.

[Findings] The results show that the concept of cyber insurance in personal data protection began in the 80s and increased in the early 2000s due to digitization in all areas of people's lives. This significant development was not followed by Indonesia, with a legal vacuum regulating cyber insurance in data protection. Therefore, several things that

[*]Jufryanto Puluhulawa, Assistant Professor, Universitas Negeri Gorontalo. Law Science Department, Faculty of Law Universitas Negeri Gorontalo, Jend. Sudirman Street no. 6, Gorontalo City, 96128, Gorontalo, Indonesia. E-mail: jufryantopuluhulawa@ung.ac.id.
[**]Mohamad Hidayat Muhtar, Lecturer, Universitas Negeri Gorontalo. E-mail: hidayatmuhtar21@ung.ac.id.
[***]Mellisa Towadi, Assistant Professor, Universitas Negeri Gorontalo. E-mail: mellisatowadi@ung.ac.id.
[****]Vifi Swarianata, Lecturer, Universitas Negeri Gorontalo. E-mail: vifiswarianata@ung.ac.id.
[*****]Apripari, Lecturer, Universitas Negeri Gorontalo. E-mail: apripari@ung.ac.id.

Indonesia must do, namely Revision of the Law of the Republic of Indonesia Number 40 of 2014 concerning Insurance, Establishment of implementing regulations, need new normalization in overriding the Civil Code.
[Practical Implications] This study has legal implications for norming. In addition, it has implications for changes in the concept of insurance in Indonesia because, so far, cyber insurance services are still conventional.
[Originality/Value] On an Indonesian scale, this research is the first to comprehensively discuss cyber insurance for data protection.

Keywords: Cyber Insurance. Data Protection. Legal Void.

INTRODUCTION

Attention to data protection in Indonesia, in general, has been emphasized in the 1945 Constitution of the Republic of Indonesia ('UUD'). In particular, Article 28G paragraph 1 states that everyone has the right to personal protection, family, honor, dignity, and property under his control and has the right to a sense of security and protection from the threat of fear to do or not do something which is the proper human rights. In line with the constitution's substance, personal data is now like a valuable asset, which in M. Arsyad Sanusi's view, is like a commodity with high economic value SANUSI, 2004, so it must be maintained and appropriately managed in today's digitalization world.

In several international instruments, such as the OECD Guidelines and the Data Protection Convention from the Council of Europe, personal data is information about an identified or identifiable natural person. Another definition of personal data is data in the form of identity, code, symbol, letter, or a number of a person's marker that is private and confidential SAUTUNNIDA, 2018.

Society's dependence on information technology is increasing, so the risk is higher NAPITUPULU, 2017. The digital revolution has created an innovative capacity to acquire, store, manipulate and transmit volumes of data in real-time, vast and complex. Therefore, the digital revolution is often considered synonymous with the data revolution. These developments have encouraged the collection of various data, no longer dependent on considerations of what data might be helpful in the future.

However, almost all data is collected, the government and the private sector are competing to increase their data storage capacity, and data erasure is becoming less and less frequent. They discover new value in the data, treated like a tangible asset. This new era of data management is commonly referred to as Big Data. The interaction of digital society in using the internet depends on the availability, integrity, and confidentiality of information in cyberspace.

Although insurance companies have insured all types of disaster products and events for hundreds of years, cyber insurance, which covers corporate losses

and costs stemming from cyber-attacks, is a relatively new concept that Lloyd's of London (Lloyd's) insurance company started as one of. The first company to sell policies for cyber-attack-related incidents in 1999. Twenty years later, cyberattacks have become a daily occurrence, and one successful breach can cost an organization/company hundreds of thousands, even millions of dollars TALESH, 2018. This opens the horizon of thinking that most people think that digitalization, on the one hand, brings benefits to civilization, but on the other hand, digitalization brings new problems as well as challenges in this era of the Industrial Revolution 4.0 PULUHULAWA, PULUHULAWA e KATILI, 2020.

Cybercrime is one of the most critical business risks for companies worldwide in the 21st century. Cyber risk can be defined as 'any risk arising from using information and communication technology (ICT) that compromises the confidentiality, availability or integrity of data or services. Operational technology (TO) damage ultimately causes business disruption, infrastructure damage (critical), and physical property damage. Generally, breaches of obligations and confidentiality regarding data protection, business interruption, and data theft can result in financial damage and reputational loss WREDE, STEGEN e GRAF VON DER SCHULENBURG, 2020.

