MUKADIMAH
Jurnal Pendidikan, Sejarah, dan Ilmu-ilmu Sosial
Program Studi Pendidikan Sejarah FKIP - Universitas Islam Sumatera Utara, Medan
e-Journal: http://jurnal.uisu.ac.id/index.php/mkd | e-mail: mukadimah@fkip.uisu.ac.id
ISSN: 2622-1373 (Online)
ISSN: 2614-1159 (Print)
Vol. 8 No. 2
August 2024

Digital Legal Education and Cybersecurity Awareness: A Bibliometric Study on Student Behavior

Lia Sautunnida*, Department of Law, Universitas Syiah Kuala, Banda Aceh, Indonesia
Ridayani, Department of Civic Education, Universitas Syiah Kuala, Banda Aceh, Indonesia
Khairani, Department of Law, Universitas Syiah Kuala, Banda Aceh, Indonesia
Eka Kurniasari, Department of Law, Universitas Syiah Kuala, Banda Aceh, Indonesia
Anta Rini Utami, Department of Law, Universitas Syiah Kuala, Banda Aceh, Indonesia
Iwan Fajri, Department of Social Sciences Education, Universitas Syiah Kuala, Indonesia

ABSTRACT

This study analyzes current trends in the integration of digital technologies with legal education and their impact on cybersecurity awareness among students. Through a bibliometric approach, the research identifies challenges, opportunities, and future directions in digital legal education, emphasizing the importance of a holistic approach that encompasses technical, digital rights, and ethical dimensions. While technology is increasingly embedded in legal education, human-centeredness and ethical considerations remain underrepresented in cybersecurity curricula. The findings reveal that current cybersecurity education predominantly focuses on technical and legal aspects, thereby neglecting critical humanistic factors necessary for comprehensive training. This paper underscores the need for more interactive and innovative educational strategies, such as collaborative learning and virtual reality simulations, to bridge the skills gap and adequately prepare students for the digital challenges of the modern world. Future research should further explore these strategies to enhance the effectiveness of cybersecurity education within legal studies, equipping students to navigate the complexities of a digitally driven age.

ARTICLE HISTORY

Received	03/08/2024
Revised	06/08/2024
Accepted	16/08/2024
Published	17/08/2024

KEYWORDS

Digital legal education; cybersecurity awareness; digital ethics; interactive learning; virtual reality simulations.

***CORRESPONDENCE AUTHOR**

liasautunnida@usk.ac.id

DOI: https://doi.org/10.30743/mkd.v8i2.9726

INTRODUCTION

Digital legal education, which aims to equip students with the necessary skills to navigate the intersection of law and technology, faces a critical problem: the inadequate integration of cybersecurity awareness within its framework. This issue arises because the rapid evolution of cyber threats has outpaced the development of digital legal curricula, leaving students underprepared to handle the complexities of cybersecurity in real-world legal contexts (Altameem et al., 2023; Gerontakis et al., 2023). The problem is further exacerbated by the disconnect between the theoretical knowledge provided by digital platforms and the practical application of cybersecurity measures. Many students lack the digital literacy required to fully grasp and implement cybersecurity practices, which can lead to significant vulnerabilities in protecting sensitive legal information (Krundyshev & Kalinin, 2021; Sallos et al., 2019).

This issue is problematic because it undermines the effectiveness of digital legal education in preparing students for the demands of the modern legal environment. Educational institutions often prioritize legal content over technological aspects, resulting in an oversight of the crucial role that cybersecurity plays in the digital legal field (Cabaj et al., 2018; Kam & Katerattanakul, 2024; Salmine et al., 2023). Moreover, the varying levels of students' prior access to digital devices and digital literacy contribute to disparities in their understanding and engagement with cybersecurity content (Al-Janabi & Al-Shourbaji, 2016; Antones, Silva & Marques, 2021). This research is important because, without a thorough integration of cybersecurity studies into digital legal education, students may be ill-equipped to safeguard the integrity of legal information in the digital age. Therefore, this study seeks to investigate the extent of cybersecurity awareness in digital legal education and assess its

impact on student behavior and preparedness, highlighting the necessity of addressing this gap to enhance the overall efficacy of legal education in a digital world.

So far, what remains poorly discussed in the existing studies are important components of harmonizing digital legal education and cybersecurity awareness in shaping behavior. Earlier research works always consider the digitalization of legal education in a linear way, thus probably missing the complexity of cybersecurity awareness that should correspond to it. This research does not deal with the basic link between digital legal education and comprehension by students of cyber security. Major three trends that can be noted with the existing literature are studies that underpin the efficacy of digital legal education without delving into the cyber-security dimensions in detail (Gulyamov et al., 2023; Jacob et al., 2020; Dawson, 2018; Bondarenko et al., 2022; Storr & McGrath, 2023; Karasheva et al., 2024). Second, studies that analyze the negative impacts arising from the lack of cybersecurity education within digital legal curricula include studies by Crabb et al. (2024) and Gulyamov et al. (2023). Third, studies that map challenges of digital literacy among law students in the adoption of cybersecurity technologies—Gulyamov et al. (2023), Kallonas et al. (2024), Marksbury & Bryant (2019), Rodrigues et al. These trends, on the other hand, reveal that the integration of digital legal education and cybersecurity awareness in impacting student behaviour had not been captured extensively.

The paper will address the limitations identified by past research where the current studies have not independently looked into how digital-based legal education impacts cybersecurity understanding and behavior of students. The use of technology in legal studies is much dependent on students' knowledge and awareness levels of cybersecurity, yet current research has not made it the center of discussions as earlier identified. How students perceive and behave with regard to cybersecurity needs more exploration in order to establish how digital legal education could fill the gaps. Accordingly, three research questions (RQs) are proposed: (1) What are the current research trends in digital legal education and cybersecurity awareness? (2) How does digital legal education influence cybersecurity awareness and behavior among students, according to existing literature? and (3) What are the primary research gaps and future directions in the field of digital legal education and cybersecurity awareness? Answering these questions provides a deeper understanding that serves as the foundation for formulating educational policies and learning strategies to maximize the goals of adopting digital legal education while also enhancing cybersecurity awareness and behavior. This bibliometric analysis will identify research patterns, reveal significant findings, and highlight areas in need of further research, thereby making an important contribution to the development of a more comprehensive and relevant curriculum in the digital era.

