JURNAL ILMIAH METADATA, E-ISSN :2723-7737, Vol.7 No.2
Edition May 2025, Published : 30-05-2025, Page: 277-292
DOI: 10.47652/metadata.v7i2.638

RISK MANAGEMENT STRATEGY TO REDUCE THE POTENTIAL FOR BUSINESS DISPUTES IN MSMES IN MEDAN CITY

By
Sarman Sinaga
Universitas Mandiri Bina Prestasi
Email : sarmansinaga17@gmail.com

ABSTRACT

This study examines the implementation of effective risk management strategies to minimize the potential for business disputes in Micro, Small, and Medium Enterprises in Medan City. This study analyzes various challenges faced by MSMEs, including limited capital, product quality issues, and lack of innovation and government support, which often trigger disputes. The methods used include qualitative descriptive analysis to identify the root of the problem and the formulation of strategic recommendations that are applicable to MSME actors in the region. A comprehensive literature review is the main foundation in identifying common dispute patterns and best risk management practices that have proven effective in the context of similar MSMEs. The implementation of this strategy is expected to strengthen the position of MSMEs in facing market dynamics and minimize losses due to unexpected business conflicts. This research is expected to be able to make a significant contribution to the development of an adaptive and proactive risk management framework, especially in an effort to prevent the escalation of disputes into litigation that is detrimental to MSME operations. Focusing on risk mitigation strategies, such as product diversification and quality improvement, is also crucial to minimize potential disputes in the future.

Keywords: Risk Management, Business Disputes, MSMEs, Medan City.

STRATEGI MANAJEMEN RISIKO UNTUK MENGURANGI POTENSI SENGKETA BISNIS PADA UMKM DI KOTA MEDAN

ABSTRAK

Penelitian ini mengkaji implementasi strategi manajemen risiko yang efektif untuk meminimalisir potensi sengketa bisnis pada Usaha Mikro, Kecil, dan Menengah di Kota Medan. Studi ini menganalisis berbagai tantangan yang dihadapi UMKM, termasuk keterbatasan modal, masalah kualitas produk, serta kurangnya inovasi dan dukungan pemerintah, yang seringkali menjadi pemicu sengketa. Metode yang digunakan meliputi analisis deskriptif kualitatif untuk mengidentifikasi akar permasalahan dan perumusan rekomendasi strategis yang aplikatif bagi pelaku UMKM di wilayah tersebut. Studi literatur yang komprehensif menjadi landasan utama dalam mengidentifikasi pola sengketa umum dan

JURNAL ILMIAH METADATA, E-ISSN :2723-7737, Vol.7 No.2
Edition May 2025, Published : 30-05-2025, Page: 277-292
DOI: 10.47652/metadata.v7i2.638

praktik manajemen risiko terbaik yang telah terbukti efektif dalam konteks UMKM serupa. Penerapan strategi ini diharapkan dapat memperkuat posisi UMKM dalam menghadapi dinamika pasar dan meminimalkan kerugian akibat konflik bisnis yang tidak terduga. Penelitian ini diharapkan mampu memberikan kontribusi signifikan dalam pengembangan kerangka kerja manajemen risiko yang adaptif dan proaktif, khususnya dalam upaya mencegah eskalasi sengketa menjadi litigasi yang merugikan operasional UMKM. Fokus pada strategi mitigasi risiko, seperti diversifikasi produk dan peningkatan kualitas, juga sangat penting untuk meminimalkan potensi sengketa di masa depan.

Kata Kunci: Manajemen Risiko, Sengketa Bisnis, UMKM, Kota Medan.

INTRODUCTION

Micro, Small, and Medium Enterprises play a crucial role as the backbone of the national economy, including in the city of Medan, with a significant contribution to labor absorption and an increase in gross domestic product (Sahputra et al., 2021). The MSME sector has proven to be resilient in facing economic crises, even becoming a catalyst for the community's economy in the midst of a global pandemic (Isalman et al., 2022). However, despite having resilience, MSMEs remain vulnerable to various risks that have the potential to trigger business disputes, especially in uncertain economic conditions such as during the recession due to COVID-19 which caused negative economic growth in Q2 and Q3 2020 (Mardanugraha & Akhmad, 2023). This condition highlights the urgency of implementing a comprehensive risk management strategy to minimize potential conflicts and ensure the sustainability of MSME operations in the midst of fluctuating market dynamics (Rengganawati & Taufik, 2020).

