FACING A VUCA WORLD: STRENGTHENING CRIMINAL LEGAL PROTECTION FOR DISTANCE EDUCATION IN THE DIGITAL ERA

MJA Chandra[1], ZJ Fernando[2], PM Wahyuni[3]

[1, 3]*Universitas Terbuka (INDONESIA)*
[2]*Bengkulu University (INDONESIA)*

jeffri.chandra@ecampus.ut.ac.id

Abstract

In an era defined by Volatility, Uncertainty, Complexity, and Ambiguity (VUCA), the rapid advancement of digital technologies has reshaped both educational systems and the criminal legal landscape. Distance education, now integral to modern learning, faces unique threats, including cyber harassment, data breaches, digital fraud, and unauthorized access to online educational platforms. This study examines the urgent need for strengthened criminal legal protections specifically tailored to safeguard distance education in the digital age. It explores how criminal law must adapt to address these challenges, ensuring a safe and secure environment for educators and students alike. By analyzing primary, secondary, and tertiary sources, and employing positivist, interpretative, and critical approaches, this research identifies the primary criminal risks to distance education and evaluates existing legal frameworks for their effectiveness in the VUCA context. Findings reveal that the effectiveness of criminal law protections hinges on rapid adaptability, proactive policy-making, and robust technological integration. The study also underscores the importance of collaboration among educational institutions, law enforcement, and policymakers in creating a protective framework that responds to the complexities of digital threats. Key recommendations include updating criminal law provisions to address cyber-related educational crimes explicitly, enhancing digital literacy and awareness among educators and students, and implementing strict data protection standards. This research offers critical insights for policymakers, educational institutions, and legal professionals in developing a responsive and resilient legal framework for distance education, aimed at fostering a secure digital learning environment in a rapidly evolving world.

Keywords: VUCA, Criminal Legal Protection, Distance Education, Digital Era

1 INTRODUCTION

In the current era of globalization, humans are witnessing the emergence of new and unique challenges in the field of criminal law, which are triggered by rapid and significant changes in technology and digitalization.[1] The world humans now face is characterized by Volatility, Uncertainty, Complexity, and Uncertainty (VUCA), which creates a fast-moving and uncertain

foundation for the criminal legal system in Indonesia.[2] Entering the digital era has profound implications for the structure and function of criminal law. The emergence of cybercrime, other digital crimes, and digital law enforcement is creating a new paradigm in criminal law that demands rapid and flexible adaptation.[3] Therefore, assessing and understanding how criminal law can and must adapt in this VUCA world is essential to maintain its relevance and effectiveness.[4] First of all, one must consider the speed of technological change. Rapid developments in information and communications technology (ICT) have opened up space for new and complex crimes that were previously unimaginable. Cybercrime, which includes online fraud, identity theft, data hacking, and so on, poses significant challenges to traditional criminal laws generally designed to deal with conventional crimes.[5] Therefore, there is an urgent need to adapt and modernize criminal laws to remain effective in dealing with this new type of crime.

One of the main concerns in this environment is the rapid pace of technological change. Advances in information and communication technology (ICT) have opened up opportunities for complex and previously unimaginable crimes, many of which directly impact distance education. Cybercrimes, including online fraud, identity theft, and unauthorized access to educational platforms, pose significant challenges to traditional criminal law, which is generally designed to address conventional and physical crimes. Therefore, there is an urgent need to adapt and modernize criminal law to effectively protect distance education, ensuring a safe environment for students and educators in virtual learning spaces.