This study addresses the critical problem of insufficient integration between digital legal education and cybersecurity awareness, which is rooted in the fundamental differences between traditional legal education and the demands of the digital era. Traditional legal education emphasizes theoretical knowledge and case analysis, often neglecting the technical skills required for effective cybersecurity practices. This creates a significant gap in students' preparedness to address the cybersecurity challenges they will encounter in the professional legal environment. As digital legal education increasingly incorporates technology to enhance learning, it often faces resistance from established educational practices that are deeply rooted in classical teaching methods (Drapezo et al., 2022; Korobova et al., 2022; Yavorskiy et al., 2020; Yu, 2022).

The core issue identified in this study is the lack of a comprehensive curriculum that integrates both legal and technical knowledge, which is necessary for students to develop a robust understanding of cybersecurity. To thoroughly investigate this problem, this study employs a bibliometric analysis to systematically review and quantify existing research on the integration of digital legal education and cybersecurity awareness. By analyzing the citation patterns, co-authorship networks, and keyword trends in the literature, this study aims to identify the gaps in current research and provide

insights into how digital legal education can be better aligned with the technical demands of cybersecurity. The findings from the bibliometric analysis will help in understanding the extent to which existing literature has addressed this issue and will offer guidance for developing a holistic curriculum design that bridges the current gap in legal education. This study is particularly informed by the works of scholars such as Jackson (2016), Jones et al. (2021), Pasvenskienė and Astromskis (2020), Bauling (2023), and Makdee et al. (2023), who have explored various aspects of this integration.

METHOD

The subject of this study centers on the problem of digital legal education and cybersecurity awareness among students. This paper goes beyond the typical gaps in the existing literature through an exploration of how digital legal education impacts students' cybersecurity awareness and behavior in order to inform practical interventions and policies toward enhancing the current educational practices.

This research adopts a bibliometric study approach, utilizing a systematic review to analyze existing literature. The data used comprises peer-reviewed articles published between 2014 and 2024, focusing on digital legal education and cybersecurity awareness among students. The comprehensive literature search was conducted in the Scopus academic database, using keywords such as "Digital Legal Education," "Cybersecurity Awareness," "Student Behavior," "Impact of Digital Education on Cybersecurity," "Cybersecurity in Higher Education," "Digital Literacy and Cybersecurity," "Legal Education and Student Outcomes," "Educational Technology in Legal Studies," "Cybersecurity Programs in Education," and "Integrating Cybersecurity into Legal Education."

The data sources were selected based on specific inclusion criteria: articles must be peer-reviewed, written in English, and specifically address digital legal education or cybersecurity awareness among students (Gernhardt & Groš, 2022). Studies focusing on general cybersecurity or legal education without digital components were excluded. Key information, including publication year, authors, journal name, research focus, methodologies, key findings, and identified research gaps, was systematically extracted from the selected articles and organized into a database for analysis.

Data collection involved a thorough search and screening process. Initially, search results were filtered by title and abstract to identify relevant studies. Full texts of potentially relevant articles were then reviewed to confirm their eligibility based on the inclusion criteria. Multiple reviewers independently assessed the inclusion of articles and the accuracy of data extraction, resolving any discrepancies through discussion and consensus.

The techniques of data analysis were found to be of two types: qualitative and quantitative. From a bibliometric point of view, patterns and trends in the literature are identified through frequency of publication, count of citations, co-authorship networks, and thematic clusters (Aria & Cuccurullo, 2017). Some software or tools to help manage this regard include Biblioshiny, which allows for the visualization of bibliometric networks and trends using the previously mentioned principles (Aria et al., 2024). The qualitative synthesis of the findings was done based on how digital legal education impacts students' cybersecurity awareness and behavior. This synthesis will bring to light the key research gaps and propose further research directions. With the application of a broad and systematic approach, it will have the capability to provide a robust view of the current research situation and be able to offer relevant insights for educators, policymakers, and researchers in the field.

RESULT

The results of bibliometric analysis on digital legal education and cybersecurity awareness are structured in three major sections: The first section illustrates the current research trends in the field of digital legal education and cybersecurity awareness. The second section presents an analysis of how digital legal education impacts the existing literature on cybersecurity awareness and behavior in students. Section 3 Primary research gaps and future directions in the domain of digital legal education and cybersecurity awareness.

Current trends in research on digital legal education and cybersecurity awareness

Analyzing the current trends in digital legal education and cyber security awareness research: By research streams, this is being studied across different disciplines. This paper provides insights into the dominant research trends, geographical and institutional distribution of studies, and collaborative networks among researchers. An understanding of these trends will be crucial to determine where the attention has been focused, who the main contributors are in the field, and to what extent international collaboration occurs (Figure 1). The current review is very much foundational for further exploration of the idea that research in digital legal education is dynamic.

The results of the bibliometric analysis indicate that research on digital legal education and cybersecurity awareness has increased significantly over the past five years. As shown in the annual scientific production graph, the number of publications has steadily increased, reaching a peak in 2023 before slightly declining in 2024 (Figure 2). This growth reflects the increasing interest in the integration of technology into legal education.

The frequently emerging topics in this research include the use of e-learning platforms, digital case-based learning methods, and the role of technology in enhancing legal literacy and cybersecurity awareness. The word cloud and topic treemap reveal that "education," "students," "medical student," "e-learning," and "curriculum" are among the most frequently occurring keywords (Figure 3). This indicates a strong focus on how technology can be leveraged to optimize the learning process in legal education and enhance cybersecurity awareness.

