LEGAL ASPECTS OF IMPLEMENTATION OF INSURANCE AGREEMENTS BASED ON INSURANCE PRINCIPLES IN CYBER INSURANCE

Purgito[1], Ratna Januarita[2], Toto Tohir Suriaatmadja[3]
[1] Student of Law Faculty of Bandung Islamic University
[2,3] Lecturers of Law Faculty of Bandung Islamic University
dosen01862@unpam.ac.id

ABSTRACT
Cyber insurance was born along with the development of information technology. The problem discussed is the implementation of insurance agreements in cyber insurance carried out based on insurance principles which include the principles of utmost good faith, indemnity, and subrogation. Implementation of the principle of utmost good faith is not solely borne by the Insured but is also the responsibility of the Insurer. Implementing the principle of indemnity in insurance agreements when a risk occurs that causes losses in cyber insurance can encounter obstacles when submitting a claim. Inhibiting factors include the difficulty of determining the actual value of losses accurately. Meanwhile, the factor that hinders the implementation of subrogation is that the whereabouts of third parties who cause losses are often difficult to know. Even if it is known but is outside Indonesian jurisdiction, then this will create difficulties for the implementation of subrogation rights. The method used is normative juridical to assess the extent to which the implementation of insurance agreements is based on insurance principles in cyber insurance and inhibiting factors. The research results show that the implementation of insurance agreements based on insurance principles in cyber insurance experiences obstacles, namely the difficulty of implementing the principles of indemnity and subrogation in insurance agreements.

Keywords : Cyber Insurance, Implementation of Insurance Agreements, Insurance Principles.

A. BACKGROUND

The development of information technology has experienced a tremendous acceleration in the last few decades. This technology has changed the way we work, communicate and do business. According to a report from the International Data Corporation (IDC), global spending on information technology is expected to reach $4.2 trillion in 2021, an increase of 8.6% from the previous year.[1] This development spans sectors such as banking, health, education, and manufacturing, all of which rely on digital infrastructure for

[1] IDC. (2021). Worldwide IT Spending Forecast. Retrieved from https://www.idc.com

day-to-day operations.

The rapid development of technology has resulted in us being very dependent on technology. Currently, the technology that plays the biggest role is information technology and data processing. This has given rise to the phenomenon of digital transformation and digitization which is changing the way businesses and organizations operate.[2] With the help of interconnected processes and information technology, companies can achieve their goals by generating added value and balancing the benefits and risks of information technology.[3]

Today, increasing connectivity between business and our daily lives is driving business transformation and improving the lives of employees and customers around the world. Therefore, the Government, Private Sector, Business Actors and the Indonesian Digital Society can be a future benchmark for the challenges and threats of cyber security that occur.[4]

The increase in cyber security threats in the digital era has become a major concern for many organizations and individuals. According to the latest report from Cybersecurity Ventures, it is estimated that losses due to cyber crime will reach $6 trillion in 2021. In an increasingly advanced digital era, digital security is a very important thing to pay attention to. System hacking, theft of personal data, theft of financial data, embezzlement, fraud, and post-attack disruption of normal business activities are some examples of such attacks. This is definitely very detrimental and can affect the development of digital transformation, especially in the economic and financial fields.[5]

The importance of protecting data and information can no longer be ignored. One solution that can be used to overcome cyber risks is by implementing cyber insurance. Cyber insurance can provide financial protection and technical assistance in the face of cyber attacks. Because cyber insurance is an important component of the digital world, cyber risk management is very important and is at the core of the digital world. Therefore, the insurance

[2] Bencsik, A., Hargitai, D. M., & Kulachinskaya, A. (2022). Trust in and Risk of Technology in Organizational Digitalization. *Risks*, *10*(5). https://doi.org/10.3390/risks10050090.

[3] Erniwati, S., & Kurnia, N. (2015). An Analysis of Information Technology on Data Processing by using Cobit Framework. International Journal of Advanced Computer Science and Applications, 6(9). https://doi.org/10.14569/ijacsa.2015.060920

[4] Rahmawati, C. (2020, November). Tantangan Dan Ancaman Keamanan Siber Indonesia Di Era Revolusi Industri 4.0. In *Prosiding Seminar Nasional Sains Teknologi dan Inovasi Indonesia (SENASTINDO)* (Vol. 2, pp. 299-306).

[5] Fitran Briliano (2022, Sept 22). Keamanan Siber, Urgensi di Tengah Transformasi Ekonomi Digital, https://www.idntimes.com/opinion/social/fw-rocket/urgensi-keamanan-siber-c1c2#:~:text=Menurut%20data%20dari%20Cybersecurity%20Ventures%2C%20diperkirakan%20pada%20tahun,triliun%20per%20tahun%20yang%20disebabkan%20oleh%20serangan%20siber, (diakses tanggal 12 Juni 2024 pukul: 19.48 wib).

industry must ensure and provide facilities for the cyber insurance market so that it continues to grow and develop strongly.[6]

The rapid digitalization of the economy and social relations is the main reason why the issues of cyber risk, cyber threats and cyber security continue to become increasingly important. The digitalization of the economy and social relations brings serious new opportunities and threats and is not the only source of opportunities for development and innovation. Unintentional or deliberate cyber events can cause loss of availability, integrity and confidentiality of digital data.[7]

Cyber risk results from the use of technology and is the biggest new threat facing businesses and consumers, namely exposure to losses related to the use of electronic equipment, computers, information technology and virtual reality. The security of consumer, financial, and health information is increasingly important. Theft of identity and personal, financial, and health information can occur due to hackers, malware, viruses, tracking software, eavesdropping, eavesdropping, robocalls, and solicitations. Nearly all major industries were impacted by this breach; these include financial services, healthcare, government, entertainment, sales, insurance, social networking, credit card processing, and law.[8]