The decline in sales of MSME products in Medan City by up to 68% caused by barriers to raw material supply and distribution, as well as capital difficulties, further emphasizes the need for effective business strategy adaptation (Sahputra et al., 2021). Despite this, MSMEs are often faced with limitations in knowledge about marketing strategies, low digital literacy, and difficulties in accessing technology, which collectively increase their vulnerability to commercial disputes (Yunianto & Taryadi, 2022) (Isalman et al., 2022). The multi-dimensional crisis that has occurred many times has proven that MSMEs are the savior of the nation's economy, even though the COVID-19 pandemic has had a much heavier impact than the

JURNAL ILMIAH METADATA, E-ISSN :2723-7737, Vol.7 No.2
Edition May 2025, Published : 30-05-2025, Page: 277-292
DOI: 10.47652/metadata.v7i2.638

previous crisis (Retnawati et al., 2020). However, the pandemic period can also be seen as an opportunity for MSMEs to evaluate performance and formulate new strategies to maintain business sustainability (Haryanto et al., 2022). Based on the survey, as many as 88% of micro businesses experienced a lack of cash and more than 60% reduced their workforce due to the impact of the pandemic, which shows that many MSMEs are unable to pay their employees' salaries and are forced to lay them off (Siska & Prapto, 2021) (Diah et al., 2021).

This condition highlights the need for MSMEs to adopt a proactive approach in risk management to identify, analyze, and mitigate potential disputes that can hinder the growth and sustainability of their businesses (Siska & Prapto, 2021). Digital transformation is crucial in facing this challenge, allowing MSMEs to gain a better understanding of consumer preferences and behaviors, so that marketing activities can be more targeted and efficient (Pramesti et al., 2021). The use of information technology and the adoption of digital marketing are increasingly essential for MSMEs to remain competitive and adaptive to market changes, while reducing the risk of disputes arising from economic uncertainty (Santi et al., 2024). The increased use of digital platforms and social media has become an adaptive solution for MSMEs in reaching consumers quickly and consistently during the pandemic, requiring them to be technologically literate and innovate in marketing techniques (Harini et al., 2022) (Anggraini et al., 2022). Therefore, MSMEs need to implement effective digital marketing strategies to expand market reach and increase sales, while minimizing potential disputes related to promotion and distribution (Haryanto et al., 2022) (Syukri & Sunrawali, 2022).

Digital marketing offers a wider reach and lower costs than traditional marketing methods, allowing MSMEs to survive and even thrive in the midst of a crisis (Wicaksono, 2023). This strategy includes optimizing the role of digital marketing through social media platforms such as Facebook and Instagram, which have been proven to significantly increase transactions and sales of MSME products (Anggraini et al., 2022). The use of social media has become a strategic alternative for MSMEs to strengthen their market position and reduce potential disputes arising from the limitations of conventional promotions (Endarwati et al., 2022). Digital marketing includes the use of the internet and supporting applications to create a wide network, which plays an important role in consumer purchasing decisions (Putri &

JURNAL ILMIAH METADATA, E-ISSN :2723-7737, Vol.7 No.2
Edition May 2025, Published : 30-05-2025, Page: 277-292
DOI: 10.47652/metadata.v7i2.638

Sulaeman, 2022). The importance of digital literacy and the ability to adapt to changes in consumer behavior in the digital ecosystem are determining factors for the success of MSMEs in reducing the risk of disputes in this era (Fuadi et al., 2021). The ability of MSMEs to utilize digital marketing can help them achieve sales targets, thereby minimizing the risk of disputes (Siska & Prapto, 2021).

Digital marketing, or _digital marketing_, has evolved to become a fundamental element in modern business strategies, allowing businesses to reach a wide audience through various online channels (Priatama et al., 2021). This approach not only optimizes the visibility of products and services, but also opens up new opportunities for direct interaction with consumers, which in turn can reduce the potential for misunderstandings that lead to disputes (Faradila, 2023). The use of social media as a means of promotion and marketing communication has been proven to be effective in increasing the brand awareness of MSME products, allowing them to compete with larger business entities (Wulandari & Supratman, 2018). The use of social media has become a strategic alternative for MSMEs to strengthen their market position and reduce potential disputes arising from the limitations of conventional promotions (Endarwati et al., 2022). Digital marketing optimization also requires a deep understanding of consumer behavior and market trends to ensure that the strategies implemented are relevant and effective, thereby narrowing the gap in disputes related to customer expectations (Sinaga et al., 2021). The proportion of MSMEs that use online sales is still relatively low because many do not technically understand online sales procedures, so training and skill development in digital marketing are essential to overcome this barrier (Nasution et al., 2022). This training can include improving the competence of human resources in the digital era, which is crucial to improve the quality and competitiveness of local businesses (Hamsal et al., 2024).