Then, we have to think about the uncertainties that arise from the complexity and dynamics of the VUCA world. In an ever-changing world, it is tough to predict what new types of crime will emerge and how they will develop.[6] This poses a significant challenge for policymakers and legal practitioners, who must always stay one step ahead of criminals in creating and implementing effective laws. To do so, they need a deep understanding of technology and social change and the flexibility to adapt to those changes. Furthermore, criminal law must also address the unique complexities associated with integrating this technology into distance education, where digital threats like cyber harassment and unauthorized access to online learning platforms can disrupt the educational process and compromise the safety of students and teachers alike..[7] In an increasingly digitalized society, the boundaries between the virtual and natural worlds are becoming increasingly blurred. This raises complex questions about jurisdiction, rights, and obligations and how to enforce the law in an increasingly integrated

world.[8] A multidisciplinary approach involving technologists, legal practitioners, and policymakers is critical to developing laws addressing these complex crimes.[9]

In addition, it is necessary to consider how to create a criminal law system that can handle the ambiguity that arises from a VUCA world. In an environment full of uncertainty and complexity, criminal law needs flexibility and adaptability to address changes and new challenges that continue to emerge.[10] This may involve developing new approaches to law enforcement, combining advanced technology and data analysis to create more effective and proactive law enforcement strategies. In the context of distance education, this flexibility is crucial, as new types of digital threats to students and educators require responsive and adaptive measures to ensure safety in online learning environments. Effective legal education for the general public, legal practitioners, and educators is more important than ever to achieve this. Providing information and training specifically tailored to the challenges faced in distance education can help build a better understanding of the potential and risks associated with criminal law in this digital era.

2 METHODOLOGY

This research is carried out by collecting primary, secondary, and tertiary sources of information and evaluating library resources or secondary data, which is also known as library research.[11] Positivism, interpretive, and critical techniques were used to search for answers or solutions to the problems developed through this research. The character of this research is descriptive-prescriptive, utilizing content analysis.[12]

3 RESULTS

In a modern-day horizon defined by Volatility, Uncertainty, Complexity, and Uncertainty, a phenomenon often summarized as a "VUCA World", the challenges faced by the criminal justice system are becoming increasingly multidimensional.[13] Facing this new reality requires intelligent and anticipatory adaptation in criminal law tools, which are now faced with threats that are increasingly dynamic and global in scale, especially those emerging from the digital space. Phenomena such as cybercrime, the spread of false information or disinformation, and other technology-related crimes have affected the way we administer justice and maintain social security.[14] In the context of distance education, these digital threats have unique implications, as online learning platforms become vulnerable to cyberattacks, disinformation, and unauthorized access, posing risks to both students and educators. Amid these rapid

fluctuations, criminal law must combine classical legal principles with innovations inspired by technology and social change to build a solid foundation in facing the challenges posed by the "VUCA World" and to safeguard the integrity and safety of distance education.

3.1 Cybersecurity and Data Protection in a VUCA world

In facing the dynamics of Volatility, Uncertainty, Complexity, and Ambiguity (VUCA), criminal law must evolve significantly to address the challenges of cybersecurity and data protection. Universal legal institutions are currently required to carry out in-depth revisions and substantial changes, considering that digital crimes such as fraud, identity theft, and malware attacks have become real and persistent threats in this digital era. In the context of distance education, these threats are particularly concerning, as online learning environments are increasingly targeted by cybercriminals who exploit vulnerabilities in educational platforms, thereby endangering the safety and privacy of students and educators. This is a domain where borderless transnational crime threatens individual and collective security, making a change in the legal paradigm necessary.[15]

In the latest report published by Id-SIRTII/CC, an institution operating under the auspices of the BSSN Cyber Security Operations Directorate, it has been revealed that Indonesia is facing increasing cyber security threats, with more than 1.6 billion incidents of traffic anomalies or attacks recorded. Cyber during 2021. This figure of 1,637,973,022 results from continuous 24/7 monitoring by the BSSN National Cyber Security Operations Center, carried out from January 1 to December 31, 2021.[16] The AwanPintar.id site has just published a report regarding cyber security in Indonesia during the first semester of 2023. The report entitled "Indonesia is Alert-Recognizing Digital Threats in Indonesia" reviews various trends in cyber attacks in Indonesia in depth. This report reveals several essential data regarding the level of cyber-attacks in Indonesia. Among the vital information contained in it is that around 347,172,666 cyber attacks were recorded in the first six months of this year, according to data released by AwanPintar.Indonesia experienced an average of 1,918,081 cyber attacks daily during the six months. This report also describes the ten main types of cyber attacks that most frequently hit Indonesia.[17]

How can criminal law be adapted to more effectively protect citizens from cybercrime, including fraud, identity theft, and malware attacks? First, the revision of criminal law should include the development of a clear and standardized definition of "cybercrime." In the field of distance education, this definition should also encompass crimes specifically targeting

educational platforms, such as unauthorized access to virtual classrooms, data theft from online learning systems, and cyber harassment of students or teachers. This broad definition would provide a solid legal foundation for prosecuting perpetrators. It is also essential to include stricter sanctions for those committing cybercrimes to create a deterrent effect and prevent repetition.