Cyber risk generally relates to the risk of financial loss, disruption or damage to an organization's reputation caused by the failure of its information technology systems. Cyber risks can occur in a variety of ways, such as operational IT risks due to factors such as poor system integrity. Apart from that, cyber risk can arise due to cyber crime. Smart technology, digitalization and globalization have increased the propensity and intensity of cybercrime.[9] There are important and influential factors in explaining the incidence of cyber risk and the amount of loss, namely size, risk of transmission, and legal responsibility. The importance of these three factors applies not only to the financial industry but also to other industries exposed to cyber risks.[10]

---

[6] Muh. Fajrul Falah (2023, May 5). Tren Risiko Cyber Insurance di 2023, https://mediaasuransinews.co.id/asuransi/tren-risiko-cyber-insurance-di-2023/). Diakses tanggal 02 April 2024, pukul 20.20 wib

[7] Strupczewski, G. (2021). Defining cyber risk. Safety Science, 135. https://doi.org/10.1016/j.ssci.2020.105143

[8] Talesh, S. A. (2018). Data Breach, Privacy, and Cyber Insurance: How Insurance Companies Act as "Compliance Managers" for Businesses. Law and Social Inquiry, 43(2). https://doi.org/10.1111/lsi.12303

[9] Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: a systematic review of data availability. Geneva Papers on Risk and Insurance: Issues and Practice, 47(3), 698–736. https://doi.org/10.1057/s41288-022-00266-6

[10] Eling, M., & Jung, K. (2022). Heterogeneity in cyber loss severity and its impact on cyber risk measurement. Risk Management, 24(4). https://doi.org/10.1057/s41283-022-00095-w

Cybercrime threats such as hacking, malware and phishing are increasing and can threaten sensitive data and the continuity of a company's business. Hacking[11] is an activity where someone tries to exploit weaknesses in a computer system or network and gain unauthorized access to change or steal data that should not be accessible. This activity is usually carried out by cyber criminals called hackers. Malware[12] is a generic term used to refer to malicious or malicious programs designed to damage, interfere with, or steal data without the user's permission. Meanwhile, ransomware is a type of malware designed to encrypt data on a computer, so that users cannot access it. Phising[13] is a technique used by cyber criminals to steal personal or company information by tricking victims into providing that data. Thus, protection through cyber insurance is an important solution to reduce the risk of loss due to cyber attacks.

There needs to be special insurance for cyber risk as a solution, namely by using a type of insurance related to cyber risk. The insurance industry is one of the businesses that has been impacted by technological developments. The development of a separate market for cyber insurance is driven by the need to address cyber risks and digital transformation challenges.[14]

How the insurance agreement is implemented based on insurance principles in cyber insurance? What are the obstacles faced in implementing the principles of the agreement? These questions are important to study further in order to provide legal certainty and legal protection in the framework of risk management in cyber insurance.

B. RESEARCH METHODOLOGY

This research uses a normative juridical research approach, namely research that places law as a system of norms. Normative juridical research studies principles, norms, rules, agreements, court decisions, and legal doctrine or teachings.[15]

This research connects a concept based on literature in the field of insurance law which is linked to the facts of contractual relationships that occur in practical settings in

[11] https://itbox.id/blog/hacking-adalah/
[12] https://digitalsolusigrup.co.id/pahami-perbedaan-malware-dan-ransomware/
[13] https://techbuddy.id/kamus/phishing-2353/
[14] Hatzivasilis, G., Chatziadam, P., Petroulakis, N., Ioannidis, S., Mangini, M., Kloukinas, C., Yautsiukhin, A., Antoniou, M., Katehakis, D. G., & Panayiotou, M. (2019). Cyber insurance of information systems: Security and privacy cyber insurance contracts for ICT and helathcare organizations. IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks, CAMAD, 2019-September. https://doi.org/10.1109/CAMAD.2019.8858165.
[15] Mukti Fajar ND dan Yulianto Achmad, *Dualisme Penelitian Hukum Normatif & Empiris*, Pustaka Pelajar, Yogyakarta, 2010, p. 34.

cyber insurance products. Based on the approach to the data collected, this type of research is qualitative research, namely research that produces descriptive data.[16] This research is descriptive analytical in nature, namely describing the implementation of insurance agreement principles in the practice of the cyber insurance industry in Indonesia.

In this qualitative research, the author tries to explain the actual facts in a practical setting regarding the implementation of agreements in cyber insurance, then examines the obstacles or constraints in implementing agreements related to insurance law from a cyber-insurance perspective. Based on the location of this research, it is library research.[17]

The approach method is intended to obtain information from various aspects regarding legal issues to find answers, which includes a conceptual approach according to expert opinion (doctrine) related to insurance legal material, a statutory approach, and a comparative approach as part of a complementary approach to comparisons with foreign countries regarding insurance, especially cyber insurance.[18]

C. FINDING & DISCUSSION

1. IMPLEMENTATION OF THE PRINCIPLES OF UTMOST GOOD FAITH INDEMNITY AND SUBROGRATION IN CYBER INSURANCE

In insurance law there is a legal relationship between the Insurer and the Insured regarding risk management. This legal relationship arises because of an insurance agreement called an insurance policy. The policy states the rights and obligations of the parties based on general agreement principles such as the principle of consensualism, the principle of good faith and freedom of contract. Apart from that, insurance agreements are also guided by insurance principles such as insurable interest, utmost good faith, indemnity and subrogation. The insurance company and the policyholder have a legal relationship with each other as a result of the contracts they signed contained in the agreement. In the agreement, each party has the rights and obligations stipulated in the agreement, which must be obeyed and implemented in accordance with the law.[19] The legal relationship between the insurer and the insured party arises from the existence of an insurance agreement that has been made by

[16] Kaelan, *Metodologi Kualitatif Bidang Filsafat, Paradigma*, Yogyakarta, 2005, p. 5

[17] Muhammad Teguh, *Metode Penelitian Ekonomi; Teori dan Aplikasi*, PT. Raja Grafindo Persada, Jakarta, 1999, p. 14.