LITERATURE REVIEW

This review will explore in depth the concept of risk management, identify different types of business disputes relevant to the context of MSMEs, as well as analyze the regulatory framework, including the important role of the Electronic Information and Transaction Law, in

JURNAL ILMIAH METADATA, E-ISSN :2723-7737, Vol.7 No.2
Edition May 2025, Published : 30-05-2025, Page: 277-292
DOI: 10.47652/metadata.v7i2.638

legal risk mitigation and personal data protection (Aprilianti, 2025) (Lubis, 2024). Legal protection for consumers is also guaranteed by the use of regulations related to electronic commerce, both through litigation and non-litigation channels (Ramli et al., 2020). Further discussions will include practical strategies that MSMEs can implement to minimize potential disputes, such as the implementation of clear contracts and alternative dispute resolution mechanisms, in line with the principle of prudence in daily business operations. This review will also discuss how innovation and adoption of digital technology can support MSMEs in building operational resilience and reducing vulnerability to disputes, especially those related to increasingly sophisticated cybercrime (Lubis, 2024).

The importance of a comprehensive legal framework, as stipulated in the Criminal Code, is increasingly relevant to face the rapidly growing challenges of cybercrime, including in the context of protecting MSMEs from various forms of digital violations and disputes (Lubis, 2024). In line with the rapid development of information technology, digitalization has penetrated all fields, including the business sector, providing significant convenience in the dynamics of fast-paced communication and information (Ramli et al., 2020). Cybercrime, such as personal data misuse, online fraud, and defamation, has become a serious threat that requires strict regulations to protect MSME actors from financial and reputational losses (Lubis, 2024). This rampant cybercrime phenomenon highlights the importance of digital literacy and understanding of regulations such as the ITE Law as the main prevention tool (Aprilianti, 2025). In addition, regulations related to consumer protection in electronic commerce transactions still need to be improved, considering that their implementation is not optimal and is still spread across various laws that require further implementation regulations (Putri, 2022). In line with these dynamics, the existing legal framework, including the Consumer Protection Law, has not been fully able to comprehensively adapt consumer protection in digital transactions, particularly in cases involving cross-border jurisdictions (Putri, 2022) (Fista et al., 2023).

Therefore, a review of the effectiveness of existing protection laws as well as recommendations for a robust consumer protection framework in the digital age is needed (Rahman et al., 2023). In this context, it is important to discuss various forms of disputes that

JURNAL ILMIAH METADATA, E-ISSN :2723-7737, Vol.7 No.2
Edition May 2025, Published : 30-05-2025, Page: 277-292
DOI: 10.47652/metadata.v7i2.638

may arise, including those related to consumer protection in e-commerce that are still inadequate and potential fraud in buying and selling transactions (Sudarmanto, 2020). Existing regulations, such as the Criminal Code, have provided a strong basis for cracking down on various forms of crime, including cybercrime, but their implementation still faces challenges in terms of adapting to the evolving modus operandi (Lubis, 2024). Although the ITE Law has provided a significant initial legal framework, its implementation still needs improvement to ensure fairness and effectiveness, especially in addressing the multi-interpretation articles known as "rubber articles" (Aprilianti, 2025).

This indicates the need for continuous regulatory updates and harmonization between various existing regulations in order to accommodate the complexity of digital transactions and provide optimal protection for MSMEs and consumers (Atsetya et al., 2020) (Bintarawati, 2022). The sustainable development of law, along with the evolution of society, requires dynamic regulatory adaptation to function as an instrument of social engineering, especially in the context of rapid modernization, to always be relevant to the times (Rinaldi et al., 2023). The review will also discuss how innovation and adoption of digital technology can support MSMEs in building operational resilience and reducing vulnerability to disputes, especially those related to increasingly sophisticated cybercrime. It is important to underline that although the Criminal Code and the ITE Law provide a legal basis, jurisdictional challenges often arise, especially if the perpetrator is abroad while the victim is in Indonesia, which makes it difficult to enforce the law without a mutual assistance agreement (Lubis, 2024). However, regulations related to consumer protection in Indonesia, especially in the context of e-commerce, are still inadequate and are often faced with divergent interpretations, especially in distinguishing between constructive criticism and defamation that can lead to legal disputes (Siregar, n.d.).