According to McAfee and the Center for Strategic and International Studies, cybercrime consumed at least $600 billion in 2017 of the entire global economy, or nearly one percent of the global GDP lost to cybercrime each year. Data breach security incidents have become commonplace annually and cost hundreds of millions. As a result, the market for insuring these losses has proliferated in the last decade. Cyber insurance is a broad term for insurance policies that cover first and third-party losses due to computer-based attacks or damage to company information technology systems. Examples include hacking or other incidents of unauthorized persons illegally gaining access to computer systems and attacks on systems by viruses or other malware ROMANOSKY, ABLON, *et al.*, 2109.

The losses above are caused by the increasing number of human activities controlled by technology and the internet. Coupled with the large amount of data stored by internet technologies, there is an increased risk of cyberattacks, defined as deliberate and malicious acts intended to damage an organization's critical ICT infrastructure via the internet. The economic consequences of these cyberattacks can be far-reaching as companies must repair or replace equipment and pay additional labor to upgrade cybersecurity programs and equipment, cover consultant fees, and even pay heavy regulatory fines for failing to protect confidential information to comply with breach reporting requirements—data or to implement necessary privacy or security measures.

Privacy is a complex concept consisting of 'three independent and reduced elements: confidentiality, anonymity, and solitude. Each of these elements is independent. Therefore, loss or violation may occur due to the intrusion of any of the three elements GAVISON, 1980. In addition, significant data breaches often lead to costly litigation and cross-litigation between multiple parties due to their interdependence, resulting in high costs for cybercrime losses NIEVAS, 2020.

Usually, cyber insurance provides 2 (two) types of coverage: the first party, which covers damage to the insured due to cyber incidents. Furthermore, third-party coverage protects liability provided in the event of a cyber incident that harms the client or related parties. These types usually include coverage for any expenses related to public relations, legal fees, and business interruptions. Cyber insurance policies are generally written on a claims-made basis, while the insured must notify the claim during the policy period KRISNAREINDRA, 2021.

In this regard, cyber insurance in Indonesia has yet to become something urgent. This is based on information from the executive director of the Indonesian General Insurance Association (AAUI), who stated that until the end of 2017, there were no more than ten cyber insurance companies, primarily foreign ones. Some of them are PT Asuransi Tokio Marine Indonesia, PT AIG Insurance Indonesia, and PT Chubb General Insurance Indonesia SANDY, 2019. In addition, according to Google Trends, Indonesia has not found sufficient data that discusses cyber insurance, as described in the following picture:

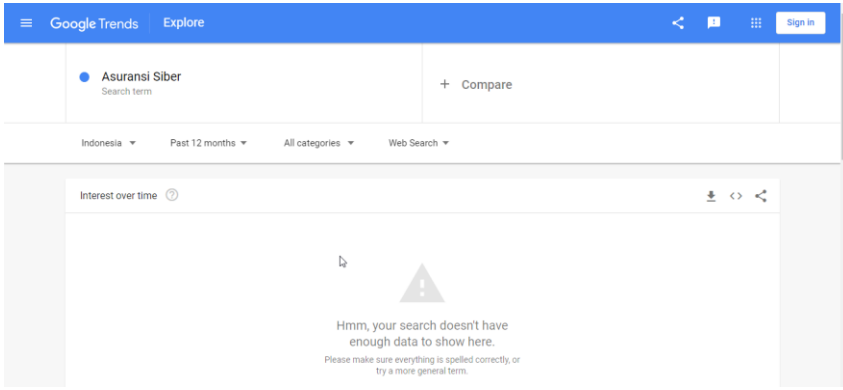

Figure 1 – Graphic Data that Discusses Cyber Insurance.

The lack of interest in cyber insurance in Indonesia is because this type of insurance is still relatively new and is different from conventional insurance. In particular, the legal framework for cyber insurance still needs to be stronger. Ni Gusti Ayu Putu Nitayanti confirmed this, and Ni Made Ari Yuliartini Griadhi in conventional periscopes, in general, that until now, Indonesia has no special rules governing the protection of personal information. Regulations regarding the protection of personal information are still separate in several laws and regulations, so a special arrangement regarding the protection of personal information is needed to create legal certainty NITAYANTI e GRIADHI, 2014.