[18] Agus Yudha Hernoko, *Hukum Perjanjian Asas Proporsionalitas Dalam Kontrak Komersial*, Cet ke-2, Kencana Prenadamedia Group, Jakarta, 2011, p. 39.

[19] Syamsuddin, M., & Putri, C. S. (2022). Proteksi Hukum Bagi Pemegang Polis Asuransi Terhadap Pailitnya Perusahaan Asuransi. SALAM: Jurnal Sosial dan Budaya Syar-i, 9(2). https://doi.org/10.15408/sjsbs.v9i2.25112

the parties.[20]

Cyber insurance can be defined as an insurance product that provides protection against cyber security risks faced by an organization or individual. The types of cyber insurance policies can vary, ranging from protection against financial losses due to cyber attacks to post-attack recovery costs. Cyber security threats can come from various types of attacks, such as malware, phishing, ransomware, and so on. The impact of this cyber threat is not only felt by companies, but also individuals who are vulnerable to identity and personal data theft.

The history of cyber insurance can be traced back to the beginning of the development of information technology and the internet. Rapid technological developments have opened the door to increasingly sophisticated and detrimental cyber attacks. Along with that, the need for protection against these risks has encouraged the birth of cyber insurance products.

Because cyber security governance in Indonesia is still partial and sectoral, handling cyber security issues is not yet integrated. This makes cyber threats even more real, especially when linked to cyber security threats for government and private companies. Therefore, cyber security management must be carried out in an integrated manner to protect the state and nation from cyber attacks. The National Cyber and Crypto Agency (BSSN), as a government agency responsible for cyber security, is expected to help build a cyber security legal framework that must be complied with by all stakeholders related to the implementation of cyber security in Indonesia. In addition, this legal framework must include regulations that enable the enforcement of crimes that occur in cyberspace, so that violations committed in cyberspace can be punished.[21]

This paper discusses the legal aspects of implementing insurance agreements, insurance principles in cyber insurance. First, we will discuss the principle of utmost good faith. There are several terms related to this principle of utmost good faith. There is something called good faith, perfect honesty, or the principle of the best possible honesty. Meanwhile, outside Indonesia, there are those who call it in Latin, namely uberrima fides and in English it is called the Principle of utmost good faith.[22]

The principle of utmost good faith explains that before closing the insurance

[20] Sabrie, H. Y., & Amalia, R. (2015). Karakteristik Hubungan Hukum Dalam Asuransi Jasaraharja Terhadap Klaim Korban Kecelakaan Angkutan Umum. Yuridika, 30(3), 387-406.

[21] Sudarmadi, D. A., & Runturambi, A. J. S. (2019). Strategi Badan Siber dan Sandi Negara (BSSN) Dalam Menghadapi Ancaman Siber di Indonesia. Jurnal Kajian Stratejik Ketahanan Nasional, 2(2).

[22] Mulhadi, *Dasar-Dasar Hukum Asuransi*, PT. RajaGrafindo Persada, 2017, p.83.

agreement, the Insured has an obligation to provide information regarding the condition of the object that is the object of insurance. This is different from the provisions contained in Article 1338 paragraph (3) of the Civil Code which stipulates that "agreements must be implemented in good faith by both parties. "The implementation of good faith as intended by Article 1338 paragraph (3) of the Civil Code lies in the implementation of the insurance agreement."

Looking at the concept of Indonesian law, in relation to the principle of utmost good faith, it is regulated in Article 251 of the Commercial Code, which states that "Every statement that is false or untrue, or every failure to disclose things known to the Insured, no matter how good faith he has." ", which is of such a nature that if the Insurer had known the actual situation, the agreement would not have been closed or closed with the same conditions, resulting in the cancellation of the coverage." The provisions in Article 251 of the KUHD above emphasize to the Insured that the Insured is obliged to notify or convey all correct information (material facts) to the Insurer regarding the object of insurance.

As intended in Article 251 of the Commercial Code, which states that the principle of utmost good faith is not absolutely only imposed on the Insured but is also intended or becomes a burden on the Insurer. This is supported by the opinion of an expert, Like Wise Farwell L.J which is also supported by Carter, who said that "an insurance agreement is an agreement that requires uberrima fides, not only by the Insured but also by the Insurance Company as the Insurer". However, Carter stated that the obligation to notify was prioritized by the Insured, because the Insurer had a more passive position. In practice in Indonesia, insurance companies currently adhere to Carter's opinion.

Law No. 40 of 2014 concerning Insurance, the principle of utmost good faith has been emphasized in Article 31 paragraph (2) which reads "Insurance Agents, Insurance Brokers, Reinsurance Brokers, and Insurance Companies are obliged to provide information that is correct, not false, and/or not mislead the Policy Holder, Insured, or Participants regarding the risks, benefits, obligations and costs associated with the insurance products or sharia insurance products offered." The sentence in Article 31 paragraph (2) in the phrase "Insurance companies are obliged to provide correct, not false and/or not misleading information to Policy Holders...", shows that the principle/principle of utmost good faith or perfect good faith is something that must be implemented by insurance companies in carrying out their business. However, on the other hand, the policy holder or insured must also implement the principle of utmost good faith, namely by providing truthful information regarding the condition/condition of the insured object as stated in Article 251 of the

Commercial Code.

In cyber insurance practices, both the Insurer and the Insured are obliged to follow the provisions in Law No. 40 of 2014 and in the Commercial Code. As explained in Article 31 No.40 of 2014, the principle of utmost good faith or perfect good faith is something that must be implemented by insurance companies in carrying out their business, namely regarding cyber benefits and risks related to protecting the Insured's data. Likewise, in Article 251, it is stated that the policy holder or insured must also implement the principle/principle of utmost good faith, namely by providing truthful information relating to the condition/condition of the object being insured, namely providing honest information relating to the condition of the object in the form of insured data.