Additionally, the law must equip law enforcement with the tools and resources necessary to detect, investigate, and address cybercrime.[18] his may involve specialized training for members of the police and other law enforcement agencies, the development of dedicated cybersecurity units, and the creation of a national cyber monitoring center aimed at identifying and responding to cybersecurity threats in real time. In the context of distance education, specific training modules for cybersecurity units could be developed to address security threats unique to online learning platforms and digital classrooms, ensuring the safety of all participants. Inter-agency coordination at the national and international levels will be vital in dealing with increasingly complex and cross-border cyber threats.

In preventing and dealing with large personal data leaks, the main task is to build an ecosystem where citizens' data is protected legally and technically. This includes strengthening regulations regarding the management and use of personal data by government and private entities. Companies and organizations should be required to adopt strict data security standards, protect user information from unauthorized access, and ensure adequate incident response protocols to identify and respond to data leaks quickly.

Meanwhile, legal reform should include providing more efficient and effective legal avenues for victims of data breaches to seek redress. This includes streamlining legal processes to allow victims to sue companies or entities responsible for data leaks more easily. In the context of distance education, this might involve implementing protections for students' and teachers' data on educational platforms, allowing them to seek legal recourse in case of data breaches. Additionally, these updates should lead to the creation of an independent oversight body with the authority to oversee and ensure compliance with data protection laws. Furthermore, introducing criminal penalties for serious breaches of data protection law could effectively ensure that personal data is valued and protected seriously. This move, combined with widespread education and public awareness programs,

It is also essential to consider the role of technology in facilitating the implementation of criminal law in the digital era. New technologies such as artificial intelligence and extensive

data analysis can be used to assist in the early detection of data leaks and other cyber crimes.[19] In this case, the development of technology that supports cybersecurity must be balanced with efforts to ensure that the use of this technology does not interfere with individual rights and freedoms, including the right to privacy. In distance education, the use of AI for detecting and mitigating cyber threats on educational platforms must also prioritize protecting students' and educators' privacy and personal rights. Criminal law needs to adopt a dynamic and flexible approach to ensure this balance, allowing for rapid adaptation to technological changes and security threats.[20] This could include creating a legal framework that allows for rapid updates and adjustments to laws and regulations to ensure they remain relevant and effective in protecting society from ever-growing cybercrime. Overall, facing a VUCA world by adapting criminal law in the digital era is a complex but critical task. Through an innovative, collaborative, and proactive approach, we can create a more resilient and effective legal framework that protects citizens from cybercrime and personal data breaches while promoting justice, security, and prosperity for all, particularly in the rapidly expanding field of distance education.

3.2 Extradition, Criminal Law Jurisdiction in the Digital Era in a VUCA World

In an increasingly uncertain, complex, and ambiguous (VUCA) world, extradition procedures and criminal law jurisdiction in the digital era have become critical issues. In the digital era, crimes can occur across geographical boundaries, challenging the implementation of traditional laws.[21] Criminals can efficiently operate from other countries, making closer international cooperation in extradition essential to ensure that offenders can be prosecuted according to applicable law. In the context of distance education, these challenges are particularly relevant as cyber threats targeting online learning platforms can often originate from abroad, making international cooperation vital to protect students and educators from cross-border digital crimes. Meanwhile, criminal law jurisdiction in the digital era also requires significant adjustments. Laws should be able to encompass new aspects of digital crime, such as cybercrime, online fraud, and identity theft. With the rise of distance education, it is crucial that jurisdictional laws also address crimes specifically targeting educational platforms, including unauthorized access, data theft, and cyber harassment of students and instructors. This may require governments to collaborate with other parties, such as internet service providers and social media platforms, to track and identify digital criminals.[22] In addition, more dynamic legal adaptation is needed to consider the speed of change in the digital world,