Regarding insurance regulation, Indonesia has Law (UU) Number 40 of 2014 concerning Insurance, but the Act and implementing regulations need to explain the concept of cyber insurance specifically. Therefore, it is essential to regulate more strictly about cyber insurance in Indonesia to minimize the risks that arise when there is a theft or breach of company data MADAMBA, PULUHULAWA, *et al.*, 2021.

One example occurred on April 17, 2020, when an international hacker with the nickname 'Why So Dank' managed to hack Tokopedia. According to @underthebreach, the hacked data contained emails, passwords, and usernames with 91 million accounts and 7 million merchant accounts hacked. The perpetrators sold the data for US $ 5,000 or around Rp. 74 million FATHUR, 2020. Tokopedia is also experiencing legal problems over this data leak with a claim for compensation of 100 billion Rupiah.

The right to privacy is one of the rights inherent in everyone. The right to privacy is the dignity of every person that must be protected. Personal data relates to a person's characteristics, name, age, gender, education, occupation, address, and position in the family MAHIRA, YOFITA e AZIZAH, 2020. Therefore, the weak regulation of cyber insurance in Indonesia harms business development because companies, in the event of data hacking, will face several risks: claims for compensation, reputational damage, and the risk of temporary operational termination.

PROBLEM STATEMENT

The problems studied in this paper are focused on analyzing the concept of cyber insurance in protecting data, as well as a study of the urgency of regulating cyber insurance in Indonesia to minimize the impact of losses due to data hacking.

METHOD

This research is categorized into the normative legal research type based on the issues and themes raised as a research topic. The research approach used is the conceptual approach, philosophical approach, and analytical approach. It ends with the conclusion that aims to generate new findings as answers from the subject matter that has been set as well as will be analyzed with the descriptive-analytical method, namely by describing the laws and regulations that apply to the legal theory and practices of law enforcement positively related to the problem MARZUKI, 2014.

DISCUSSION

The Concept of Cyber Insurance in Protecting Data

Conventional insurance is not designed to cover cyber risks. Such policies, for example, general commercial liability, director's and officers' errors and omissions, and data theft and ransoms, usually do not contain express coverage for these risks in conventional insurance KISLOFF, AHUJA e BANK, 17.

Cyber insurance has been around since the late 1970s, with the market growing out of risk from technological developments/errors and negligence. In the 1980s, policies regarding cyber insurance were first introduced, designed primarily for financial institutions and blue-chip organizations. The number of insurance providers offering products has gradually grown due to technological developments CAMILLO, 2017. There is a growing awareness that cyberspace only sometimes matches conventional insurance coverage.

To avoid uncertainty about coverage for cyber risk, cyber insurance offers policies to manage potential losses from data breaches, ransomware attacks, theft or loss of unencrypted assets, business email intrusion, cloud misconfiguration exploits, and other cybercriminal activities. Personal data breaches and security incidents have become commonplace, with thousands of cases occurring each year and some costing hundreds of millions of dollars. Case in point: A cyber researcher from Singapore, DarkTracer, reported a leak of credential data from over 49 thousand government sites worldwide. In addition, as many as 40,629 internet users in Indonesia were infected with Stealers such as Redline, Raccoon, Vidar, and others. In addition, there are 502 thousand more credential data for access to the .id domain (dot id), which was leaked and distributed through dark sites ASHARI, 2022.

In essence, this phenomenon is not in line with the idea of The Right to Privacy or the right not to be disturbed. Warren and Brandheis are of the view that with the development and advancement of technology, there is a public

awareness that there has been awareness that there is a person's right to enjoy life LATUMAHINA, 2014.

The massive number of personal data breaches and security incidents implies that the market for insurance against losses has snowballed in recent decades. Cyber insurance is a broad term for insurance policies that cover first and third-party losses due to computer-based attacks or malfunctions of company information technology systems.

Increased crime using information technology has been identified since 2003, for example, carding crimes (credit card fraud), ATM/EDC skimming, hacking, cracking, phishing (internet banking fraud), malware (viruses/worms/trojans/bots), cybersquatting, pornography, online gambling, transnational crime (drug trafficking, mafia, terrorism, money laundering, human trafficking, underground economy). Cybercrime is a hacking event or another occurrence of an unauthorized person gaining access to a computer system, an attack on the system by a virus, or other malware ROMANOSKY, ABLON, *et al.*, 2109.