This research predominantly originates from countries with advanced educational technology infrastructures, such as the United States, the United Kingdom, Germany, Spain, and Ukraine (Figure 4). The geographic distribution map and country production graph illustrate the dominance of these countries in contributing to the research (Figure 5).

International collaboration in this research has also increased, marked by a high percentage of international co-authorship at 13.64%. Many articles are authored by researchers from various countries, indicating the presence of a broad and collaborative research network. Such collaboration not only enriches the quality of the research but also aids in disseminating knowledge and best practices globally, fostering a more holistic and integrated approach to digital legal education and cybersecurity awareness.

Influence of Digital Legal Education on Cybersecurity Awareness and Behavior among Students

Based on the existing literature, digital legal education has a significant impact on cybersecurity awareness and behavior among students. Here are the key findings, challenges, opportunities, and implications associated with integrating digital legal education into cybersecurity awareness and behavior among students.

Key Findings

Awareness of the importance of cybersecurity has become an increasingly urgent need across various professions, especially with the growing use of technology in all fields. Students in non-technical disciplines, in particular, require strong cybersecurity awareness as technology becomes more prevalent in various professions (Cravens & Resch, 2023). Although knowledge of cybersecurity does not always correlate with actual cybersecurity behavior, Computer Science students exhibit slightly better cybersecurity knowledge but significantly better password hygiene practices (Cravens & Resch, 2023).

Research also indicates a strong and undeniable relationship between the level of legal awareness regarding cybercrime and students' involvement in illegal cyber activities (Alhadidi et al., 2024). Unfortunately, most students surveyed exhibited low levels of cybersecurity awareness, particularly among younger age groups. They tend to be unfamiliar with common cybersecurity terms or threats, such as phishing (Tirumala et al., 2016). Overall, students demonstrate a lack of awareness about cybersecurity and its implications, highlighting the need for cybersecurity training to help them make the most of the internet and avoid becoming victims of cyberattacks (Jagadeesan et al., 2023).

Challenges and Opportunities

On these lines, The Cyber Law and Cyber Security educational students' challenges and opportunities would mainly focus on the various areas that need to be dealt with. The prime challenges include absence of a common set syllabus, little to no faculty awareness, and few practical exposures to cyber law students (Gulyamov et al., 2023). Besides, the rapid rise in Internet and information technology use by students created colossal issues because of an unprecedented dependency on those technologies, consequently giving birth to a new spectrum of unlawful and illegal behaviors (Alhadidi et al., 2024). Another challenge lies in low-level cybersecurity awareness of students, especially at younger age groups, as well as a lack of understanding of common terms used in reference to cybersecurity and typical threats (Tirumala et al., 2016).

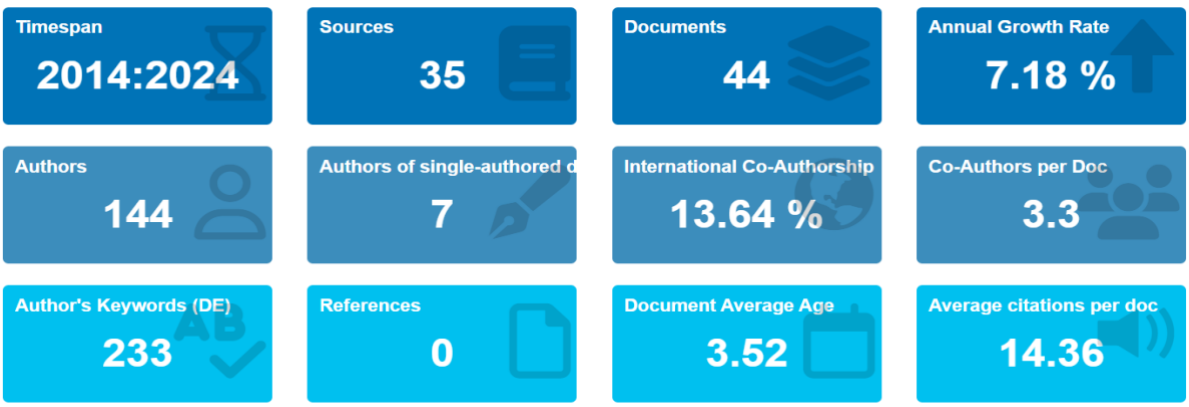

Figure 1. Bibliometric Analysis of Cybersecurity and Digital Legal Education Research: Trends and Collaborations from 2014 to 2024