The principle of indemnity is one of the principles that is quite important in indemnity insurance, because this principle is the difference between insurance and gambling and chance agreements. Insurance is different from gambling and chance agreements, insurance has the aim of reducing risk while gambling creates/creates risk.[23]

The principle of indemnity is that the amount of compensation is equal to the amount of loss suffered. Some translate the principle of indemnity as the principle of balance. However, this view has received criticism, because if the principle of indemnity is considered as a principle of balance, it means that compensation is not necessarily balanced with the actual compensation suffered by the insured.[24]

Through an insurance agreement, the insurer provides protection to the insured against possible economic losses that will be suffered. The main objective of an insurance agreement is basically the ability of the insurer to provide compensation for losses to the insured in the event of an uncertain event or incident which is a form of protection for the insured who experiences a loss. Uncertain events or events are events for which insurance is held that cannot be guaranteed to occur or cannot be guaranteed to occur and are not expected to occur.

It can be said that an event is an event that cannot be known or cannot be ascertained, even according to normal human experience it is difficult to predict. Thus, it can be said that it is very difficult to predict the occurrence of an event. In fact, it is certain that no normal human being expects a detrimental event to occur, because a normal human being is well aware that if such an event occurs it will definitely cause him to suffer because of losses.[25] H. Gunanto, an insurance expert, is of the opinion that "The principle of indemnity is implied in

[23] Abbas Salim, *Asuransi dan Manajemen Risiko*, RajaGrafindo Persada, Jakarta, 2007, p. 8.
[24] A. Junaedy Ganie, *Hukum Asuransi Indonesia*, Sinar Grafika, Jakarta, 2011, p. 208.
[25] Abdul Kadir Muhammad, *Hukum Asuransi Indonesia*, Citra Aditya bakti, Bandung, 2006, p. 120.

Article 246 of the Commercial Code which limits insurance agreements (namely loss insurance), as an agreement that intends to provide compensation for loss, damage or loss (Indemnity) that the Insured may suffer due to being hit by a danger. where the time of closing of the insurance agreement cannot be ascertained".[26]

Providing compensation in insurance must not result in the insured's financial condition being in a more advantageous position compared to the position before the loss experienced by the insured. Thus, it is only limited to the initial position or initial state of the insured's position or state. An Insured who experiences a loss, in this insurance, is simply placed in the original position or the position where the insured who has not experienced a loss is positioned. In this case, Compensation in this case is defined as compensation for losses from the Insurer to the Insured in proportion to the losses actually suffered/experienced by the Insured.[27] The principles of civil law which are in line with the principle of Indemnity explain that in insurance there is a prohibition on enriching oneself unlawfully, or also known as onrechtmatige verrijking, namely enriching oneself without rights.[28]

The principle of indemnity provides a guideline or measure, namely that compensation must be truly in accordance with the true value of the object that suffered the loss. This principle explains that a person or insured who suffers a loss is only placed back in the same position as before the loss occurred. The principle of indemnity is used to measure the amount of loss, for example in a fire insurance agreement, which determines the value of compensation by measuring the actual value of the loss, namely the compensation value of property damaged by fire which is then reduced by the depreciation value.[29]

The Principle of Indemnity is also followed by the principle of Insurable Interest. Thus, there must be continuity between interest and the principle of indemnity, and the insured must have a genuine interest in the possibility of suffering loss due to the occurrence of uncertain events or events that are not expected to occur.[30] The meaning of interest referred to here is that there is a connection or legal relationship between the insured and the object that is the

[26] H. Gunanto dalam Ridwan Khairandy, *Pengantar Hukum Dagang*, FH UII Press, Yogyakarta, 2006, p. 203.

[27] *Ibid*.

[28] Emmy Pangaribuan Simanjutak, dalam Ridwan Khairandy, Pengantar Hukum Dagang, FH UII Press, Yogyakarta, 2006, p. 203-204.

[29] Elsi Kartika Sari dan Advendi Simangunsong, *Hukum Dalam Ekonomi*, Cetakan kelima (edisi 2), PT. Grasindo, Jakarta, 2008, p. 108.

[30] Sri Redjeki Hartono dalam Ridwan Khairandy, *Pengantar Hukum Dagang*, FH UII Press, Yogyakarta, 2006, p. 202.

object of insurance. Often it can also be said that what is called interest is wealth or subjective rights which, if an uncertain event or incident occurs, will cause losses for the insured. So, here it appears that the interest in insurance is something that cannot be ignored.[31]

The principle of indemnity with the principle of interest only applies to insurance that has interests that can be valued in money, so that the implementation of the principle of indemnity in cyber insurance practices related to cyber risks that occur which cause losses in terms of damage or loss of data must be calculated in money. Determining the true value of losses related to damage or loss of data is a challenge in the cyber insurance industry.

Given the important role of insurance companies in the insurance industry in maintaining the trust of their customers, insurance companies in Indonesia must be very careful in protecting personal data. Failure to protect personal data can harm a company's reputation and integrity.[32] However, this vigilance remains vulnerable to the emergence of cyber risks. Cyber risks arising from cyber attacks can cause losses. Losses that arise are the responsibility of the insurance company, which in this case acts as the Insurer for the emergence of cyber risks.

Next is related to the principle of subrogation. The principle of subrogation itself is regulated in Article 284 of the Commercial Code (KUHD) which reads: "The insurer who has paid for the loss of the insured item, obtains all rights that the insured would have had against a third party in relation to the loss; and the insured is responsible for any actions that may harm the insurer's rights against the third party."

