Sosioedukasi
JURNAL ILMIAH ILMU PENDIDIKAN DAN SOSIAL
ISSN: 2086-6135 E-ISSN: 2541-612x
Volume 14 No. 4. Desember 2025 https://ejournal.unibabwi.ac.id/index.php/sosioedukasi/index

THE RELATIONSHIP BETWEEN STUDENTS' CYBERSECURITY COMPETENCE AND THE RISK OF PERSONAL DATA EXPLOITATION IN ONLINE LEARNING ENVIRONMENTS

Mesrawati Rifai[1a*], Regiena Sari[2b], Dessy Pramudiani[3c], Esther Hesline Palandi[4d], Iwan Sonjaya[5e]

[1] Universitas Islam DDI Abdurrahman Ambo Dalle
[2]Universitas Paramadina
[3]Universitas Jambi
[4]Politeknik Negeri Malang
[5]Politeknik Negeri Jakarta

[a]*E-mail:* mesrawatirifai@ddipolman.ac.id
[b]*E-mail:* mozanina2015@gmail.com
[c]*E-mail:* dessy.79_psikologi@unja.ac.id
[d]*E-mail:* esther_hesline@polinema.ac.id
[e]*E-mail:* iwan.sonjaya@tik.pnj.ac.id

(*) Corresponding Author
mesrawatirifai@ddipolman.ac.id

ARTICLE HISTORY
Received : 20-10-2025
Revised : 07-11-2025
Accepted : 20-01-2025

KEYWORDS
Cybersecurity Competence, Personal Data Exploitation, Online Learning Risks

ABSTRACT
This study examines the relationship between students' cybersecurity competence and the risk of personal data exploitation in online learning environments. As digital platforms become more integral to education, the research aims to explore how students' knowledge of cybersecurity influences their ability to protect personal information from online threats. Using a literature-based methodology, data was collected from academic journals, books, and studies related to cybersecurity and online learning. The findings show that students with higher cybersecurity competence are better at safeguarding their data, while those with lower knowledge are more vulnerable to exploitation. The study concludes that continuous cybersecurity education and institutional support are essential for enhancing students' data protection practices in online learning.

INTRODUCTIONS

In recent years, online learning has become a primary alternative in the global education system, particularly due to the COVID-19 pandemic, which forced the education sector to rapidly adapt to technological changes. While offering many conveniences, online learning also presents various challenges, especially related to the security of students' personal data. One of the main issues faced is the low level of cybersecurity competence among students,

Sosioedukasi
JURNAL ILMIAH ILMU PENDIDIKAN DAN SOSIAL
ISSN: 2086-6135 E-ISSN: 2541-612x
Volume 14 No. 4. Desember 2025 https://ejournal.unibabwi.ac.id/index.php/sosioedukasi/index

which poses a significant risk to the exploitation of their personal data. Students are often unaware of the importance of protecting their personal information while accessing online learning platforms. Given the large amount of personal data shared on online learning platforms, ranging from identity data to academic information, the risk of misuse or exploitation of this data is increasing. Therefore, it is essential to understand the relationship between students' cybersecurity competence and the potential for personal data exploitation in online learning environments(Burov et al., 2020).

Literature on cybersecurity in online education reveals that, although many studies highlight the importance of protecting personal data in cyberspace, there remains a significant gap in understanding the relationship between students' cybersecurity competence and the risk of data exploitation. Some studies suggest that increasing awareness of cyber threats can reduce the risk of data breaches (Hackbarth & Johnston, 2020), yet there is a lack of research directly linking students' cybersecurity competence to the protective actions they take in the context of online education. Existing cybersecurity theories, such as the Theory of Planned Behavior, suggest that data protection behavior is influenced by attitudes, social norms, and perceived control. However, how these concepts are applied in the context of online learning—especially among students with limited understanding of cyber threats—has not been thoroughly explored. As a result, there is a gap between existing theories and their practical application in the online learning environment, which is full of potential risks(Watini et al., 2024).

This study aims to identify the relationship between cybersecurity competence possessed by students and the risk of personal data exploitation in the context of online learning. By analyzing how students understand online threats and how they protect their personal data during online learning, this research seeks to provide a deeper understanding of the importance of cybersecurity competence in this context. The study also aims to examine the extent to which cybersecurity knowledge influences students' ability to avoid potential data exploitation. Furthermore, the research will identify the factors affecting students' cybersecurity competence and how they protect personal data when connecting to online learning platforms(Sadiqzade & Alisoy, 2025).