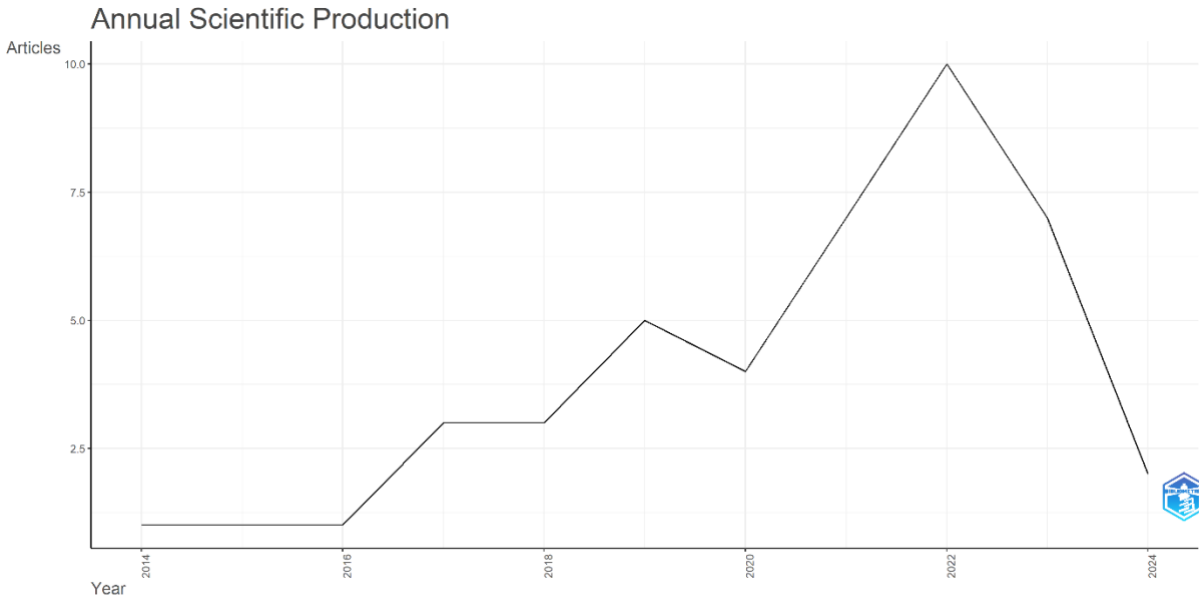

Figure 2. Annual Scientific Production in Cybersecurity and Digital Legal Education Research (2014-2024)

Figure 3. Key Themes in Research on Cybersecurity Awareness and Digital Legal Education

However, the challenges have also offered numerous opportunities. Some of the opportunities include incorporating collaborative learning, simulations, real-world case studies, and technology among students in learning their cyber laws to improve the quality of teaching and outcomes (Gulyamov et al., 2023). Other opportunities include devising proper strategies to enhance the cybercrime awareness of students and subsequently decreasing their involvement in such types of crimes (Alhadidi et al., 2024). Furthermore, tailored cyber security training and interventions for

students from higher learning institutions will enhance the improvement of their cyber security behavior (Fatokun et al., 2019).

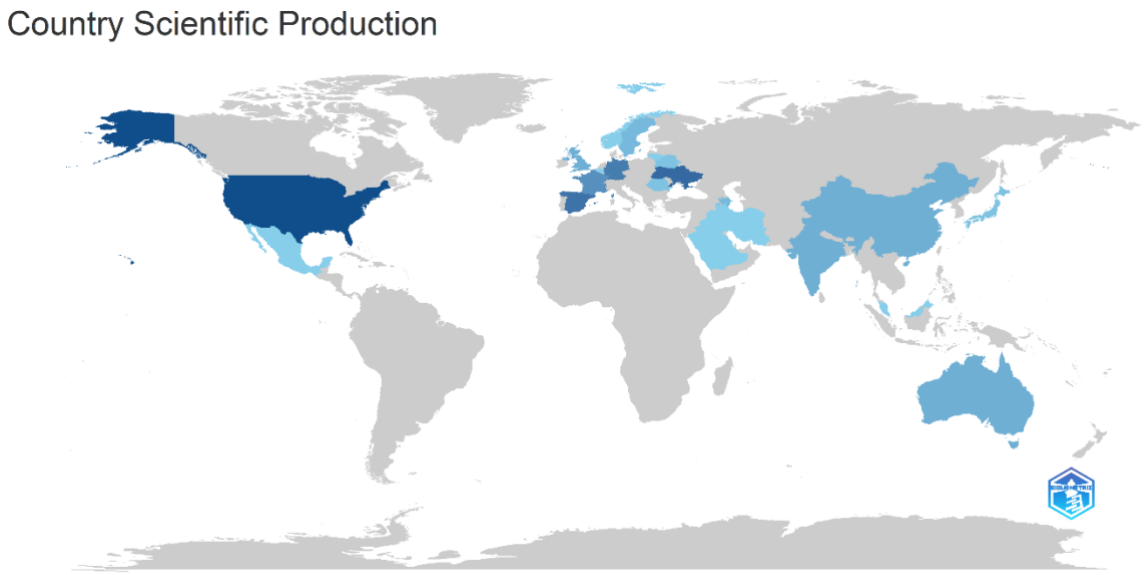

Figure 4. Global Distribution of Scientific Production in Cybersecurity and Digital Legal Education

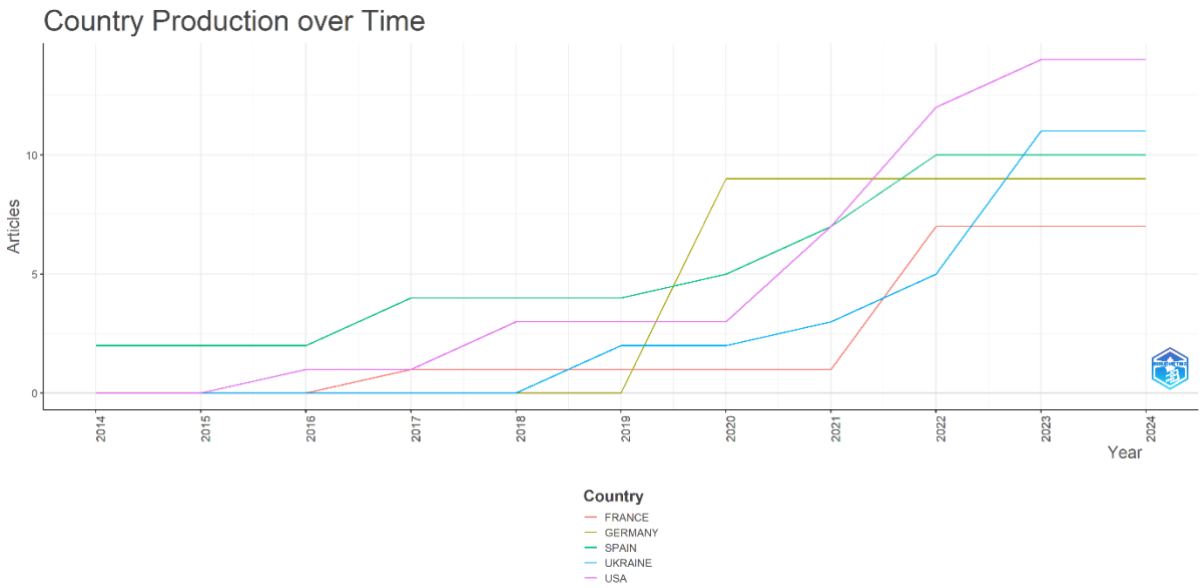

Figure 5. Trends in Scientific Production by Country Over Time in Cybersecurity and Digital Legal Education (2014-2024)

Different Approaches to Digital Legal Education

This growth in online learning has made it necessary for students to be trained in cybersecurity for them to fully exploit the benefits of the internet without falling prey to cyberattacks (Jagadeesan et al., 2023). The implementation of a cybersecurity curriculum into higher education thus becomes an inevitable process to make students face the digital world with ease and ensure that the cyberspace is safer and more secure for every other person online (Jagadeesan et al., 2023).