In insurance law, if the insured has received compensation for losses from the insurer, he can no longer obtain rights from the third party who caused the loss. The rights to the third party are transferred to the insurer who has paid the loss to the insured. The purpose of this provision is to prevent the insured from obtaining double compensation which is contrary to the principle of balance or enriching themselves without rights. This principle is actually a logical consequence of the principle of indemnity, namely only providing compensation to the insured for the losses they suffer. If the insured turns out to have a claim from another party after receiving compensation, then the insured has no right to receive it, and this right passes to the insurer.[33]

---

[31] Sentosa Sembiring, *Hukum Asuransi*, Nuansa Aulia, Bandung, 2014, p.31

[32] Januarita, R., Alamsyah, I. F., & Perdana, A. (2024). Guardians of data: TruMe Life's continuous quest for data protection. Journal of Information Technology Teaching Cases. https://doi.org/10.1177/20438869241242141

[33] B. Parera, A., & Tumanggor, M. S. (2021). Application Of Business Principles Insurance In Indonesia. Journal of Law, Politic and Humanities, 2(1). https://doi.org/10.38035/jlph.v2i1.49

In practice, the right of subrogation must not harm the insurer's rights, such as when the insured releases third parties from the obligation to pay compensation or provide compensation for their debts. Thus, when the insurer uses its subrogation rights against a third party, the person concerned no longer has a relationship with the insured, and the insured must be responsible for all its actions that are detrimental to the insurer.

Subrogation is the legal right that an insurance company has to recover money paid to the insured from the party who made the mistake. Until recently, subrogation was a somewhat difficult, complicated process, and required a lot of communication and physical examination between the insurance company and the insured.[34] (Bhadra et al., 2022). The implementation of the subrogation principle is always related to the principle of indemnity or the principle of balance, namely that compensation must be in accordance with or balanced with the actual value of the loss. In insurance law, the principle of indemnity states that the insured is entitled to full compensation for their losses, no more or less.[35]

Because if the Insured receives compensation payments from the Insurer and from the third party who caused the loss, then the Insured's position becomes enriched or receives a payment that exceeds the actual value of the loss. Therefore, the Insured who has received compensation from the Insurer may not receive compensation from the third party who caused the loss. So, based on the principle of subrogation, the Insured who has received compensation from the Insurer transfers his right to claim compensation to the Insured. Insurers claiming subrogation and plaintiffs claiming indemnification have one thing in common: their claims concern financial losses only..[36]

2. BARRIERS TO IMPLEMENTATION OF INSURANCE AGREEMENT PRINCIPLES IN CYBER INSURANCE

According to data from the International Data Corporation (IDC), the global cyber insurance market is expected to reach a value of USD 20 billion by 2023, indicating significant growth in the industry.[37]

The insurance business is currently receiving opportunities to make technological

[34] Bhadra, O., Sahoo, S., Kumar, C. M., & Halder, R. (2022). Decentralized Insurance Subrogation Using Blockchain. ACM International Conference Proceeding Series. https://doi.org/10.1145/3581971.3581972

[35] Ginders, K. (2016). Insurance Law and the Principle of Indemnity in Light of Ridgecrest NZ Ltd v IAG New Zealand Ltd. Victoria University of Wellington Law Review, 47(1). https://doi.org/10.26686/vuwlr.v47i1.4879

[36] Weir, T. (2012). Subrogation and indemnity. Cambridge Law Journal, 71(1). https://doi.org/10.1017/S0008197312000190

[37] IDC. (2021). Worldwide IT Spending Forecast. Retrieved from https://www.idc.com

breakthroughs. This has accelerated the digitalization of the insurance market.[38] The insurance industry is becoming more vulnerable to cyber threats due to the increased use of digital technology by industry players. This can include disruption to business operations and data theft. Therefore, progress in digitalization of the insurance industry must be balanced with improvements in information technology governance and risk management. Monitoring Information Technology is very important to prevent the negative effects of the use of Information Technology on consumers and industrial stability.[39] Cyber insurance promotes internet security and is an important part of digital risk management.[40]

Cyber Insurance is an effective solution in dealing with digital security threats. By providing financial and operational protection, cyber insurance helps organizations to mitigate risks arising from cyber-attacks. However, on the other hand, there are challenges in the form of less than optimal forms of legal protection in cyber insurance practices. This challenge must be answered by creating laws and regulations that provide optimal protection for Insurers and Insureds who are bound by insurance agreements or policies.

Based on data from the Institute of Internal Auditors (IIA), the Financial Services Authority (OJK) recorded that losses due to cybercrime worldwide in 2023 will reach 8 trillion US dollars. According to Sophia Wattimena, Chair of the OJK Audit Board, losses due to ransomware worldwide are estimated to reach 265 billion US dollars in 2031. According to data from the National Cyber and Crypto Agency (BSSN), from January to October 2023 there were 361 million cyber attacks in Indonesia. therefore, these numbers are quite significant.[41]

In the digital era, it cannot be denied that cyberspace has become very important in all activities. This makes company owners vulnerable to cyber criminals in terms of the security of customers' or consumers' personal data. This requires cyber insurance designed to protect vulnerable parties. The study of how law and technology relate to each other is now more important than ever. To name a few examples, advances in technologies such as artificial intelligence, information communications, biological and chemical engineering, and space travel technology have forced us to reconsider what we know about basic concepts

[38] Mustafina, A. A., Kaigorodova, G. N., Alyakina, P. D., Velichko, N. Y., & Zainullina, M. R. (2020). Digital technology in insurance. Advances in Intelligent Systems and Computing, 908. https://doi.org/10.1007/978-3-030-11367-4_65

[39] Otoritas Jasa Keuangan, Roadmap Perasuransian Indonesia 2023-2027, 2023.

[40] Bolot, J., & Lelarge, M. (n.d.). Cyber Insurance as an Incentive for Internet Security.

[41] Hanif Reyhan Ghifari, OJK: Akibat Kejahatan Siber, Dunia Rugi 8 T Dolar AS pada 2023, https://tirto.id/ojk-akibat-kejahatan-siber-dunia-rugi-8-t-dolar-as-pada-2023-gSPd, diakses tanggal 4 Juni 2024 pukul 22.21 wib).

in tort and insurance law.[42]

Each business is responsible for its own risk. Risk transfer such as buying insurance is a strategy to overcome risk. Demand for cyber insurance products continues to increase as a result of these risks.[43] By having a cyber insurance policy a person has the right cyber insurance coverage, so they will be able to provide important support to help the business stay afloat. In the event of a cyber attack, a cyber insurance policy will cover the financial costs, financial risks and reputation of first parties and third parties if data or electronic systems have been lost, damaged, stolen or damaged. The insurance policy reimburses costs for cybercrime investigations, recovering data lost in security breaches and computer system recovery, loss of income resulting from business closures, reputation management, extortion payments demanded by hackers, and notification costs, in the event you are requested to notify affected third parties.