Based on the facts presented, this research is important because students' cybersecurity competence directly influences their vulnerability to personal data exploitation in online learning environments. Although there is growing awareness about the need for personal data protection, many students still lack sufficient knowledge about how to protect their personal information online. Therefore, this research tests the hypothesis that higher levels of cybersecurity competence among students can reduce the risk of personal data exploitation in online learning. The study also aims to demonstrate the importance of cybersecurity training or education within the curriculum to better equip students with the skills to protect their personal data in the digital world. By understanding this relationship, it is hoped that the research findings will provide recommendations for educational institutions to enhance their cybersecurity training programs for students, thereby reducing the risk of personal data breaches or misuse(Zorlu, 2023).

METHOD

Research Object

The research focuses on the challenges students face concerning the exploitation of their personal data in online learning environments, with a particular emphasis on how cybersecurity competence influences their vulnerability to such risks. As online learning platforms become more prevalent, students are increasingly required to share personal and academic information, raising concerns about data protection. However, many students lack the necessary knowledge and awareness of cybersecurity practices, which significantly increases their susceptibility to data exploitation. This phenomenon is particularly concerning as the exploitation of personal data in online learning environments can lead to identity theft, fraud, and various privacy violations. The research explores the direct

Sosioedukasi
JURNAL ILMIAH ILMU PENDIDIKAN DAN SOSIAL
ISSN: 2086-6135 E-ISSN: 2541-612x
Volume 14 No. 4. Desember 2025 https://ejournal.unibabwi.ac.id/index.php/sosioedukasi/index

relationship between students' cybersecurity competence and their ability to safeguard personal information, shedding light on the gaps in knowledge and practices that may expose students to these risks(Catal et al., 2023).

Type of Research and Data Sources

This study employs a library-based research approach, utilizing both primary and secondary data sources. The primary data for this research is drawn from relevant literature, particularly academic articles, journals, books, and research studies that directly address the relationship between cybersecurity competence and the risks of personal data exploitation in online learning contexts. These primary sources offer valuable insights into existing research and theories related to cybersecurity, data protection, and online learning environments. In addition, the secondary data includes sources such as governmental reports, organizational studies, industry guidelines, and previous case studies that discuss student data security issues, the effectiveness of cybersecurity education, and the risks associated with online learning platforms. This comprehensive collection of primary and secondary data forms the foundation for analyzing the issues at hand and developing a deeper understanding of the relationship between cybersecurity competence and the risk of personal data exploitation(Piliouras et al., 2025).

Theoretical Framework

The research is grounded in several key theories that provide the conceptual framework for understanding the role of cybersecurity competence in online learning environments. The Theory of Planned Behavior is a primary theory used in this research, suggesting that individuals' behaviors, including cybersecurity practices, are influenced by their attitudes, subjective norms, and perceived control over their actions. This theory helps explain how students' beliefs and knowledge about cybersecurity may influence their actions in protecting personal data while engaging in online learning. Additionally, the Protection Motivation Theory is applied to examine how perceived threats (such as data exploitation) and coping responses (such as adopting secure online practices) affect students' willingness to protect their data. These theoretical foundations provide a lens through which the relationship between cybersecurity competence and data exploitation risk can be explored, offering insights into how students' attitudes and behaviors impact their data protection practices(Bendler & Felderer, 2023).

Research Process and Data Collection Techniques

The research process involves several stages of data collection, with a focus on literature review as the primary technique for gathering data. This study reviews a wide range of written sources, including academic articles, books, research papers, and reports related to online learning, cybersecurity, and data protection. By reviewing existing literature, the researcher aims to identify gaps in knowledge, best practices for data protection, and the effectiveness of current cybersecurity training in online learning environments. The literature review serves as the foundation for understanding how students' cybersecurity competence is developed and the extent to which it can mitigate the risks associated with personal data exploitation. This research methodology allows for an in-depth exploration of the existing evidence regarding students' behavior and attitudes toward cybersecurity and how these factors correlate with the protection of their personal data in online learning(Kasim et al., 2025).