In addition, despite regulatory efforts, challenges such as asymmetric information, lack of supervision, and the protection of consumers' personal data are still crucial issues in online transactions (Romdoni, 2024). This ambiguity is often exacerbated by the existence of multi-interpretation articles in the ITE Law that have the potential to be a tool of criminalization, especially Article 27 paragraph regarding defamation, which has triggered calls for revision from various circles (Muldani, 2022) (Siregar, n.d.) (Suliyono, 2022). This ambiguity of

JURNAL ILMIAH METADATA, E-ISSN :2723-7737, Vol.7 No.2
Edition May 2025, Published : 30-05-2025, Page: 277-292
DOI: 10.47652/metadata.v7i2.638

interpretation not only hinders consistent law enforcement, but can also create uncertainty for micro, small, and medium enterprises as well as consumers (Siregar, n.d.) (Limilia & Fuady, 2021). Therefore, the urgency to revise and harmonize various related regulations, including a comprehensive revision of the ITE Law, is crucial to create a legal ecosystem that is fairer and adaptive to the development of digital technology (Limilia & Fuady, 2021) (Atsetya et al., 2020). The Indonesian government has taken significant steps in strengthening the legal and institutional framework to address these challenges, including the establishment of the State Cyber and Cryptography Agency (Lubis, 2024).

This step shows a commitment to improving cybersecurity and protecting various parties, including MSMEs, from evolving digital threats. Consumer protection in electronic transactions is becoming increasingly important considering the rapid development of e-commerce in Indonesia, which is supported by regulations such as Law Number 8 of 1999 concerning Consumer Protection and Government Regulation Number 80 of 2019 concerning Trade Through Electronic Systems (Romdoni, 2024). However, the current regulations are not fully able to provide optimal protection for consumers in cross-border e-commerce transactions, considering the weak bargaining position of consumers in this context (Sugianto et al., 2021). Therefore, an in-depth study is needed on the effectiveness of the implementation of this regulation and the identification of legal loopholes that need to be followed up to provide a stronger guarantee of protection for consumers and MSME actors (Romdoni, 2024). This is crucial considering that digital business innovations, such as e-commerce, have changed the transaction landscape from conventional to virtual, requiring a continuous adaptation of the legal framework (Ramli et al., 2021).

Thus, a holistic approach that includes regulatory revisions, law enforcement capacity building, and public education is needed to mitigate the risk of disputes and foster a safe business environment for MSMEs in the digital era (Suliyono, 2022). In this context, the ITE Law, although it provides a legal basis for consumer protection in electronic transactions, still leaves homework related to aspects of jurisdiction and law enforcement against foreign entities operating in the Indonesian digital realm (Astuti & Atmojo, 2022). On the other hand, there is no clarity on business license obligations for online business actors, which can hinder

JURNAL ILMIAH METADATA, E-ISSN :2723-7737, Vol.7 No.2
Edition May 2025, Published : 30-05-2025, Page: 277-292
DOI: 10.47652/metadata.v7i2.638

government supervision of community activities and consumer protection (Yulianita, 2020). This ambiguity is exacerbated by the difficulty in proving product defects or non-conformities of the goods received by the buyer, as in the case of returns on e-commerce platforms, where buyers can often only document the condition of the goods when they were received as preliminary evidence (Vera, 2021). Therefore, the urgency to revise and harmonize various related regulations, including a comprehensive revision of the ITE Law, is crucial to create a legal ecosystem that is more equitable and adaptive to the development of digital technology (Siregar, n.d.). This is in line with Article 15 paragraph of the UUITE which mandates every electronic system operator to ensure reliable and safe system operations, as well as be responsible for any disruption that occurs (Fauzi & Ansari, 2020). Existing regulations also need to be strengthened to move from the principle of _caveat emptor_ (responsible buyers) to _caveat venditor_ (responsible sellers), in order to ensure more comprehensive consumer protection in online transactions (Ramli et al., 2021).

The principle of absolute responsibility for business actors, as stipulated in the Consumer Protection Law No. 8 of 1999, is crucial to ensure that consumers are not burdened with proving the wrongdoing of business actors (Eleanora, 2018). The application of this principle is expected to increase the accountability of business actors and balance the legal position between consumers and producers in electronic transactions, especially those involving digital products or services (Kesuma & Triputra, 2020). The implementation of the ITE Law shows that although most students are aware of its existence, an in-depth understanding of its content is still limited, which correlates with high rates of cyberbullying and shows the importance of more effective legal education (Siregar, n.d.). Increasing legal awareness, especially regarding the Electronic Information and Transaction Law, is very important because the low understanding of the public, including students, can contribute to an increase in cases of cybercrime such as cyberbullying (Elizamiharti et al., 2019) (Siregar, n.d.).