In Indonesia itself, not many insurance companies offer this insurance policy. One of the players in the cyber insurance industry in Indonesia is AIG Indonesia through CyberEdge® insurance. On the AIG website it is said that this insurance has several protection facilities specifically designed to help manage and reduce the effects of data breaches and the consequences of loss of company information.[44]

In Indonesia, cyber insurance is still a relatively new product but is starting to get greater attention from companies and consumers. The Financial Services Authority (OJK) has issued regulations related to cyber insurance, namely Regulation of the Financial Services Authority of the Republic of Indonesia Number 8 of 2024 concerning Insurance Products and Marketing Channels for Insurance Products. However, this POJK cannot explicitly provide protection for data and information in the digital environment. In the explanation of Article 58 POJK, it is stated about the Digital Implementation of Insurance Products. What is meant by "organizing Insurance Products digitally" is activities related to Insurance Products by Insurance Companies or Sharia Insurance Companies that use electronic system facilities, the processes of product selection, risk selection, payment of Premiums/Contributions, and issuance of Insurance Policies are carried out digitally without requires a face-to-face process. So, it is not a cyber-insurance product specifically designed

[42] Lubin, A. (2021). INSURING EVOLVING TECHNOLOGY. CONNECTICUT INSURANCE LAW JOURNAL, 28(1).

[43] Zeller, G., & Scherer, M. (2022). A comprehensive model for cyber risk based on marked point processes and its application to insurance. European Actuarial Journal, 12(1). https://doi.org/10.1007/s13385-021-00290-1

[44] Agus Sofian Eka Hidayat, Cyber insurance di Era 4.0, Pentingkah, https://datapolis.id/asuransi-siber-di-era-4-0-pentingkah/, diakses tanggal 13 Juni 2024 pukul 10.15 wib).

to protect businesses from threats in the digital era such as data breaches or malicious cyber hacking of work computer systems. This is certainly a challenge for the development of the insurance industry in Indonesia, especially cyber insurance.

Despite the huge opportunities in the cyber insurance industry, there are also obstacles, namely the lack of specific and comprehensive regulations regarding cyber insurance, which means that the implementation of cyber insurance law in Indonesia is still limited. The gap between regulations and practice in the field is also an obstacle in implementing cyber insurance.

Implementing the principle of indemnity in insurance agreements when a risk occurs that causes losses in cyber insurance can encounter obstacles when submitting a claim. Inhibiting factors include the difficulty of determining the actual value of losses accurately. This is understandable considering that the insurance object that is covered is data in a computer system. Therefore, special expertise is needed to be able to analyze objects that are at risk of damage or loss of data due to cyber-attacks.

In assessing losses arising from damage or loss of data, both parties, namely the Insurer and the Insured, must apply the principle of utmost good faith. The principle of uutmost good faith is not absolutely only imposed on the Insured but is also intended or becomes a burden on the Insurer. This is supported by the opinion of an expert, Like Wise Farwell L.J which is also supported by Carter, who said that an insurance agreement is an agreement that requires uberrima fides, not only by the Insured but also by the Insurance Company as the Insurer.

Furthermore, it is related to the implementation of the subrogation principle in insurance agreements. In accordance with the insurance agreement, the insurance company accepts all the insured's rights from the person responsible for the damage. The insurer assumes the role of the insured and utilizes its right to subrogate the insured's rights. For Insurers, subrogation is not an obligation but a right.[45]

In cyber insurance, the principle of subrogation can be used to reduce the financial losses incurred by the insurance company due to a successful cyber-attack. The insurance company can take over the insured's right to sue other parties who are responsible for the loss. The act of subrogation has two benefits, namely reducing risks for companies that

[45] Dimov, T. (2018). SUBROGATION IN INSURANCE CONTRACT. Knowledge International Journal, 28(6). https://doi.org/10.35120/kij28061985t

collect consumer data and encouraging vendors to maintain better data security.[46] In other words, subrogation typically provides dual benefits, namely risk mitigation for the companies collecting consumer data and incentives for better data security on the part of the vendors storing the data.

The right of subrogation arises because of the actions of a third party which causes loss to the object of insurance. For the losses incurred, the third party can be sued for compensation. Based on Article 1365 of the Civil Code, it is stated that every act that violates the law and causes loss to another person requires the person who caused the loss through his fault to compensate for the loss. In this case, the Insurer as the owner of the object has the right to demand compensation from the third party who caused the loss. However, in the context of insurance, after the Insurer provides compensation to the Insured, the right to sue transfers to the Insurer. In conventional loss insurance, finding out which third party caused the loss is not difficult, because when the risk occurs, it can be immediately known to the Insured. However, the problem becomes different when the insurance object is a cyber insurance object, namely in the form of cyber security risk. The whereabouts of third parties who cause losses are often difficult to know. Even if it is known but is outside Indonesian jurisdiction, then this will create difficulties for the implementation of subrogation rights.

Therefore, it is necessary to find a solution on how to resolve this legal problem. In this case, state involvement is needed to help with this problem. Referring to various laws and regulations that regulate cyber data security, including Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE), Law Number 27 of 2022 concerning Protection Personal Data (PDP Law), Presidential Regulation of the Republic of Indonesia Number 47 of 2023 concerning National Cyber Security Strategy and Cyber Crisis Management (PP 47/2023). These three laws and regulations only regulate the protection of legal objects and subjects related to data security, but do not regulate how to assist insurance companies in implementing subrogation rights.