The initial concern over this was the spread of viruses and other types of malwares that could potentially lead to legal liability. However, the increased appreciation of cyber vulnerabilities sometimes translates into demand for cyber insurance. Most of the company's spending during the late 1990s and early 2000s focused on loss mitigation and network security. Meanwhile, insurers grappling with these emerging risk areas are reluctant to offer significant line sizes for largely untested products and where there is a dearth of historical loss data to measure and price risk. There is a feeling among insurance and corporate risk buyers that the cyber insurance market remains a niche area, lacking the coverage and capacity they need ROMANOSKY, ABLON, *et al.*, 2109.

Apart from this, the development of cyber insurance has progressed quite rapidly, accompanied by the increasing number of human activities that intersect with the internet. The coverage of protection provided by cyber insurance is as follows:

(1) Post-incident forensic investigations;
(2) Data retrieval and recovery, including negotiation and payment of ransomware requests;
(3) Notice of breach to comply with legal and contractual obligations;
(4) Credit monitoring and identity theft protection services for those affected by the incident;
(5) Management of public relations and communications to reduce potential reputational damage;
(6) Network business disruption; and

(7) Attorney's fees related to the notification of infringement.

If you look at the explanation above, the existence of cyber insurance to minimize losses from cybercrime is one of the preventive ways that can be done. Preventive legal action can be interpreted as the protection provided by the government to prevent violations that can cause harm ASRI, 2018. Unfortunately, in Indonesia, the regulations and concepts of cyber insurance have yet to be comprehensively regulated in the legislation. Even in the general context of the protection of personal data itself, no specific regulation covers it.

The Urgency of Cyber Insurance Regulations in Indonesia to Minimize the Impact of Losses Due to Data Hacking

Indonesia is one of the countries with the most significant number of internet users worldwide. Internet users in 2017 touched 143.26 million people. That number has increased a lot compared to previous years, namely, 2016, which counted 132.7 million people, and 2015, which was 110.2 million people PUTRA, 2021. Currently, internet users in Indonesia are approximately 73.7% of the total population in the 2019-2020 period (Q2) GUNAWAN, AULIA, *et al.*, 2021.

The number of internet users of that size has a considerable risk of cybercrime regarding data protection. If you look at it from a broader perspective, this crime has attacked several large companies, especially those engaged in online buying and selling (Electronic Commerce / E-commerce), by hacking user data to be traded illegally. Some of these companies, namely Tokopedia and Bukalapak, were hacked, and millions of user data were stolen/taken and traded freely in cyberspace.

This certainly causes losses for users and companies with a significant loss of value. Not to mention the issue of the company's credibility and also lawsuits against the company. Therefore, the importance of cyber insurance in Indonesia is part of the adaptation of technological developments and legal protection. The absence of a guarantee that e-commerce transactions are free from attempts to destroy/manipulate data will undoubtedly impact decreasing public trust in this system. Whereas in business transactions in the current global era, legal certainty and security are the pillars supporting the development of economic activity. It should be noted that personal data or information has become very valuable and vulnerable as a commodity. Hence, it poses a risk of vulnerability to misuse or theft of personal data FAD, 2021.

Theoretically, from a legal point of view, insurance is a: risk coverage agreement between the insured and the insurer that promises to pay for the loss caused by the insured risk to the insured. The concept is that the insurer aims to

obtain payment of a premium as a reward while the Insured aims to be free from risk and obtain compensation if a loss occurs in his interests NAVISA, 2020.

What he understands is that any risk that arises and is capable of causing harm to the insured's interests can be used as an object of insurance or, in other words, can be insured. This means that all forms of transactions in electronic commerce should be ensured to ensure legal certainty and security in transactions and minimize the risk of losses that may occur. Legal certainty will bring justice, which is when there is legal certainty. If viewed from the perspective of the grand theory of the civil law system, legal objectives can be realized in the form of justice, certainty, and benefit. If viewed from the perspective of utilitarian legal theory, personal data insurance is essential to provide the maximum benefit to the most significant number of people.