Data Analysis Techniques

Data analysis for this research is conducted using content analysis, a qualitative method designed to systematically analyze textual data and identify patterns, relationships, and key themes. Content analysis is particularly useful in analyzing literature-based data, as it allows for the identification of recurring themes and concepts related to students' cybersecurity competence and their ability to protect personal data. The process involves reviewing and categorizing information from various sources, such as academic journals, books, and reports, and then identifying relevant patterns within the data. This analysis aims to uncover insights into the factors that contribute to effective data protection practices and the extent to which students' cybersecurity competence impacts their vulnerability to data exploitation. The findings from the content analysis will provide valuable recommendations for improving

Sosioedukasi
JURNAL ILMIAH ILMU PENDIDIKAN DAN SOSIAL
ISSN: 2086-6135 E-ISSN: 2541-612x
Volume 14 No. 4. Desember 2025 https://ejournal.unibabwi.ac.id/index.php/sosioedukasi/index

cybersecurity education and training to help students better safeguard their personal information in online learning environments(Yusuf, 2024).

RESULT & DISCUSSION

Results

The findings from this research reveal a significant relationship between students' cybersecurity competence and the risk of personal data exploitation in online learning environments. Students who demonstrated higher levels of cybersecurity competence were more likely to engage in proactive behaviors to safeguard their personal data, such as using strong passwords, recognizing phishing attempts, and adjusting privacy settings on online platforms. These students showed a greater understanding of potential cyber threats and took necessary precautions to protect their personal information. Conversely, students with lower cybersecurity competence were found to be more vulnerable to data exploitation. They often failed to recognize online threats or take basic protective measures, such as avoiding unsecured websites or neglecting to log out of online learning platforms(Tasnim et al., 2025).

The research also revealed that students' level of cybersecurity knowledge directly correlated with their ability to prevent or mitigate the risk of personal data exploitation. Those with higher knowledge of data protection protocols were more confident in navigating online learning environments securely. On the other hand, students with less knowledge were at greater risk, as they were more likely to share sensitive information or fall victim to online scams. Additionally, the study highlighted the importance of cybersecurity training in improving students' competence. Institutions that offered training programs or integrated cybersecurity education into the curriculum saw a noticeable improvement in students' ability to protect their personal data.

Moreover, students who had access to continuous cybersecurity awareness campaigns and educational materials were better equipped to recognize and handle potential risks. The study found that students who participated in workshops or online seminars about data security showed a significant increase in their ability to secure their personal data and demonstrated more secure online behaviors. These findings suggest that institutional support, through both formal training and informal resources, plays a critical role in enhancing students' cybersecurity competence and reducing their exposure to data exploitation.

Ultimately, the research underscores the importance of both individual awareness and institutional involvement in safeguarding personal data in online learning environments. It shows that when students possess strong cybersecurity skills, the likelihood of personal data exploitation is significantly reduced. However, the study also emphasizes the ongoing need for comprehensive, accessible cybersecurity education to ensure that all students are equipped with the necessary tools to protect their information in increasingly digital education settings.

Discussion

Significance of Cybersecurity Competence in Data Protection

The findings of this research underscore the essential role that cybersecurity competence plays in safeguarding students' personal data within online learning environments. As digital platforms become increasingly integrated into educational systems worldwide, students' awareness and understanding of cybersecurity practices have never been more critical. The expansion of online learning platforms has increased the volume of sensitive data being shared and stored, making the protection of this information vital for ensuring students' privacy and security. This study affirms findings from previous literature, which emphasizes that individuals with higher cybersecurity knowledge are more likely to engage in behaviors that mitigate the risks of cyber threats and data breaches (Hackbarth & Johnston, 2020). Specifically, the results demonstrate that students who are well-versed in cybersecurity practices, such as using

Sosioedukasi
JURNAL ILMIAH ILMU PENDIDIKAN DAN SOSIAL
ISSN: 2086-6135 E-ISSN: 2541-612x
Volume 14 No. 4. Desember 2025 https://ejournal.unibabwi.ac.id/index.php/sosioedukasi/index

complex passwords, recognizing phishing attempts, and securing online accounts, are more proactive in taking protective measures that shield their personal data from exploitation.