D. CONCLUSIONS AND RECOMMENDATIONS

Based on the description above, it can be concluded that the implementation of insurance agreements in cyber insurance is carried out based on the principles of insurance agreements. The implementation of an insurance agreement cannot be carried out or

[46] Heath, B. (2018). Before the breach: The role of cyber insurance in incentivizing data security. In George Washington Law Review (Vol. 86, Issue 4).

implemented if there has not been a risk to the Insured, but it can only be implemented when something occurs that causes a loss or the risk of an event occurring that causes a loss to the Insured. The implementation of cyber insurance agreements must be based on the principles of utmost good faith, indemnity and subrogation. Related to good faith, the agreement must be implemented in good faith by both parties. The implementation of the principle of utmost good faith is not absolutely only imposed on the Insured but is also intended or becomes a burden on the Insurer. The principle of indemnity provides a guideline or measure, namely that compensation must be truly in accordance with the true value of the object that suffered loss. The principle of indemnity with the principle of interest only applies to insurance that has interests that can be valued in money, so that the implementation of the principle of indemnity in cyber insurance practices related to cyber risks that occur which cause losses in terms of damage or loss of data must be calculated in money. Determining the true value of losses related to damage or loss of data is a challenge in the cyber insurance industry. Meanwhile, the implementation of the subrogation principle is always related to the principle of indemnity or the principle of balance, namely that compensation must be in accordance with or balanced with the actual value of the loss. In insurance law, the principle of indemnity states that the insured is entitled to full compensation for their losses, no more or less. When the Insurer has provided compensation to the Insured, then the right of subrogation arises, namely the transfer of the right to sue from the Insured to the Insurer to claim compensation from a third party.

Despite the huge opportunities in the cyber insurance industry, there are also obstacles, namely the lack of specific and comprehensive regulations regarding cyber insurance, which means that the implementation of cyber insurance law in Indonesia is still limited. The gap between regulations and practice in the field is also an obstacle in implementing cyber insurance. Implementing the principle of indemnity in insurance agreements when a risk occurs that causes losses in cyber insurance can encounter obstacles when submitting a claim. Inhibiting factors include the difficulty of determining the actual value of losses accurately. This is understandable considering that the insurance object that is covered is data in a computer system. Therefore, special expertise is needed to be able to analyze objects that are at risk of damage or loss of data due to cyber-attacks. Meanwhile, the factor that hinders the implementation of subrogation is that the whereabouts of third parties who cause losses are often difficult to know. Even if it is known but is outside Indonesian jurisdiction, then this will create difficulties for the implementation of subrogation rights. In order to manage cyber risks related to the implementation of insurance

agreements based on insurance principles, it is necessary to create laws and regulations that specifically regulate the cyber insurance industry. If there are obstacles in implementing agreements based on insurance principles, the presence of the state is required, namely encouraging the state to be actively involved in risk mitigation, especially through the implementation of subrogation by making procedures and provisions formulated in statutory regulations. This effort will have a positive impact, namely creating an increasingly advanced and developing business climate, especially in the cyber insurance industry.

REFERENCES / BIBLIOGRAPHY :

Book:

A. Junaedy Ganie, Hukum Asuransi Indonesia, Sinar Grafika, Jakarta, 2011
Abbas Salim, Asuransi dan Manajemen Risiko, RajaGrafindo Persada, Jakarta, 2007
Abdul Kadir Muhammad, Hukum Asuransi Indonesia, Citra Aditya bakti, Bandung, 2006
Agus Yudha Hernoko, *Hukum Perjanjian Asas Proporsionalitas Dalam Kontrak Komersial*, Cet ke-2, Kencana Prenadamedia Group, Jakarta, 2011
Elsi Kartika Sari dan Advendi Simangunsong, Hukum Dalam Ekonomi, Cetakan kelima (edisi 2), PT. Grasindo, Jakarta, 2008
Emmy Pangaribuan Simanjutak, dalam Ridwan Khairandy, Pengantar Hukum Dagang, FH UII Press, Yogyakarta, 2006
H. Gunanto dalam Ridwan Khairandy, Pengantar Hukum Dagang, FH UII Press, Yogyakarta, 2006
Kaelan, Metodologi Kualitatif Bidang Filsafat, Paradigma, Yogyakarta, 2005
Muhammad Teguh, Metode Penelitian Ekonomi; Teori dan Aplikasi, PT. Raja Grafindo Persada, Jakarta, 1999
Mukti Fajar ND dan Yulianto Achmad, *Dualisme Penelitian Hukum Normatif & Empiris*, Pustaka Pelajar, Yogyakarta, 2010
Mulhadi, *Dasar-Dasar Hukum Asuransi*, PT. RajaGrafindo Persada, 2017
Sentosa Sembiring, Hukum Asuransi, Nuansa Aulia, Bandung, 2014
Sri Redjeki Hartono dalam Ridwan Khairandy, Pengantar Hukum Dagang, FH UII Press, Yogyakarta, 2006

Journal:

B. Parera, A., & Tumanggor, M. S. (2021). Application Of Business Principles Insurance In Indonesia. Journal of Law, Politic and Humanities, 2(1). https://doi.org/10.38035/jlph.v2i1.49
Bencsik, A., Hargitai, D. M., & Kulachinskaya, A. (2022). Trust in and Risk of Technology in Organizational Digitalization. Risks, 10(5). https://doi.org/10.3390/risks10050090
Bhadra, O., Sahoo, S., Kumar, C. M., & Halder, R. (2022). Decentralized Insurance Subrogation Using Blockchain. ACM International Conference Proceeding Series. https://doi.org/10.1145/3581971.3581972
Bolot, J., & Lelarge, M. (n.d.). Cyber Insurance as an Incentive for Internet Security.