Therefore, the improvement of the educational curriculum, especially in courses related to professional ethics and cyber law, is essential to increase digital legal literacy among the younger generation (Elizamiharti et al., 2019). Expanding the scope of education not only among students, but also for MSME actors, will strengthen their understanding of rights and

JURNAL ILMIAH METADATA, E-ISSN :2723-7737, Vol.7 No.2
Edition May 2025, Published : 30-05-2025, Page: 277-292
DOI: 10.47652/metadata.v7i2.638

obligations in the digital realm, as well as help them identify and mitigate the risk of disputes that may arise (Siregar, n.d.). Regulations related to personal data protection, as stipulated in Article 26 paragraph of Law of the Republic of Indonesia Number 19 of 2016, also require special attention to ensure that consumer data is safe from misuse by irresponsible parties (Rahmi, 2020). The strengthening of the personal data legal framework also includes regulations related to data collection, storage, and use, as highlighted in comparison with the legal framework for personal data in Singapore and the European Union, which shows the urgency of harmonization and legal reform in Indonesia (Anggraeni, 2018).

In addition, Law Number 10 of 1998 concerning Banking and Law Number 19 of 2016 concerning Information and Electronic Transactions, as well as Law Number 8 of 1999 concerning Consumer Protection, play an important role in providing a legal framework to ensure the security of electronic banking transactions and customer protection (Fauziah & Apriani, 2021). The importance of this education is also relevant to the existence of a legal basis for electronic contracts that are still not formally regulated, thus strengthening the urgency of understanding the underlying law of the applicable agreement (Sulistyowati et al., 2020). This regulatory update must also include legal protection for digital consumers who are vulnerable to data abuse and increasingly sophisticated cybercrime (Sulistyowati et al., 2020) (Hanafiah, 2022). Cybercrime, including online fraud and identity theft, continues to increase along with the development of technology and increasingly widespread connectivity (Lubis, 2024).

METHODOLOGY

Cybercrime threats such as phishing, malware, and online fraud are significant risks that can have a serious impact on the security, privacy, and well-being of individuals, so it is important to understand the tactics of cybercriminals and implement strong digital security practices (Butarbutar, 2023). The increase in cases of online fraud and narcotics-related crimes, such as the one in Indonesia, shows the need for a more adaptive legal framework and stricter enforcement to address the ever-evolving modus operandi (Lubis, 2024). Cybercrime, particularly online fraud and e-commerce fraud, is a growing concern, especially those

JURNAL ILMIAH METADATA, E-ISSN :2723-7737, Vol.7 No.2
Edition May 2025, Published : 30-05-2025, Page: 277-292
DOI: 10.47652/metadata.v7i2.638

targeting individuals through online platforms (Lubis, 2024). However, digital banking service innovations also increase the risks faced by banks and customers, requiring comprehensive legal protection (Tarigan & Paulus, 2019). Legal protection for customers in digital banking services is regulated by OJK Regulation No. 12/POJK.03/2018, which functions as a preventive measure in maintaining customer security (Tarigan & Paulus, 2019).

However, the dynamics of law enforcement in Indonesia are often faced with limited resources, training, and inter-agency coordination, which can hinder the effectiveness of handling cybercrime cases and business disputes (Lubis, 2024). These limitations include the lack of comprehensive regulations related to digital banking, especially for Islamic banking, as well as the lack of strong regulations such as laws to regulate digital banking transactions as a whole (Amrillah, 2020). This approach needs to be strengthened with recent case analysis to identify evolving cybercrime patterns and effective legal responses (Lubis, 2024). The government, legal institutions, and the community must work together to create a transparent and effective legal system in eradicating cybercrime (Lubis, 2024). In addition, increasingly complex cybercrimes, such as the use of computers and internet networks for illegal purposes such as fraud, intellectual property theft, and privacy violations, require a more sophisticated and adaptive legal response (Idellie & Atok, 2023).

Improving the protection of MSME data and digital assets through a comprehensive approach to cybersecurity, including post-pandemic threat detection and mitigation, is a strategic imperative to minimize losses due to cybercrime (Herdiana et al., 2021). The impact of these cybercrimes is not only limited to financial losses, but can also damage the public's reputation and trust in business entities and financial institutions (Chintia et al., 2019). The threat of cybercrime has grown significantly, encompassing various forms of crime that utilize information technology for illegal purposes (Dermawan et al., 2023). Digital transformation in the banking sector, including Islamic banking, also brings new challenges related to cybersecurity and customer data protection, which demands the development of adaptive risk management strategies (Susanti, 2024). An effective risk management strategy must consider technical, legal, and operational dimensions to ensure comprehensive protection of digital assets and sensitive information (Dermawan et al., 2023).