Implications for the Future

There is an urgent requirement to raise the awareness of cybersecurity among students, particularly those at younger ages, as deterrence to criminal behaviors in creating a safer cyberspace environment. The purpose is to ensure that cybersecurity education is included in the curricula of higher education institutions and thus prepare students to face the realities that the digital world presents while solving the problem of inadequate cybersecurity awareness among students (Jagadeesan et al., 2023).

The existing literature gives valuable insights about the effects of digital legal education on the awareness and behaviors of students regarding cybersecurity. It reveals that there is a tremendous demand for specialized cybersecurity training, the inclusion of cybersecurity education in the curriculum, and challenges related to low levels of cybersecurity awareness among students, generally, and more so in the younger age brackets. This study underscores the importance of dealing with cybersecurity education in making the online environment safe and secure for students.

Primary Research Gaps and Future Directions

From the review of the literature above, the section below identifies primary research gaps and future directions in the domain of digital legal education and cybersecurity awareness.

Research Gaps

The existing curriculums in cybersecurity studies are more technical and focused on economics, the law, and national security. However, it becomes quite obligatory to adopt a people-centered approach, championing the protection of human rights and digital rights in this education itself. These have been found to be extremely important (Caulkins et al., 2016; Jerman Blažič & Jerman Blažič, 2022). They also do not have integrated knowledge to indicate best practices in the deployment of tools, technologies, and digital learning interventions within legal education. This gap can point towards areas where recent research has been lacking on the issues, perhaps leaving knowledge gaps (Storr & McGrath, 2023).

Major challenges in education on cyber laws include the fact that there are no standard curricula, there is a scarcity of faculty knowledge, and students do not have adequate practical exposure. The above challenges are the problems identified as research gaps that exist within the cyber law education domain (Gulyamov et al., 2023). In this regard, the interdisciplinarity of the cybersecurity education field is important for achieving a proper level of cybersecurity education for all members of society according to their status and role. This underscores potential gaps in cybersecurity education, for which a more holistic and inclusive approach needs to be pursued (Jacob, Peters, & Yang, 2020).

Future Directions

Future research should, thus, take the development of human-centered cybersecurity curricula as a top priority. This would be important in dealing with the unique challenges emanating from the human dimension of cybersecurity, which is mostly lacking in curricula focused on technical and legal aspects (Caulkins et al., 2016). When approached from a human-centered perspective, cybersecurity education can increase its effectiveness in dealing with issues concerning human rights and digital rights.

Cyber law education can further be improved by focusing on innovative pedagogy. Better quality teaching should be rethought with more interactive ways of learning, including collaborative

learning, simulations of real case studies, and integration of technology, such as gamification and virtual reality simulations, to improve the quality of teaching and hence student outcomes (Gulyamov et al., 2023). Such innovations make learning not only more engaging but also help students understand the intricacies of cyber law from a practical and more relevant context.

There is also the need for efforts to reduce the skills gap in cybersecurity education. This can be achieved through better educational frameworks that incorporate new forms of information applications, such as remote laboratories and virtual classrooms. The introduction of advanced learning tools and methods avails students with the readiness and actual means to face life challenges in an ever-dynamic cyber world. According to Mukherjee et al. (2024).

DISCUSSSION

Current trends in research on digital legal education and cybersecurity awareness

The present research gives insights into trends and development within the sphere of digital legal education, supplemented by raising cybersecurity awareness. It provides, indeed, a holistic understanding of how the spheres have evolved in recent years. From the analysis of bibliometric information and the research results themselves, some key insights have been drawn upon, and those are reviewed in the following sections.

First, from the above trend analysis of the development of the research landscape in digital legal education and awareness creation on cybersecurity, the process has been quick. The increase in the number of publications has increased in the last five years and peaked in 2023. This corresponds with the increased interest in the integration of technology in legal studies, more so with respect to cybersecurity (Gulyamov et al., 2023; Jerman Blažič & Jerman Blažič, 2022). Such growth underlines the need to ready legal professionals with digital skills for the navigation through complex legal issues, which are the reality of today.

On this note, further exploring the nature of this research, it is clear that there is a primary intention on how technology will be capitalized on to advance legal education and improve awareness of cyber-security. The most commonly explored topics include the use of e-learning platforms, case-based digital learning methods, and the role of technology in enhancing legal and cybersecurity literacy (Jacob et al., 2020; Dawson, 2018). These findings indicate that practical, not just theoretical, digital tools are needed to be infused in the curriculum so that the students are better prepared in the wider and increasingly digital legal environment.

Geographically, research contributions have been led by countries with strong educational technology infrastructures, including the United States, the United Kingdom, Germany, Spain, and Ukraine. This concentration of efforts in research sets an implication that such countries are leaders in embracing and innovating within digital legal education (Crabb et al., 2024; Jerman Blažič & Jerman Blažič, 2022). But it also calls for deeper worldwide participation to ensure that the challenges in digital legal education and cybersecurity are globally addressed.

Also, the rising trend in international collaboration—signified by this 13.64% figure of international co-authorship—reflects that cybersecurity and digital legal education are international issues of significance with global relevance to humanity (Tirumala et al., 2016; Caulkins et al., 2016). Collaborations add value to research, bringing a global aspect to the sharing of knowledge and best practices, leading toward a unified and combined approach to ameliorate the issues in these areas. Such a partnership is necessary to deliver strategies that are applicable across the wide diversity of legal and educational systems around the world.