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: a systematic review of data availability. Geneva Papers on Risk and Insurance: Issues and Practice, 47(3), 698–736. https://doi.org/10.1057/s41288-022-00266-6

Dimov, T. (2018). SUBROGATION IN INSURANCE CONTRACT. Knowledge International Journal, 28(6). https://doi.org/10.35120/kij28061985t

Eling, M., & Jung, K. (2022). Heterogeneity in cyber loss severity and its impact on cyber risk measurement. Risk Management, 24(4). https://doi.org/10.1057/s41283-022-00095-w

Erniwati, S., & Kurnia, N. (2015). An Analysis of Information Technology on Data Processing by using Cobit Framework. International Journal of Advanced Computer Science and Applications, 6(9). https://doi.org/10.14569/ijacsa.2015.060920

Ginders, K. (2016). Insurance Law and the Principle of Indemnity in Light of Ridgecrest NZ Ltd v IAG New Zealand Ltd. Victoria University of Wellington Law Review, 47(1). https://doi.org/10.26686/vuwlr.v47i1.4879

Hatzivasilis, G., Chatziadam, P., Petroulakis, N., Ioannidis, S., Mangini, M., Kloukinas, C., Yautsiukhin, A., Antoniou, M., Katehakis, D. G., & Panayiotou, M. (2019). Cyber insurance of information systems: Security and privacy cyber insurance contracts for ICT and helathcare organizations. IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks, CAMAD, 2019-September. https://doi.org/10.1109/CAMAD.2019.8858165.

Heath, B. (2018). Before the breach: The role of cyber insurance in incentivizing data security. In George Washington Law Review (Vol. 86, Issue 4).

Januarita, R., Alamsyah, I. F., & Perdana, A. (2024). Guardians of data: TruMe Life's continuous quest for data protection. Journal of Information Technology Teaching Cases. https://doi.org/10.1177/20438869241242141.

Lubin, A. (2021). INSURING EVOLVING TECHNOLOGY. CONNECTICUT INSURANCE LAW JOURNAL, 28(1).

Mustafina, A. A., Kaigorodova, G. N., Alyakina, P. D., Velichko, N. Y., & Zainullina, M. R. (2020). Digital technology in insurance. Advances in Intelligent Systems and Computing, 908. https://doi.org/10.1007/978-3-030-11367-4_65

Rahmawati, C. (2020, November). Tantangan dan Ancaman Keamanan Siber Indonesia di Era Revolusi Industri 4.0. In *Prosiding Seminar Nasional Sains Teknologi dan Inovasi Indonesia (SENASTINDO)* (Vol. 2, pp. 299-306).

Sabrie, H. Y., & Amalia, R. (2015). Karakteristik Hubungan Hukum Dalam Asuransi Jasaraharja Terhadap Klaim Korban Kecelakaan Angkutan Umum. Yuridika, 30(3), 387-406.

Strupczewski, G. (2021). Defining cyber risk. Safety Science, 135. https://doi.org/10.1016/j.ssci.2020.105143.

Sudarmadi, D. A., & Runturambi, A. J. S. (2019). Strategi Badan Siber dan Sandi Negara (BSSN) Dalam Menghadapi Ancaman Siber di Indonesia. Jurnal Kajian Stratejik Ketahanan Nasional, 2(2).

Syamsuddin, M., & Putri, C. S. (2022). Proteksi Hukum Bagi Pemegang Polis Asuransi Terhadap Pailitnya Perusahaan Asuransi. SALAM: Jurnal Sosial Dan Budaya Syar-i, 9(2). https://doi.org/10.15408/sjsbs.v9i2.25112

Talesh, S. A. (2018). Data Breach, Privacy, and Cyber Insurance: How Insurance Companies Act as "Compliance Managers" for Businesses. Law and Social Inquiry, 43(2). https://doi.org/10.1111/lsi.12303

Weir, T. (2012). Subrogation and indemnity. Cambridge Law Journal, 71(1). https://doi.org/10.1017/S0008197312000190

Zeller, G., & Scherer, M. (2022). A comprehensive model for cyber risk based on marked point processes and its application to insurance. European Actuarial Journal, 12(1). https://doi.org/10.1007/s13385-021-00290-1

Internet:

Agus Sofian Eka Hidayat, Cyber insurance di Era 4.0, Pentingkah, https://datapolis.id/asuransi-siber-di-era-4-0-pentingkah/, diakses tanggal 13 Juni 2024 pukul 19.15 wib).

Fitran Briliano (2022, Sept 22). Keamanan Siber, Urgensi di Tengah Transformasi Ekonomi Digital, https://www.idntimes.com/opinion/social/fw-rocket/urgensi-keamanan-siber-c1c2#:~:text=Menurut%20data%20dari%20Cybersecurity%20Ventures%2C%20diperkirakan%20pada%20tahun,triliun%20per%20tahun%20yang%20disebabkan%20oleh%20serangan%20siber, (diakses tanggal 12 Juni 2024 pukul: 19.48 wib).

IDC. (2021). Worldwide IT Spending Forecast. Retrieved from https://www.idc.com

Muh. Fajrul Falah (2023, May 5). Tren Risiko Cyber Insurance di 2023, https://mediaasuransinews.co.id/asuransi/tren-risiko-cyber-insurance-di-2023/. Diakses tanggal 02 April 2024, pukul 20.20 wib

Hanif Reyhan Ghifari, OJK: Akibat Kejahatan Siber, Dunia Rugi 8 T Dolar AS pada 2023, https://tirto.id/ojk-akibat-kejahatan-siber-dunia-rugi-8-t-dolar-as-pada-2023-gSPd, (diakses tanggal 4 Juni 2024 pukul 22.21 wib).

Laws and Regulations:

Law Number 40 of 2014 concerning Insurance

Commercial Code (KUHD/WvK).

Civil Code (KUHPerdata/BW).

Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions (UU ITE),

Law Number 27 of 2022 concerning Personal Data Protection (UU PDP)

Presidential Regulation of the Republic of Indonesia Number 47 of 2023 concerning the National Cyber Security Strategy and Cyber Crisis Management.

Regulation of the Financial Services Authority of the Republic of Indonesia Number 8 of 2024 concerning Insurance Products and Marketing Channels of Insurance Products

Financial Services Authority, Indonesian Insurance Roadmap 2023-2027, 2023.