including addressing new challenges such as using sophisticated encryption technology by criminals. Overall, facing a VUCA world requires a more holistic and integrated approach to addressing extradition and criminal law jurisdiction issues in the digital era. This includes creating a more adaptive legal framework that can respond swiftly to the latest technological developments and strengthening international cooperation to combat transnational crime in the digital world. Such an approach will be essential to ensure the safety and security of distance education platforms, fostering a protected online learning environment in a rapidly changing global landscape.[23]

Facing the challenges of a VUCA world in the context of extradition and criminal law jurisdiction in the digital era requires a strategic approach and concrete solutions. The following are some concrete solutions that Indonesia can adopt:

3.2.1 Establishment of a Special Cyber Security Unit

Establishing a particular unit trained to handle crimes in the digital era. This unit must have digital forensics expertise and work closely with similar institutions in other countries to facilitate the extradition process and cross-border law enforcement. For the education sector, this unit can provide added protection for online learning environments by addressing cyber threats specifically targeting distance education platforms.

3.2.2 Ratification of International Treaties

Accelerate the ratification process of international treaties dealing with transnational and cybercrime, such as the Budapest Convention on Cybercrime, which can facilitate inter-state cooperation in extradition and law enforcement. Such treaties would also be instrumental in safeguarding distance education platforms from cross-border digital crimes.

3.2.3 Modernization of the Law

Revise and modernize existing laws to ensure that they cover the latest digital crimes and enable the effective prosecution of individuals or groups involved in criminal activities in the digital world. This modernization should include provisions that specifically address cyber threats targeting educational institutions and online learning platforms.

3.2.4 Collaboration with the Private Sector

Strengthen cooperation with the private sector, especially internet service providers and social media platforms, in tracking and preventing digital crime. This can be through providing more

effective cybercrime reporting channels and cooperation in investigations. Such collaboration is crucial for enhancing security in distance education, where private platforms are often used.

3.2.5 Education and Public Awareness

Increase public education and awareness regarding digital crimes and how to protect themselves from these crimes. This can be done through public information campaigns and integrating cyber security education into the formal education curriculum. Distance education providers could also integrate cybersecurity training, ensuring that students and educators are aware of how to stay safe online.

3.2.6 Technology Infrastructure Development

Develop a technological infrastructure that enables more effective monitoring of criminal activity in the digital world and facilitates communication and coordination between different law enforcement agencies. This infrastructure should include tools for monitoring digital threats specific to online educational platforms to ensure a secure learning environment. Such adaptability would ensure that laws remain relevant in protecting students, educators, and educational institutions in the face of emerging digital threats.

3.2.7 Adaptable Legal System

Creating a legal system that can adapt quickly to technological developments by creating legal mechanisms that allow for rapid adjustment of regulations and statutes to respond to new challenges arising from technological evolution.

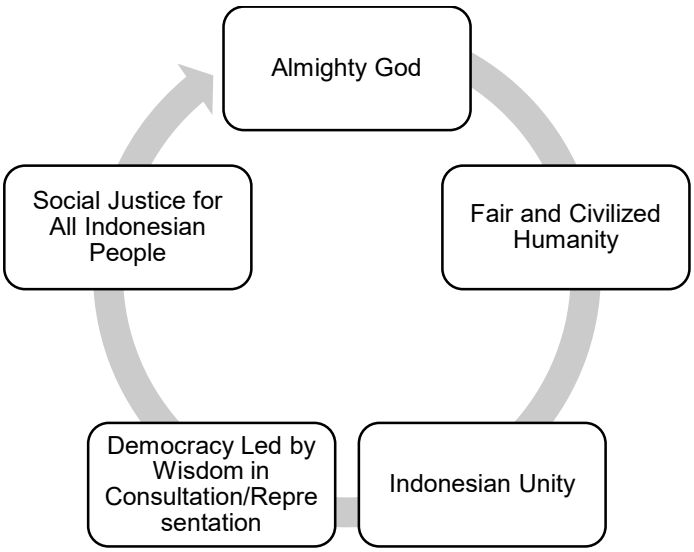
By implementing these concrete solutions, Indonesia can increase its ability to overcome the challenges of extradition and criminal law jurisdiction in the digital era in a VUCA world and create a society that is safer and more protected from the threat of digital crime.