JURNAL ILMIAH METADATA, E-ISSN :2723-7737, Vol.7 No.2
Edition May 2025, Published : 30-05-2025, Page: 277-292
DOI: 10.47652/metadata.v7i2.638

RESULT & DISCUSSION

The significant increase in global network penetration and advances in mobile internet in Indonesia have increased the vulnerability of organizational information security to cyber threats (Islami, 2018). Cyberattacks, such as the WannaCry ransomware case in 2017 that paralyzed companies and hospitals in more than 150 countries including Indonesia, highlight the urgency of cybersecurity challenges for policymakers in the information age (Islami, 2018). Modern cybercrime not only includes acts of hacking and digital fraud, but also involves the extension of traditional criminal behaviors adapted into the digital realm, such as theft, fraud, money laundering, and illegal trading conducted online (Idellie & Atok, 2023). The use of information technology for cybercrime, both as a tool and a target, is increasingly prevalent and raises pros and cons related to increasing the ease of access to technology (Chintia et al., 2019). Cybersecurity challenges in Indonesia are exacerbated by a lack of national commitment, as reflected in the 2017 Global Cybersecurity Index assessment which placed Indonesia at a low rank (Islami, 2018). The protection of personal data is crucial in digital health administration, given the sensitivity of patient information and the potential for large losses due to security breaches and data leaks (Fauzi et al., 2024).

This issue is exacerbated by the lack of public understanding of cyber risks and how to mitigate them, as well as the uneven availability of information technology infrastructure, especially in remote areas (Chintia et al., 2019). This phenomenon shows that despite efforts to raise awareness, there are still many loopholes that can be exploited by irresponsible parties, especially in the context of the exploitation of sensitive data for personal or group gain (Nova et al., 2022). The increase in the number of internet users also indirectly increases threats in cyberspace, which makes cybersecurity a crucial solution to maintain the confidentiality, integrity, and availability of information (Budiman, 2022). This cross-border cybercrime threat requires international cooperation and the adoption of global security standards to create a safer and more reliable digital ecosystem (Lubis, 2024). The Government of Indonesia has initiated a national cybersecurity strategy and implemented short- and long-term programs, but there are still challenges and obstacles in its implementation, especially in terms of human resources, procedures, and prevention policies (Islami, 2018). This comprehensive approach requires

JURNAL ILMIAH METADATA, E-ISSN :2723-7737, Vol.7 No.2
Edition May 2025, Published : 30-05-2025, Page: 277-292
DOI: 10.47652/metadata.v7i2.638

synchronization between adaptive regulations, the development of qualified human resource capacity in the field of cybersecurity, and increased public awareness of digital risks (Abdillah et al., 2021).

In this context, the formation of coordinated and systematically integrated policies is very crucial, considering that cyber defense efforts in Indonesia have not yet become a coordinated national initiative, but are still sectoral and depend on the interests and capabilities of each entity (Rizal & Yani, 2016). The importance of defining national vital infrastructure in Indonesia is becoming increasingly urgent in dealing with defense and security threats in the cyber domain, considering the high dependence of a country on information and communication technology (Setiyawan, 2019). Evolving cyber threats also include risks to the manufacturing industry that adopts new technologies without adequate safeguards, creating increased danger and targeting sabotage of industrial entities (Simorangkir, 2021). Cybercrime that is transnational in nature has caused significant economic and social losses, demanding adaptive and proactive legal responses to address its complexity (Lubis, 2024). Cyber terrorism, which has the potential to damage vital public service facilities, requires cyber counter-terrorism capabilities through cyber patrol, deterrence, enforcement, and surveillance (Threat et al., 2021). Therefore, a comprehensive strategy is needed that includes the formation of special cyber forces to deal with increasingly real cyber wars (Hasan, 2022), as well as improving national cybersecurity policies to protect state sovereignty from military and non-military threats (Rizal & Yani, 2016).

The initiative to establish the State Cyber and Cryptography Agency in 2017 is a strategic step by the Indonesian government in building national cyber defense capabilities, although its implementation still faces various obstacles in efforts to strengthen capacity and cross-sector coordination (Lubis, 2024) (Aji, 2023). The Indonesian government needs to reconsider the most appropriate defense strategy to deal with non-military threats in the modern era, including through the formation of a reserve component that has qualified capabilities in defending the country as a supporting element of the main defense force (Indrawan & Efriza, 2018). The use of cyber technology as a military and strategic tool shows a shift in the dimension of war from physical to non-physical, confirming the need for adaptation of national

JURNAL ILMIAH METADATA, E-ISSN :2723-7737, Vol.7 No.2
Edition May 2025, Published : 30-05-2025, Page: 277-292
DOI: 10.47652/metadata.v7i2.638

security strategies ("Cyber Security Risk Analysis in the Digital Transformation of Public Services in Indonesia," 2023). The importance of creating a cyber defense force is crucial in dealing with the threat of cyber warfare in this technological era, which requires an effective strategy from the Indonesian government (Candra et al., 2021). Increasing public legal awareness of potential cyber risks and the legal consequences of data breaches is an important element in a cyber defense strategy (Lubis, 2024). The government can also strengthen prevention strategies through public education on the Electronic Information and Transaction Law to increase understanding of the limits on the responsible use of digital technology (Siregar, n.d.). The aspect of state defense is an essential factor in maintaining the sustainability of a country from various threats, both internal and external, including cyber threats that continue to increase (Mahira et al., 2020). This education can include increasing digital literacy, strengthening internal policies, awareness campaigns, and empowering complaint services for cyber-related cases (Siregar, n.d.).