In sum, the findings of this study indicate a call for further research on the integration of technology into legal studies and a slight shift towards increasing the level of students' cybersecurity awareness in the process (Alhadidi et al., 2024; Jagadeesan et al., 2023). Such problems are global, so the development and diffusion of holistic educational solutions that can be adaptively used in different cultural and institutional contexts should continue—with high intensity. These efforts would be necessary to ensure legal professionals are equipped to navigate the digital threats and opportunities of the future.

Influence of Digital Legal Education on Cybersecurity Awareness and Behavior among Students

An area of increasing significance, as evidenced by reflection in recent literature, is the influence of digital legal education on cybersecurity awareness and behavior among students. Technology integration in legal education is changing the perception a student carries and what reactions are made against any possible cybersecurity threats. These findings, together with future challenges and opportunities, are discussed further.

First of all, the literature articulates that in the digital context of legal education, there is a very significant influence on the level and behavior of students' cybersecurity. With increasing technology use in professions, the need for good cybersecurity awareness in nontechnical fields like law has become more pressing (Cravens & Resch, 2023). However, with the increased level of knowledge, there is a gap in cybersecurity knowledge with respect to actual behaviors. For instance, students in technical fields, including Computer Science, perform slightly better concerning knowledge but significantly better in practices like password hygiene than the other students (Cravens & Resch, 2023). This indicates that, although knowledge could be a precondition, it is not enough to change behavior and, hence, calls for more practical, behavior-oriented training.

The said challenges and opportunities in integrating digital legal education with cybersecurity awareness underline several areas of key focus. Among the prominent challenges is the lack of standardized curricula, faculty knowledge, and practical exposure for students enrolling in cyber law education courses (Gulyamov et al., 2023). Another point that has contributed to the increased dependence of this area of the internet and information technology, creating new spectrums of illegal/illicit behavior, is the rapid growth in the use of the Internet and information technology by students (Alhadidi et al., 2024). This shows a considerable gap in students' cybersecurity knowledge, most especially among the lower age group of students (Tirumala et al., 2016). But these are challenges that throw up opportunities too, in the sense that integration of collaborative learning, simulations, real-world case studies, and technology with cyber law education will lift teaching quality and student outcomes (Gulyamov et al., 2023).

Thus, different approaches toward digital legal education are emerging as responses to the current challenges. The upsurge of e-learning necessitates students to have an adequate understanding of cybersecurity in order to maximize the benefits of the internet and avoid being victims of cyberattackers (Jagadeesan et al., 2023). Integration of the subject matter of cybersecurity in higher education curricula is among the best strategies to prepare learners for the realities of the digital world and assures a safer and more secure online environment for all (Jagadeesan et al., 2023). It has to be completely versatile and flexible enough to be adapted to students from various other disciplines.

Implication for the future is to raise the level of awareness of cybersecurity for students, with special emphasis on younger students, so that their involvement in criminal behaviors can be reduced and the environment online becomes much safer (Alhadidi et al., 2024; (Jagadeesan et al., 2023;

Tirumala et al., 2016). The current move will integrate cybersecurity education into the regular higher education curriculum toward preparing students for the real digital world and bridging existing gaps in cybersecurity knowledge. This effort is not only a benefit to safeguard students but also a direct contribution to the general goal of maintaining a secure digital space.

In conclusion, the literature provides valuable information on the impact of digital legal education on cybersecurity awareness and behavior among students. It emphasizes that there should be special cybersecurity training, inclusion of the subject in the curriculum, and that generally, many students are not aware of different aspects of security, especially the young ones. This is quite an important issue for the online environment of the safer and more secure dealings with the students.

Primary Research Gaps and Future Directions

Primary research gaps and future directions in the exploration of digital legal education and cybersecurity awareness offer areas of research needing to be pursued. Identification of these gaps can help researchers focus on addressing the most relevant issues in a way that would improve the effectiveness of educational strategies in the field.

Current curricula in cybersecurity education stress technical, economic, legal, and national security aspects. There is a strong need for a human-centered approach to be taken up with regard to preserving human and digital rights within this education framework (Caulkins et al., 2016; Jerman Blažič & Jerman Blažič, 2022). This gap indicates a major fault in the current state of curricula and a lack of comprehensive coverage for the ethical and humanistic dimensions of cybersecurity. Secondly, there is no consolidated best-practice knowledge when using digital tools, technologies, and interventions in legal education to help avoid the gaps regarding how best the digital resources should be rolled out (Storr & McGrath, 2023).

There are other supplementary challenges for cyber law education, such as the lack of uniform curricula, a shortage of faculty expertise, and a lack of practical exposure for students (Gulyamov et al., 2023). These reasons are all the more indication of the fact that cybersecurity teaching has to be done in a more holistic and inclusive manner, which should include persons at different echelons of society corresponding to their roles. The interdisciplinary nature of cybersecurity education further underlines the needs of a curriculum that considers not only technical skills but also broader social and ethical considerations (Jacob et al., 2020).

Future research should be oriented toward the development of human-centered cybersecurity curricula. This is vital in laying out a curriculum that will try to solve the unique challenges that are brought by the human dimension in cybersecurity, and which tends not to be focused on more technical curricula, as posited by Caulkins et al. (2016). Human rights and digital ethics move center stage in emphasizing how cybersecurity education can be even more effective in addressing the problems and challenges in these very areas.

Besides, the interaction in the teaching methodologies of cyber law education has to be more enriched and innovative. Simulating real-life case studies and applying new technologies such as gamification and virtual reality simulations are some of the innovations enhancing learning and teaching quality, with the outcome of students increased (Gulyamov et al., 2023). These innovations do not only make learning more engaging but also make students understand the intricacies of cyber law in a practical and relevant context.