3.3 Adaptation Strategy Facing a VUCA World and Legal Protection: Indonesian Perspective and the Role of Pancasila

Adapting to emerging content manipulation technologies such as deepfakes requires a multidisciplinary response integrating legal, technological, and social efforts.[24] From a criminal law perspective, this could involve the development of new laws that specifically target the creation and distribution of deepfakes with the intent to defraud or harm. These criteria ensure that only genuinely harmful behavior is regulated, while non-harmful artistic or innovative experiments are allowed free rein. In the context of distance education, this is especially important as deepfake technology can be misused to create fake lectures, manipulate educational content, or even impersonate educators, which poses risks to students and undermines trust in digital learning platforms. Developing targeted legal frameworks to address these risks will be crucial to maintaining a safe and trustworthy environment in online education.

In facing the VUCA world in Indonesia, adapting criminal law is not only a demand but also a necessity. The main focus of this process is to integrate the noble values of Pancasila in every element and process of criminal law.[25] In viewing Pancasila as a "grundnorm" and "staatfundamentalnorm", it is understood that Pancasila acts as a foundation that regulates the main principles of national and state life in Indonesia.[26] As a "grundnorm", Pancasila functions as a fundamental norm that influences and shapes Indonesia's legal framework. From this perspective, Pancasila carries the weight of noble values which are the essence of the identity of the Indonesian nation, directing the creation and implementation of other legal regulations which are in line with the five precepts which are the pillars of the state. Furthermore, as a "staatfundamental norm", Pancasila becomes the driving force that defines the state order, builds unity and harmony in a pluralistic society, and ensures that the government focuses on social justice and the welfare of all Indonesian people.[27] In the context of distance education, integrating Pancasila values into criminal law can help guide regulations aimed at protecting students, educators, and educational content from digital crimes. This alignment ensures that online learning environments remain safe and that educational justice is upheld, reflecting the spirit of Pancasila even in digital spaces. These two roles ensure that Indonesia grows as a country that is not only strong in its legal structure but also in maintaining and nurturing the values that reflect the character and aspirations of the Indonesian nation.

Figure 1. The values of Pancasila



a. First, in overcoming Volatility, criminal law must be more dynamic and flexible to respond to rapid social changes by constantly referring to the first principle of Pancasila, namely Belief in One Almighty God, which guides us to always stand on the values of truth and justice. In the context of distance education, this adaptability is crucial to address rapid technological changes that impact online learning platforms, ensuring that the values of truth and justice are maintained even in digital learning environments;
b. The uncertainty that characterizes a VUCA world requires criminal law that is more predictive and proactive. By instilling the second principle, Just and Civilized Humanity, criminal law in Indonesia must be able to protect the rights of citizens by promoting social justice and reducing legal uncertainty through consistent and fair law enforcement. For distance education, this means establishing proactive measures to protect students and educators from digital threats, ensuring a secure and just environment that respects the dignity and rights of all participants;
c. The complexity of various aspects of life today requires a more comprehensive legal strategy. Referring to the third principle, Indonesian unity, criminal law must work to maintain social harmony and integration, by placing common interests above all else, and trying to understand and overcome the root causes of various criminal acts that occur. In the context of distance education, this principle encourages criminal law to address the collective risks that digital threats pose to educational institutions, ensuring

that students and educators can participate in online learning in a safe, unified environment;

d. Overcoming uncertainty requires more precise and more transparent criminal law. Adopting the fourth principle, Democracy Led by Wisdom in Deliberation/Representation, criminal law must be more open in its decision-making process by providing more excellent space for community participation. In addition, by the fifth principle, Social Justice for All Indonesian People, criminal law must be committed to creating a just society where the interests of all levels of society are balanced. For distance education, this includes creating transparent legal processes that involve educators, students, and technology providers in discussions around safety and protection, ensuring that digital learning spaces align with the principle of social justice.