Increasing public understanding of the Electronic Information and Transaction Law is crucial in preventing cyberbullying, especially among students who are vulnerable to cases of online gender-based violence (Siregar, n.d.). National cyber capacity building through cooperation with other countries, as has been done in strengthening military resilience (Hikmawati, 2023), can be a strategic step to adopt the latest best practices and technologies in dealing with cyberattacks. This approach is in line with the need to change Indonesia's defense paradigm from relying only on the Indonesian National Army as the main force to involving a competent reserve component in defending the country, especially in dealing with non-military threats (Indrawan & Efriza, 2018). This strategy underscores the importance of synergy between military and civilian aspects in building national cyber resilience that is adaptive to global threat dynamics (Indrawan & Efriza, 2018). This strategy includes efforts to establish a safe and trusted reporting center, as well as tighten oversight of negative content on digital platforms through collaboration with social media service providers (Siregar, n.d.).

National cyber capacity building requires the integration of various elements, including adaptive regulation, skilled human resource development, and strong cybersecurity infrastructure (Lubis, 2024). Risk mitigation efforts in countering cyber threats can be

JURNAL ILMIAH METADATA, E-ISSN :2723-7737, Vol.7 No.2
Edition May 2025, Published : 30-05-2025, Page: 277-292
DOI: 10.47652/metadata.v7i2.638

categorized into three main indicators, including prevention, identification, and remediation measures (Permana, 2021).

In line with technological developments and social dynamics, as well as increasing public education about their rights and obligations in the digital realm. This is crucial considering that the rapid development of information technology has raised new challenges in law enforcement, especially related to freedom of expression and the dissemination of information on social media, which sometimes causes unrest among the public (Kamalludin & Arief, 2019). The widespread use of digital technology, while bringing convenience and efficiency, has also created new loopholes for increasingly sophisticated cybercrime (Ramli et al., 2020). The existence of symptoms of a shift in social problems from the real world to the virtual world is shown by the phenomenon of cybercrime that is happening today (Rinaldi et al., 2023). The implications of multi-interpretation articles in the Electronic Information and Transaction Law often cause discomfort and concern in society, limiting freedom of expression and opinion due to the potential for criminalization (Suliyono, 2022).

This condition requires the government to continue to carry out legal reforms, especially in cyber law enforcement, to build public trust in the judicial system (Lubis, 2024). Cyberbullying, in particular, is one of the most prevalent forms of cybercrime, where these actions are deliberately carried out repeatedly through digital media to harm others, often without a face-to-face meeting between the perpetrator and the victim (Nugraha, 2022) (Rinaldi et al., 2023). These actions include ridicule, harassment, and degradation on social media, which can lead to serious repercussions for the victim, such as anxiety, depression, and even suicidal risk (Marlef et al., 2024). Although they do not know age limits, generally the perpetrators and victims of cyberbullying are teenagers who are still in the search for their identity and are vulnerable to the influence of the peer environment (Pakai, 2021) (Ruliyatin & Ridhowati, 2021). Character education mandated by Law Number 20 of 2003 concerning the National Education System is expected to form a strong personality that is able to overcome negative impacts, such as cyberbullying, as well as encourage responsible digital literacy (Pakai, 2021).

JURNAL ILMIAH METADATA, E-ISSN :2723-7737, Vol.7 No.2
Edition May 2025, Published : 30-05-2025, Page: 277-292
DOI: 10.47652/metadata.v7i2.638

CONCLUSION

This initiative is important given that cybercrime, such as online fraud, has different characteristics than conventional crimes, demanding a more adaptive legal approach and specific regulations (Hanafiah, 2022). The increase in global network penetration and advances in the mobile internet in Indonesia further increase the vulnerability of organizational information security to cyber threats, which is a major challenge for policymakers in the information age (Islami, 2018). A significant increase in cyberattacks has led to massive financial losses and damage to critical banking processes, highlighting the need for better cybersecurity preparedness and effective countermeasures (Dermawan et al., 2023). This is reinforced by reports that in May 2017, the WannaCry ransomware cyberattack disrupted the operations of companies and hospitals in more than 150 countries, including Indonesia, which underscores the need for global cooperation in cybersecurity (Islami, 2018). An effective risk management strategy should include the identification of diverse cyber threats, including data interruptions, interceptions, and modifications, as well as attacks such as intrusions and denials of service (Saputra et al., 2023). In addition, patient data security is a crucial issue in digital health administration, where privacy breaches and data leaks can threaten patient operations and safety (Fauzi et al., 2024).