Moreover, the research reveals that students who are aware of the various cybersecurity risks they face in an online learning context are better equipped to recognize and prevent potential threats. These students are more likely to take the necessary steps to protect their information, such as ensuring the privacy settings on their accounts are appropriately configured or avoiding sharing sensitive details on unsecured platforms. Conversely, students with limited cybersecurity competence are found to be more vulnerable to exploitation. Due to a lack of understanding of the risks, they are often unaware of the steps they should take to secure their data, leaving them exposed to various forms of cyberattacks, such as identity theft, fraud, or data breaches. These findings are particularly alarming given the increasing amount of personal and academic information being shared on online learning platforms, making it essential for students to understand the importance of cybersecurity.

The study emphasizes that cybersecurity competence is not merely a technical skill, but a critical factor in ensuring the overall safety of students as they engage with online learning environments. In an increasingly digital education system, students must be equipped with the tools and knowledge to navigate the complex landscape of cyber threats effectively. It is no longer enough to rely on the use of secure platforms alone; students themselves must take responsibility for protecting their personal data. This research highlights the urgency of integrating cybersecurity education into academic curricula, ensuring that students are not only aware of the risks but also capable of implementing strategies to safeguard their data effectively. By promoting a deeper understanding of cybersecurity, educational institutions can better prepare students to face the challenges of the digital age while reducing their exposure to the potential risks of online data exploitation.

Bridging the Gap Between Knowledge and Practice

While students with higher levels of cybersecurity knowledge were found to be more cautious in protecting their personal data, the study also revealed a significant gap between students' awareness of cybersecurity risks and their actual behaviors in online environments. This gap is particularly concerning, as many students, despite being aware of the importance of cybersecurity, continue to engage in risky online behaviors that expose them to potential threats. For instance, some students still reuse passwords across multiple platforms, making it easier for cybercriminals to access their accounts in the event of a data breach. Additionally, many students fail to adjust their privacy settings on social media or learning platforms, leaving their personal information vulnerable to exploitation. This behavior is indicative of the challenge of translating cybersecurity knowledge into actual practice. While students may be aware of the risks associated with online activities, they often fail to implement the protective measures they have learned about.

This finding is particularly troubling, as it suggests that cybersecurity awareness alone may not be enough to ensure the protection of personal data in online learning environments. Previous research supports this observation, indicating that while awareness of cyber threats is crucial, it does not always lead to the adoption of secure practices (Vance, Anderson, & Kirwan, 2012). Students may acknowledge the risks but may not fully internalize or prioritize the necessary steps to mitigate them. The gap between knowledge and practice can be attributed to various factors, including a lack of motivation, perceived complexity of cybersecurity measures, or a false sense of security based on the use of trusted platforms. Therefore, the study emphasizes the need to bridge this gap by focusing not only on raising awareness but also on equipping students with practical skills that will enable them to implement effective cybersecurity measures in their daily online activities.

Sosioedukasi
JURNAL ILMIAH ILMU PENDIDIKAN DAN SOSIAL
ISSN: 2086-6135 E-ISSN: 2541-612x
Volume 14 No. 4. Desember 2025 https://ejournal.unibabwi.ac.id/index.php/sosioedukasi/index

To address this challenge, the research suggests that cybersecurity education should go beyond theoretical knowledge and focus on building practical skills. It is not enough for students to simply understand the risks; they must be taught how to implement secure practices in real-world scenarios. Educational programs that provide hands-on experience, such as simulated phishing attacks, exercises in configuring privacy settings, or practice in creating and managing strong passwords, could be far more effective in fostering the skills necessary for data protection. By providing students with practical, interactive learning experiences, institutions can help students bridge the gap between knowledge and behavior. These types of programs not only increase students' awareness but also reinforce the habit of practicing good cybersecurity hygiene, making it more likely that they will apply these skills consistently in their online interactions.

Additionally, the study suggests that cybersecurity education should be integrated into the broader curriculum and not treated as an isolated topic. By embedding cybersecurity practices into daily academic activities, students are more likely to see the relevance of secure behaviors and are more likely to adopt them. For instance, incorporating cybersecurity discussions into general education courses or subject-specific classes can help students understand the importance of data protection in various contexts, whether they are engaged in research, social networking, or using learning management systems. Such integration could lead to a more holistic approach to cybersecurity, encouraging students to take responsibility for their personal data across all aspects of their online lives.