Unfortunately, the current regulations in Indonesia do not regulate the existence of insurance related to the term cyber insurance. Synergistic with this condition, Gio Arjuna Putra said, the high number of Internet penetration and social media users in Indonesia is inversely proportional to the progress of legal and technological development. This can be seen from the stipulation of a legal product at the level of the law that explicitly regulates the protection of personal data PUTRA, 2021, especially regarding personal data insurance.

Therefore, it is crucial to establish cyber insurance regulations to protect personal data. This is following the discovery of laws and the creation of new laws by the goals of the State, which is a mandatory value to be implemented to achieve legal supremacy and justice MUHTAR, 2019. The legal vacuum in personal data protection is undoubtedly very sad, considering the need for a Personal Data Protection Law to be crucial in this era of digital disruption FATHUR, 2020. So, a progressive legal approach is needed to emphasize legal breakthroughs so that harmonizing regulations and community conditions can run well. Do not let there be a stigma that the law is left behind by the society it governs TAMPI, 2018.

On the other hand, the root of the problem is the stagnation of regulations regarding the protection of personal data, especially regarding personal data insurance, partly because the State of Indonesia is still using the old laws and regulations inherited from the Netherlands of concordance. The articles that regulate insurance or coverage issues in the Commercial Code (KUHD) are articles 246 to 308 of the KUHD. Article 246 of the Commercial Code (KUHD) states insurance or coverage is an agreement in which the insurer binds himself to the insured by obtaining a premium to provide him with compensation for a loss, damage, or not getting the expected profit, which may be suffered due to an uncertain event.

Furthermore, article 247, it is stated that the coverage can include, among others: fire hazards; (KUHD 287) the dangers that threaten unharvested agricultural products; (KUHD) the soul of one or more persons; (KUHD 302) the dangers of the sea and the dangers of slavery; (KUHD 592) the dangers of transportation on land, in rivers and inland waters. (KUHD 686).

The Law of the Republic of Indonesia Number 40 of 2014 concerning Insurance does not mention the type of cyber insurance. If you refer to the Commercial Code, the types of insurance in Indonesia are:

(1) Loss Insurance: Loss insurance is an insurance agreement in which the insurer provides services to cover the risk of loss or loss of benefits to the insured. In this case, the object of loss insurance can be in the form of houses, buildings, factories, and movable objects such as motorized vehicles, ships, and movable objects contained in or as part of the relevant fixed object MUHAMMAD, 2006.

(2) Life Insurance: Life Insurance is a business that provides risk management services that provide payments to policyholders, the insured, or other entitled parties if the insured dies or remains alive or other payments to policyholders, the insured, or other entitled parties at a specific time regulated in the agreement, the amount of which has been determined and/or is based on the results of fund management. In connection with the explanation above, there is still a legal vacuum in the regulation of cyber insurance in Indonesia. Cyber insurance cannot be categorized as loss insurance because it is so complex concerning cybercrime data hacking. Indonesia still needs to establish definite rules and standardization concerning cyber insurance policy coverage. The ambiguity of this arrangement is principally at risk of legal uncertainty and losses caused by data hacking.

Based on this, the concept of cyber insurance in Indonesia must be regulated with various considerations, including:

(1) Revision of Law of the Republic of Indonesia Number 40 of 2014 concerning Insurance: This revision of the Insurance Law is mandatory so that cyber insurance arrangements can have a clear legal basis by including a particular chapter on cyber insurance, such as loss insurance or life insurance.
(2) Need for Implementing Arrangements: Implementing regulations are regulated through government or ministerial regulations relating to

substantial matters that need a complete description. This implementing regulation is regulated regarding cyber insurance coverage, policies, premiums, and the obligation to use cyber insurance for e-commerce companies and other arrangements according to cyber insurance needs.

(3) There is a need for norms that override the Civil Law Code: This needs to be done because the legal norms, especially those that regulate insurance in the Civil Code, which was made in the colonial period, are no longer following the development of the times and current technology. This urgency should be done so that in its application later, there will be no different legal interpretations that can hinder the implementation of cyber insurance in Indonesia.

Based on this, the author argues that with the increasingly complex development of technology and world crimes related to data hacking. Indonesia needs to prepare itself, especially in terms of cyber insurance regulations, in order to minimize the risk of loss from data hacking and provide legal certainty and protection for cyber-crimes.