Thus, in facing a VUCA world, Indonesia must be able to design and adapt its criminal law to the values contained in Pancasila, thereby creating a legal system that is more adaptive, fair, and socially just.

In general, adapting criminal law in the digital era in the context of the VUCA world in Indonesia requires a dynamic, inclusive, and progressive approach aligned with the values and principles of Pancasila. This includes formulating laws that are responsive to technological developments, strengthening international cooperation to combat cross-border crime, and promoting effective legal education for the general public, legal practitioners, and distance education providers, thereby creating a safe, just, and prosperous environment for all Indonesian citizens.

4 CONCLUSIONS

In facing the dynamics and complexity of a world now characterized as volatile, uncertain, complex, and ambiguous (VUCA), Indonesia finds itself at a crucial point where legal innovation and adaptability become necessary, not an option. The results of this study explain the urgency for Indonesia to reform its criminal law so that it is more responsive and in-depth, including a deep understanding of technological developments and social evolution that are occurring at an unprecedented speed. In this context, the protection of distance education becomes an urgent area, as digital threats pose risks not only to personal data but also to the integrity of online learning environments. First and foremost, there is an urgent need to adapt and improve law enforcement approaches, focusing on effective legal education for both the

general public and legal practitioners. This includes integrating cybersecurity awareness in distance education to equip students and educators with knowledge about online threats and personal data protection, creating a culture of safety within digital learning environments. Developing responsive regulations for new types of crime, particularly in the cyber domain where crime is increasing rapidly, is essential. In this field, it is crucial to establish a clear and comprehensive definition of "cybercrime," accompanied by stricter sanctions for perpetrators, while still protecting individual rights and freedoms. In response to increasing digital security threats, Indonesia must enhance resources and training for law enforcement. This includes the creation of a specialized cybersecurity unit and a real-time monitoring center that works in an integrated manner to prevent mass data leaks and cyber threats. Such initiatives will be particularly beneficial for distance education, where online threats are prevalent, thereby fostering a secure digital environment for students and educators. Promoting closer cooperation at both national and international levels is also critical to address the cross-border nature of cybercrime effectively. Additionally, the management and protection of personal data must be revitalized through a more integrated approach, including the development of more effective legal mechanisms to assist victims of data leaks and the establishment of independent monitoring institutions. In the field of distance education, data protection is paramount, ensuring that the personal information of students and educators remains safe from unauthorized access or misuse. Amid these challenges, integrating Pancasila values into the legal framework continues to be an essential foundation for creating a dynamic, predictive, comprehensive, and transparent system. This integration establishes a necessary balance between regulating harmful behavior and allowing space for innovation and artistic expression. By upholding the principles of Pancasila, Indonesia’s grand vision is to create a safe, just, and prosperous society capable of navigating the challenges of the digital era through policies and actions guided by social justice and adaptability. In the sphere of distance education, aligning these values helps build a supportive and secure online learning environment that reflects Indonesia’s commitment to equity, justice, and mutual respect.

ACKNOWLEDGEMENTS

In developing this work, we have attempted to refer to various scientific sources that can provide new nuances and insights into legal issues in society. We are grateful to those who have helped us in this process, including book authors, journals, and others who have enriched the scientific content of this article. However, we realize this work is still imperfect and are open

to suggestions and constructive input from all parties. Despite its limitations, we hope this article can serve as a helpful reference source for academics, practitioners, and the general public when experiencing and studying legal cases.

REFERENCES

C. Belhadj Ali, "International Crimes in the Digital Age: Challenges and Opportunities Shaped by Social Media," Groningen J. Int. Law, vol. 9, no. 1, hal. 43–59, 2021, doi: 10.21827/grojil.9.1.43-59.

S. Deepti dan S. Sachin, "Managing in a VUCA World : Possibilities and Pitfalls Journal of Technology Management for Growing Economies Managing in a VUCA World : Possibilities and Pitfalls," J. Technol. Manag. Grow. Econ., vol. 11, no. 1, hal. 17–21, 2020, doi: https://doi.org/10.15415/jtmge.2020.111003.