This calls for narrowing the existing gap in education on cybersecurity skills. Much better educational frameworks that embrace innovative information applications, including remote laboratories and virtual classrooms, can play a distinctly important role in this respect. Advanced

learning tools and methodologies will also introduce the students to cope with the challenges thrown by the changing phenomenon of the cyber world.

CONCLUSION

This is one of the reasons this research was devoted to the topic of developing digital legal education for the purpose of nurturing cyber-security awareness and behavior in students. Collaboration between technology and legal education has grown in importance, providing new legal professionals with the skills and confidence to navigate in a world driven by digital technology. The article is full of arguments for this approach to cybersecurity education: one that will be more rounded than merely looking at the technicalities but would also put in place human-centered and ethical considerations.

Nevertheless, with all these advances in digital legal education, there are still significant gaps to be crossed: a basically human-centered approach in the curriculum of today, an absence of standardized educational frameworks, and generally low levels of practical exposure for students. If cybersecurity education is to meaningfully advance into the wider backdrop of legal education, then these are some of the basic gaps to be filled. By closing these gaps, the paper contributes to the ongoing discourse on improving cybersecurity education. It is a declaration that there should be a technical but ethically educated and considerate point of view from diversified origins. In its justification from a clear scientific perspective, therefore, this study espouses an interest in the embedding of human rights and digital ethics within cybersecurity education, relevant to the fostering of a safe and equal digital environment.

Future studies need to be advanced to explore the innovative pedagogical strategies up to and including the use of collaborative learning, simulations, and virtual reality in a bid to make cyber law education even more impactful. There is also the requirement for more experimentation, resulting in tools for advanced learning, which are much useful in preparing students for dynamic challenges in the cyber world. More critical initiatives, as delineated at the outset of this study, are required for broader goals to lead such efforts with a view to making the entire approach towards cybersecurity education more complete and really relevant globally.

REFERENCES

Alhadidi, I., Nweiran, A., & Hilal, G. (2024). The Influence of Cybercrime and Legal Awareness on the Behavior of University of Jordan Students. *Heliyon*.

Al-Janabi, S., & Al-Shourbaji, I. (2016). A study of cyber security awareness in educational environment in the middle east. *Journal of Information & Knowledge Management*, *15*(01), 1650007.

Altameem, A., Al-Ma'aitah, M., Kovtun, V., & Altameem, T. (2023). A computationally efficient method for assessing the impact of an active viral cyber threat on a high-availability cluster. *Egyptian Informatics Journal*, *24*(1), 61-69.

Antunes, M., Silva, C., & Marques, F. (2021). An integrated cybernetic awareness strategy to assess cybersecurity attitudes and behaviours in school context. *Applied Sciences*, *11*(23), 11269.

Aria, M., & Cuccurullo, C. (2017). bibliometrix: An R-tool for comprehensive science mapping analysis. *Journal of informetrics*, *11*(4), 959-975.

Aria, M., Le, T., Cuccurullo, C., Belfiore, A., & Choe, J. (2024). openalexR: An R-Tool for Collecting Bibliometric Data from OpenAlex. *R J.*, *15*(4), 167-180.

Bauling, A. (2023). Legal History as the Perfect Vessel: Teaching with Infographics for the Development of Digital Visual Literacy Skills in Law Students. *Potchefstroom Electronic Law Journal/Potchefstroomse Elektroniese Regsblad*, *26*(1), 1-50.

Bondarenko, S., Makeieva, O., Usachenko, O., Veklych, V., Arifkhodzhaieva, T., & Lernyk, S. (2022). The legal mechanisms for information security in the context of digitalization. *Journal of Information Technology Management*, *14*(Special Issue: Digitalization of Socio-Economic Processes), 25-58.

Cabaj, K., Domingos, D., Kotulski, Z., & Respício, A. (2018). Cybersecurity education: Evolution of the discipline and analysis of master programs. *Computers & Security*, *75*, 24-35.

Caulkins, B. D., Badillo-Urquiola, K., Bockelman, P., & Leis, R. (2016, October). Cyber workforce development using a behavioral cybersecurity paradigm. In *2016 International Conference on Cyber Conflict (CyCon US)* (pp. 1-6). IEEE.

Crabb, J., Hundhausen, C., & Gebremedhin, A. (2024, March). A Critical Review of Cybersecurity Education in the United States. In *Proceedings of the 55th ACM Technical Symposium on Computer Science Education V. 1* (pp. 241-247).

Cravens, D., & Resch, C. (2023, October). Comparison of Password Hygiene for Computer Science and Non-Computer Science Undergraduates. In *Proceedings of the 24th Annual Conference on Information Technology Education* (pp. 112-117).

Dawson, M. (2018). Applying a holistic cybersecurity framework for global IT organizations. *Business Information Review*, *35*(2), 60-67.

Drapezo, V. Y., Drapezo, R. G., Gritskevich, T. I., & Leukhova, M. G. (2022, February). Legal support of digital business: Competencies and tools training future lawyers. In *Proceeding of the International Science and Technology Conference" FarEastCon 2021" October 2021, Vladivostok, Russian Federation, Far Eastern Federal University* (pp. 885-892). Singapore: Springer Nature Singapore.

Fatokun, F. B., Hamid, S., Norman, A., & Fatokun, J. O. (2019, December). The impact of age, gender, and educational level on the cybersecurity behaviors of tertiary institution students: an empirical investigation on Malaysian universities. In *Journal of Physics: Conference Series* (Vol. 1339, No. 1, p. 012098). IOP Publishing.

Gernhardt, D., & Groš, S. (2022, May). Use of a non-peer reviewed sources in cyber-security scientific research. In *2022 45th Jubilee International Convention on Information, Communication and Electronic Technology (MIPRO)* (pp. 1057-1062). IEEE.