CONCLUSIONS

The complexity of the times has brought the development of an increasingly advanced insurance world. Conventional insurance related to data hacking and cybercrimes can no longer protect against losses. As one of the countries with the most significant internet users, Indonesia should design a cyber-crime protection system, one of the regulations regarding cyber insurance. Therefore, in this case, Indonesia needs to pay attention to several things:

(1) Revise the Law of the Republic of Indonesia Number 40 of 2014 concerning Insurance.
(2) There is a need for implementing regulations regarding cyber insurance and
(3) There is a need for norms that override the Civil Code.

In addition, in the aspect of personal data protection, it is necessary to normalize a special law that regulates the protection of personal data. This is important because, until now, Indonesia does not have a law that explicitly regulates personal data.

REFERENCES

Ashari, M. (2022). Belajar Dari Kebocoran Data Kredensial: Data Yang Paling Berharga adalah Data Pribadi. *Kementerian Keuangan Republik Indonesia,* 22 Maret 2022. Available at:

https://www.djkn.kemenkeu.go.id/kpknl-kisaran/baca-artikel/14838/Belajar-Dari-Kebocoran-Data-Kredensial-Data-Yang-Paling-Berharga-adalah-Data-Pribadi.html.

Asri, D. P. B. (2018). Perlindungan Hukum Preventif Terhadap Ekspresi Budaya Tradisional di Daerah Istimewa Yogyakarta Berdasarkan Undang-Undang Nomor 28 Tahun 2014 Tentang Hak Cipta. *JIPRO: Journal of Intellectual Property*, 1, 1, 13-23.

Camillo, M. (2017). Cyber Risk and the Changing Role of Insurance. *Journal of Cyber Policy*, 2, 1, 53-63.

Chotimah, H. C. (2019). Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara [Cyber Security Governance and Indonesian Cyber Diplomacy by National Cyber and Encryption Agency]. *Jurnal Politica*, 113-128.

Fad, M. F. (2021). Perlindungan Data Pribadi Dalam Perspektif Sadd Dzari'ah. *Muamalatuna*, 13, 1, 33-69.

Fathur, M. (2020). *Tanggung Jawab Tokopedia Terhadap Kebocoran Data.* National Conference on Law Studies (NCOLS). Jakarta: Fakultas Hukum Universitas Pembangunan Nasional "Veteran" Jakarta, 43-60.

Gavison, R. (1980). Privacy and the Limits of Law. *The Yale Law Journal*, 89, 3, 421-471.

Google Trends. Explore "Asuransi Siber". *Google Trends*, 9 July 2022. Available at: https://trends.google.com/trends/explore?geo=ID&q=Asuransi%20Siber.

Gunawan, R. (2021). Adiksi Media Sosial dan Gadget bagi Pengguna Internet di Indonesia. *Techno-Socio Ekonomika*, 14, 1, 1-14.

Kisloff, M., Ahuja, J. & Bank, A. (2021). Looking for Cyber Insurance? Legal Terms, Issues to Know. *Bloomberg Law*, 2021 September 17. Available at: https://news.bloomberglaw.com/us-law-week/looking-for-cyber-insurance-legal-terms-issues-to-know.

Krisnareindra, K. (2021). The "PDP Law" Era and Cyber Protection Urgency. *IndonesiaRe*, 15 June 2021. Available at: https://indonesiare.co.id/id/article/the-pdp-law-era-and-cyber-protection-urgency.

Latumahina, R. E. (2014). Aspek Hukum Perlindungan Data Pribadi di Dunia Maya. *Gema Aktualita*, 3, 2, 14-25.

Madamba, P. (2021). Application of Territorial Principles Against Pedophile Criminal Act Perpetrators Perpetrated by Foreign Citizens. *Jurnal Legalitas*, 14, 1, 77-84.

Mahira, D. F. F., Yofita, E. & Azizah, N. L. (2020). Consumer Protection System (CPS): Sistem Perlindungan Data Pribadi Konsumen Melalui Collaboration Concept. *Jurnal Legislatif*, 3, 2, 287-302.

Marzuki, M. P. (2014). *Penelitian Hukum:* Edisi Revisi. Jakarta: Prenadamedia Group.

Muhammad, A. K. (2006). *Hukum Asuransi Indonesia.* Bandung: Citra Aditya Bakti.