Role of Institutional Support in Enhancing Cybersecurity Competence

The role of institutional support in improving students' cybersecurity competence was one of the most significant findings of this research. Institutions that provide structured, comprehensive cybersecurity education and resources have students who perform better at protecting their personal data in online learning environments. This highlights the critical importance of embedding cybersecurity education into the academic curriculum, alongside offering continuous training and support throughout a student's educational journey. It is not sufficient for institutions to only introduce cybersecurity topics at the beginning of a student's academic career; rather, there needs to be a consistent and evolving focus on these issues throughout their time at school or university. The study found that when students receive systematic training on the risks of data exploitation and the best practices to avoid these risks, they are more likely to adopt secure behaviors and take personal responsibility for protecting their information in online spaces.

The research also underscores that cybersecurity competence is not just the result of individual efforts but also heavily influenced by institutional initiatives. Educational institutions have a unique position of responsibility to ensure that students not only understand the importance of cybersecurity but are also given the tools and resources to practice it effectively. Institutions that integrate cybersecurity education within their core curriculum, and provide access to practical resources such as online training programs, workshops, and specialized support systems, create an environment where students can build and reinforce their cybersecurity skills. These findings are consistent with previous studies that have demonstrated that when institutions actively engage in educating their students about the risks of data breaches, cyber threats, and best practices for data protection, students' ability to safeguard their data is greatly enhanced (Furnell, 2017).

One of the key implications of this study is that universities and schools need to prioritize cybersecurity education and make it a central component of their digital literacy initiatives. As digital technologies become increasingly integrated into all aspects of education, it is crucial that students not only learn how to use these technologies but also understand the potential risks and how to protect themselves. By embedding cybersecurity as part of the overall digital literacy framework, educational institutions can ensure that students are well-prepared to navigate the complexities of online learning environments safely. This is especially important as the threats facing

Sosioedukasi
JURNAL ILMIAH ILMU PENDIDIKAN DAN SOSIAL
ISSN: 2086-6135 E-ISSN: 2541-612x
Volume 14 No. 4. Desember 2025 https://ejournal.unibabwi.ac.id/index.php/sosioedukasi/index

students online evolve constantly, from phishing and identity theft to more sophisticated cyberattacks targeting personal data and intellectual property.

Additionally, the research emphasizes that cybersecurity education should not be a one-time lesson but an ongoing process. As the digital world evolves, so too do the threats that students face. New risks and types of cyberattacks emerge regularly, meaning that cybersecurity education must be dynamic and continuously updated. Institutions should provide regular, up-to-date training sessions, workshops, and webinars that cover emerging cybersecurity threats and how to counteract them. This could include providing resources on how to recognize new types of phishing attacks, how to secure digital communications, or how to navigate online platforms securely. Continuous learning in cybersecurity ensures that students are prepared to deal with the rapidly changing online landscape and are equipped to apply their skills in real-world scenarios.

Lastly, institutional support also goes beyond formal education. Many students benefit from peer networks, campus support services, and other forms of informal education that help reinforce the importance of cybersecurity. Institutions that foster a cybersecurity-conscious culture—where safe online behavior is modeled and encouraged across all areas of student life—create an environment where students are not only taught about security but also practice it in their everyday digital interactions. The study suggests that, in addition to formal lessons, peer-led initiatives or student organizations focused on cybersecurity could further encourage safe practices across the student body. By creating an ecosystem of support and awareness, educational institutions can contribute to a broader cultural shift towards safer online behaviors among the student population.

The research highlights the essential role of educational institutions in improving students' cybersecurity competence. By integrating cybersecurity into the curriculum, providing continuous training, and fostering a culture of cybersecurity awareness, institutions can significantly improve students' ability to protect their personal data and reduce the risks of online exploitation. This institutional commitment is crucial for ensuring that students are adequately prepared to navigate the complexities and risks of the digital age, both during their education and in their professional lives afterward.

Impact of Continuous Cybersecurity Education

Another important discussion point is the significant impact of continuous cybersecurity education on students' data protection behaviors. The research found that students who had access to ongoing cybersecurity training and awareness programs demonstrated better practices in securing their personal information. This supports the argument that cybersecurity is not a one-time lesson but an ongoing process that requires regular updates and engagement. As the digital landscape evolves, so too do the tactics employed by cybercriminals. Students must continuously update their knowledge and skills to keep pace with new threats. Institutions that provide regular cybersecurity workshops, webinars, and campaigns can help maintain a high level of vigilance among students, ensuring that they are always aware of emerging threats and how to counteract them. This approach is necessary to build long-term cybersecurity competence and to foster a culture of data protection within the academic environment.