BIBLIOGRAPHY

Abdillah, F., Suhadi, S., Tertia, C. P., Tarigan, A. R., Andri, A., & Fahrezi, F. (2021). Pemberdayaan Taman Baca Masyarakat dan Guru Sekolah Dasar dalam Menyiasati Pandemi Siber: Gotong Royong melalui Digital Civic Engagement. Publikasi Pendidikan, 11(2), 158. https://doi.org/10.26858/publikan.v11i2.16438

Aji, M. P. (2023). Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi) [Cyber Security System and Data Sovereignty in Indonesia in Political Economic Perspective]. Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional, 13(2), 222. https://doi.org/10.22212/jp.v13i2.3299

Akhmad, K. A., & Purnomo, S. (2021). PENGARUH PENERAPAN TEKNOLOGI INFORMASI PADA USAHA MIKRO KECIL DAN MENENGAH DI KOTA SURAKARTA. Sebatik, 25(1), 234. https://doi.org/10.46984/sebatik.v25i1.1293

JURNAL ILMIAH METADATA, E-ISSN :2723-7737, Vol.7 No.2
Edition May 2025, Published : 30-05-2025, Page: 277-292
DOI: 10.47652/metadata.v7i2.638

Ali, M. M. (2015). Determinants of Preventing Cyber Crime: a Survey Research. THE INTERNATIONAL JOURNAL OF MANAGEMENT SCIENCE AND BUSINESS ADMINISTRATION, 2(7), 16. https://doi.org/10.18775/ijmsba.1849-5664-5419.2014.27.1002

Amrillah, M. U. (2020). Urgensi Pembentukan Undang-Undang Digital Banking Bagi Perbankan Syariah Di Indonesia. Jurnal Lex Renaissance, 5(4). https://doi.org/10.20885/jlr.vol5.iss4.art12

Analisis Risiko Keamanan Siber dalam Transformasi Digital Pelayanan Publik di Indonesia. (2023). Jurnal Pewarta Indonesia, 6(2). https://doi.org/10.7454/jkskn.v6i2.10082

Ancaman, D., Media, T., Globalisasi, D., Syauqillah, M., Usman, A., Sukoco, A., & Siber, T. (2021). MEDIA, GLOBALISASI DAN ANCAMAN TERORISME. Journal of Terrorism Studies, 3(2). https://doi.org/10.7454/jts.v3i2.1039

Anggraeni, S. F. (2018). POLEMIK PENGATURAN KEPEMILIKAN DATA PRIBADI: URGENSI UNTUK HARMONISASI DAN REFORMASI HUKUM DI INDONESIA. Jurnal Hukum & Pembangunan, 48(4), 814. https://doi.org/10.21143/jhp.vol48.no4.1804

Anggraini, N. P. N., Rustiarini, N. W., & Satwam, I. K. S. B. (2022). OPTIMALISASI PEMASARAN DIGITAL BERBASIS MEDIA SOSIAL UNTUK MENINGKATKAN PENJUALAN UMKM. JMM (Jurnal Masyarakat Mandiri), 6(6), 4888. https://doi.org/10.31764/jmm.v6i6.11216

Angwaomaodoko, E. A. (2024). Cyberbullying: Legal and Ethical Implications, Challenges and Opportunities for Policy Development. International Journal of Innovative Science and Research Technology (IJISRT), 738. https://doi.org/10.38124/ijisrt/ijisrt24apr108

Anjani, N. (2021). Cybersecurity Protection in Indonesia. https://doi.org/10.35497/341779

Aprilianti, A. (2025). Efektivitas dan Implementasi Undang-Undang Informasi dan Transaksi Elektronik sebagai Hukum Siber di Indonesia: Tantangan dan Solusi. Begawan Abioso, 15(1), 41. https://doi.org/10.37893/abioso.v15i1.1002

Apriyanti, H. W. (2018). PERKEMBANGAN INDUSTRI PERBANKAN SYARIAH DI INDONESIA : ANALISIS PELUANG DAN TANTANGAN. MAKSIMUM, 8(1), 16. https://doi.org/10.26714/mki.8.1.2018.16-23

Astuti, N. K., & Atmojo, R. N. P. (2022). PERLINDUNGAN KONSUMEN ATAS RISIKO KEAMANAN INFORMASI DALAM TRANSAKSI E-COMMERCE. Honeste Vivere, 32(2), 98. https://doi.org/10.55809/hv.v32i2.135