Muhtar, H. M. (2019). Model Politik Hukum Pemberantasan Korupsi Di Indonesia Dalam Rangka Harmonisasi Lembaga Penegak Hukum. *Jambura Law Review*, 1, 1, p. 68-93.

Napitupulu, D. (2017). Kajian Peran Cyber Law Dalam Memperkuat Keamanan Sistem Informasi Nasional. *Deviance Jurnal Kriminologi*, 1, 1, 100-113.

Navisa, F. (2020). Karakteristik Asas Kepentingan (Insurable Interest) Dalam Perjanjian Asuransi. *Negara dan Keadilan*, 9, 2, 188-204.

Nievas, A. M. (2020). Cyber Insurance Today: Saving It before It Needs Saving. *Catholic University Journal of Law and Technology*, 29, 1, 111-144. Available at: https://scholarship.law.edu/jlt/vol29/iss1/4?utm_source=scholarship.law.edu%2Fjlt%2Fvol29%2Fiss1%2F4&utm_medium=PDF&utm_campaign=PDFCoverPages.

Nitayanti, N. G. A. P.; Griadhi, A. Y. N. M. (2014). Perlindungan Hukum Terhadap Informasi Pribadi Terkait Privacy Right Berdasarkan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. *Kertha Negara: Journal Ilmu Hukum*, 2, 5, 1-6.

Parker, D. B. (2007). The Dark Side of Computing: SRI International and the Study of Computer Crime. *IEEE Annals of the History of Computing*, 29, 1, 3-15.

Puluhulawa, F. U., Puluhulawa, J. & Katili, M. G. (2020). Legal Weak Protection of Personal Data in the 4.0 Industrial Revolution Era. *Jambura Law Review*, 2, 2, 182-200.

Putra, G. A. (2021). Reformulasi Ketentuan Pengelolaan Data Pribadi sebagai Ius Constituendum dalam Menjamin Perlindungan Data Pribadi Pengguna Layanan Media Sosial. *Jurnal Hukum Lex Generalis*, 2, 8, 684-700.

Putra, W. (2021). Aspek Cybercrime dalam Paylater. *Jurist-Diction*, 4, 2, 791-812.

Romanosky, S. (2019). Content analysis of cyber insurance policies: how do carriers price cyber risk? *Journal of Cybersecurity*, 5, 1, 1-19.

Sandy, O. P. (2019). Asuransi Siber di Indonesia Masih belum Diminati. *Cyberthreat.id*, 10 May 2019. Available at:

https://cyberthreat.id/read/418/Asuransi%20Siber%20di%20Indonesia%20Masih%20belum%20Diminati%20https:/cyberthreat.id/read/418/Asuransi-Siber-di-Indonesia-Masih-belum-Diminati.

Sanusi, M. A. (2004). *Teknologi Informasi dan Hukum E-commerce.* Jakarta: Dian Ariesta.

Sautunnida, L. (2018). Urgensi Undang-Undang Perlindungan Data Pribadi di Indonesia: Studi Perbandingan Hukum Inggris dan Malaysia. *KANUN: Jurnal Ilmu Hukum*, 20, 2, 369-384.

Talesh, S. A. (2018). Data Breach, Privacy, and Cyber Insurance: How Insurance Companies Act as "Compliance Managers" for Businesses. *Law & Social Inquiry*, 43, 2, 417-440.

Tampi, M. M. (2018). Menakar Progresivitas Teknologi Finansial (Fintech) Dalam Hukum Bisnis Di Indonesia. *Era Hukum-Jurnal Ilmiah Ilmu Hukum*, 16, 2, 246-281.

Wrede, D., Stegen, T. & Graf Von Der Schulenburg, J. (2020). Affirmative and silent cyber coverage in traditional insurance policies: Qualitative content analysis of selected insurance products from the German insurance market. *Geneva Pap Risk Insur Issues Pract*, 45, 4, 657-689.

The Law, State and Telecommunications Review / Revista de Direito, Estado e Telecomunicações

Contact:
Universidade de Brasília - Faculdade de Direito - Núcleo de Direito Setorial e Regulatório
Campus Universitário de Brasília
Brasília, DF, CEP 70919-970
Caixa Postal 04413

Phone: +55(61)3107-2683/2688

E-mail: getel@unb.br

Submissions are welcome at: https://periodicos.unb.br/index.php/RDET