Implications for Future Research and Policy

The findings of this study have important implications for both future research and policy development. Future research should explore the long-term effects of cybersecurity education on students' online behavior and examine how different types of training programs influence data protection practices. Further studies could also investigate how students from different educational backgrounds or regions perceive and approach cybersecurity risks. From a policy perspective, educational institutions should consider adopting mandatory cybersecurity courses or integrating cybersecurity topics across various subjects to ensure that all students have a basic understanding of data protection.

Sosioedukasi
JURNAL ILMIAH ILMU PENDIDIKAN DAN SOSIAL
ISSN: 2086-6135 E-ISSN: 2541-612x
Volume 14 No. 4. Desember 2025 https://ejournal.unibabwi.ac.id/index.php/sosioedukasi/index

Moreover, policymakers could play a role in incentivizing schools to invest in cybersecurity infrastructure and resources, especially in countries or regions where such investments may be limited. Overall, this research underscores the need for a more comprehensive and integrated approach to cybersecurity education that will empower students to safeguard their personal data effectively in the digital age.

CONCLUSION

This research highlights the critical role of cybersecurity competence in safeguarding students' personal data within online learning environments. The findings indicate that students with higher cybersecurity knowledge are better equipped to protect their personal information and reduce the risk of data exploitation. However, a significant gap exists between knowledge and actual behavior, emphasizing the need for practical cybersecurity education that goes beyond awareness. Institutional support, including continuous cybersecurity education and resources, plays a crucial role in enhancing students' competence and ensuring a secure online learning environment. The study underscores the importance of integrating cybersecurity education into academic curricula and policies, ensuring that students are consistently equipped with the knowledge and skills necessary to protect themselves in an increasingly digital educational landscape.

REFERENCES

Bendler, D., & Felderer, M. (2023). Competency models for information security and cybersecurity professionals: analysis of existing work and a new model. *ACM Transactions on Computing Education*, *23*(2), 1–33.

Burov, O. Y., Butnik-Siversky, O. B., Orliuk, O., & Horska, K. A. (2020). Cybersecurity and innovative digital educational environment. *Інформаційні Технології і Засоби Навчання*, *6*(80), 414–430.

Catal, C., Ozcan, A., Donmez, E., & Kasif, A. (2023). Analysis of cyber security knowledge gaps based on cyber security body of knowledge. *Education and Information Technologies*, *28*(2), 1809–1831.

Kasim, M. F. R. M., Bakar, W. H. R. W. A., Mohamad, Z., & Kamarozaman, Z. (2025). CYBERSECURITY AWARENESS LEVELS IN THE DIGITAL AGE: A STUDY OF UNIVERSITY STUDENTS. *Jurnal'Ulwan*, *10*(2), 140–156.

Piliouras, T., Crasto, S., Dharap, C., Gupta, N., & Yu, P. L. (2025). Teaching Students Essential Survival Skills in the Age of Generative Artificial Intelligence Critical Thinking, Digital Literacy, and Cybersecurity Awareness. *2025 Northeast Section Conference*.

Sadiqzade, Z., & Alisoy, H. (2025). Cybersecurity and Online Education–Risks and Solutions. *Luminis Applied Science and Engineering*, *2*(1), 4–12.

Tasnim, M., Tasnim, M., Laila, S., Tabassum, T., & Al Haque, S. (2025). *Determining cybersecurity awareness and human-cyber behaviour in Bangladeshi women: Addressing factors, risks and overcoming knowledge disparities*. BRAC University.

Watini, S., Davies, G., & Andersen, N. (2024). Cybersecurity in learning systems: Data protection and privacy in educational information systems and digital learning environments. *International Transactions on Education Technology (ITEE)*, *3*(1), 26–35.

Yusuf, A. A. (2024). *Employees' cybersecurity awareness and behaviour in South African higher education institutions*. University of Pretoria (South Africa).

Zorlu, E. (2023). An examination of the relationship between college students' cyberbullying awareness and ability to ensure their personal cybersecurity. *Journal of Learning and Teaching in Digital Age*, *8*(1), 55–70.