Gerontakis, G., Yannakopoulos, P., & Voyiatzis, I. (2023, November). Evaluating Cybersecurity Certifications: A Framework for Extracting Educational Scenarios in Cybersecurity Training. In *Proceedings of the 27th Pan-Hellenic Conference on Progress in Computing and Informatics* (pp. 243-248).

Gulyamov, S. S., Rodionov, A. A., Rustambekov, I. R., & Yakubov, A. N. (2023, June). The Growing Significance of Cyber Law Professionals in Higher Education: Effective Learning Strategies and Innovative Approaches. In *2023 3rd International Conference on Technology Enhanced Learning in Higher Education (TELE)* (pp. 117-119). IEEE.

Jackson, D. (2016). Human-centered legal tech: integrating design in legal education. *The Law Teacher*, *50*(1), 82-97.

Jacob, J., Peters, M., & Yang, T. A. (2020). Interdisciplinary cybersecurity: Rethinking the approach and the process. In *National Cyber Summit (NCS) Research Track* (pp. 61-74). Springer International Publishing.

Jagadeesan, S., Singh, D., Ojha, R., Ibrahim, R. K., & Alazzam, M. B. (2023, December). Implementation of an Artificial Intelligence with Cyber Security in E-Learning-Based Education Management System. In *2023 4th International Conference on Computation, Automation and Knowledge Management (ICCAKM)* (pp. 01-05). IEEE.

Jerman Blažič, B., & Jerman Blažič, A. (2022). Cybersecurity skills among European high-school students: A new approach in the design of sustainable educational development in cybersecurity. *Sustainability*, *14*(8), 4763.

Jones, E., Ryan, F., Thanaraj, A., & Wong, T. (2021). *Digital lawyering: Technology and legal practice in the 21st century*. Routledge.

Kallonas, C., Piki, A., & Stavrou, E. (2024, May). Empowering professionals: a generative AI approach to personalized cybersecurity learning. In 2024 IEEE Global Engineering Education Conference (EDUCON) (pp. 1-10). IEEE.

Kam, H. J., & Katerattanakul, P. (2014, October). Diversifying cybersecurity education: A non-technical approach to technical studies. In *2014 IEEE Frontiers in Education Conference (FIE) Proceedings* (pp. 1-4). IEEE.

Karasheva, Z., Assanova, S., Nurakhmetova, G., & Nuranova, R. (2024). Digital (Electronic) Paid Provision of Services in the Field of Legal Activity. *Law, State and Telecommunications Review*, *16*(1), 25-41.

Khan, F., Arora, S., Pargaien, S., Pande, L., & Khati, K. (2023, September). Exploring the Relationship Between Digital Engagement and Cybersecurity Practices Among College Students: A Survey Study. In *International Conference on MAchine inTelligence for Research & Innovations* (pp. 147-159). Singapore: Springer Nature Singapore.

Korobova, A. P., Volkova, N. A., & Rastoropova, O. V. (2022). Digital Transformation of Legal Education: Problems of Developing Competencies. In *Digital Technologies in the New Socio-Economic Reality* (pp. 849-857). Springer International Publishing.

Krundyshev, V., & Kalinin, M. (2021, April). Generative adversarial network for detecting cyber threats in industrial systems. In *Proceedings of International Scientific Conference on Telecommunications, Computing and Control: TELECCON 2019* (pp. 1-13). Singapore: Springer Singapore.

Lancu, E. A., TUȘA, E., Iancu, N., Simion, E., & Moise, A. C. (2023). Preventing computer crime by knowing the legal regulations that ensure the protection of computer systems. *Juridical Tribune/Tribuna Juridica*, *13*(3).

Makdee, S., Boontarig, W., & Puttasomsri, L. (2023, November). The Design and Implement of Digital Literacy Tracking System for Undergraduate Students. In *2023 7th International Conference on Information Technology (InCIT)* (pp. 503-507). IEEE.

Marksbury, N., & Bryant, E. A. (2019). Enter The Twilight Zone: The Paradox of The Digital Native. *Issues in Information Systems*, *20*(2).

Mukherjee, M., Le, N. T., Chow, Y. W., & Susilo, W. (2024). Strategic approaches to cybersecurity learning: A study of educational models and outcomes. *Information*, *15*(2), 117.

Pasvenskienė, A., & Astromskis, P. (2020). The future of legal education: do law schools have the right to be conservative? *Baltic Journal of Law & Politics*, *13*(1), 191-217.

Rodrigues, A. F., Monteiro, B. M., & Pedrosa, I. (2021, June). Cybersecurity risks: A behavioural approach through the influence of media and information literacy. In *2021 16th Iberian Conference on Information Systems and Technologies (CISTI)* (pp. 1-6). IEEE.

Sallos, M. P., Garcia-Perez, A., Bedford, D., & Orlando, B. (2019). Strategy and organisational cybersecurity: a knowledge-problem perspective. *Journal of Intellectual Capital*, *20*(4), 581-597.

Salminen, M., Candelin, N., Cullen, K., Latvanen, S., Lindroth, M., & Matilainen, T. (2023). Cybersecurity education in European higher education institutions.

Somabut, A., & Chaijaroen, S. (2017, July). Taxonomy for the design and development of learning environments to enhance Digital Literacy in higher education. IEEE.

Storr, C., & McGrath, C. (2023). In search of the evidence: digital learning in legal education, a scoping review. *The Law Teacher*, *57*(2), 119-134.

Tirumala, S. S., Sarrafzadeh, A., & Pang, P. (2016, December). A survey on internet usage and cybersecurity awareness in students. In *2016 14th annual conference on privacy, security and trust (PST)* (pp. 223-228). IEEE.

Yavorskiy, M. A., Milova, I. E., & Bolgova, V. V. (2020). Legal education in conditions of digital economy development: modern challenges. In *Digital Transformation of the Economy: Challenges, Trends and New Opportunities* (pp. 455-462). Springer International Publishing.

Yu, D. A. (2022). The educational potential of media content in the context of the formation of the individual legal culture. *Перспективы науки и образования*, (6 (60)), 583-597.