E. Russkevich, "Palingenesis of Criminal Law in the Conditions of Digital Reality," Leg. Issues Digit. Age, vol. 1, no. 1, hal. 145–159, 2021, doi: 10.17323/2713-2749.2021.1.145.159.

F.-X. Roux-Demare, "Adaptation of the Penal Response to the Globalization of Criminality," GIDTP 2022 - Glob. Innov. Dev. Trends Prospect. 2022, vol. 18, no. Gidtp 2019, hal. 185–197, 2022, doi: 10.18662/lumproc/gidtp2022/19.

S. Mittal I.P.S. dan P. P. Sharma, "A Review of International Legal Framework to Combat Cybercrime," SSRN Electron. J., vol. 8, no. 5, hal. 1372–1374, 2017, doi: 10.2139/ssrn.2978744.

P. Ekblom, "Future Imperfect: Preparing for the Crimes to Come," Crim. Justice Matters, vol. 46, no. 1, hal. 38–40, Des 2001, doi: 10.1080/09627250108553670.

M. Gastaldi, "Integration of Mobile, Big Data, Sensors, and Social Media: Impact on Daily Life and Business," 2014 IST-Africa Conf. Exhib. IST-Africa 2014, 2014, doi: 10.1109/ISTAFRICA.2014.6880670.

Y. Razmetaeva, H. Ponomarova, dan I. Bylya-Sabadash, "Jurisdictional Issues in the Digital Age," Ius Humani. Law J., vol. 10, no. 1, hal. 167–183, 2021, doi: 10.31207/ih.v10i1.240.

F. Pocar, "New Challenges for International Rules Against Cyber-Crime," Eur. J. Crim. Policy Res. 2004 101, vol. 10, no. 1, hal. 27–37, Agu 2004, doi: 10.1023/B:CRIM.0000037565.32355.10.

A. Ashworth dan L. Zedner, "Defending the Criminal Law: Reflections on the Changing Character of Crime, Procedure, and Sanctions," Crim. Law Philos., vol. 2, no. 1, hal. 21–51, Jan 2008, doi: 10.1007/S11572-007-9033-2/METRICS.

Zico Junius Fernando et al, "The Freedom of Expression in Indonesia," Cogent Soc. Sci., vol. 8, no. 1, hal. 1–11, 2022, doi: 10.1080/23311886.2022.2103944.

E. Effendi, Z. J. Fernando, A. W. Anditya, dan M. J. A. Chandra, "Trading in Influence (Indonesia): A Critical Study," Cogent Soc. Sci., vol. 9, no. 1, hal. 4–5, Des 2023, doi: 10.1080/23311886.2023.2231621.

Y. Gao, Z. Feng, dan S. Zhang, "Managing Supply Chain Resilience in the Era of VUCA," Front. Eng. Manag. 2021 83, vol. 8, no. 3, hal. 465–470, Jun 2021, doi: 10.1007/S42524-021-0164-2.

S. Sulaeman, "The Application of Criminal Sanctions Against Violations of Cybercrime," Indones. Prime, vol. 2, no. 1, hal. 56–67, 2018, doi: 10.29209/id.v2i1.15.

R. Godson dan P. Williams, "Strengthening Cooperation Against Transnational Crime," Survival (Lond)., vol. 40, no. 3, hal. 66–88, Jan 1998, doi: 10.1093/survival/40.3.66.

Kompas.com, "Indonesia Hadapi 1,6 Miliar Serangan Siber dalam Setahun, Ini Malware Terbanyak," tekno.kompas.com/, 2022. .

Agustinus Mario Damar, "Serangan Siber ke Indonesia Capai 1,9 Juta Kali per Hari, Ini Daftar 10 Teratas Tipe Serangan," www.liputan6.com/, 2023. .

T. Kellermann, "Building a Foundation for Global Cybercrime Law Enforcement," Comput. Fraud Secur., vol. 2010, no. 5, hal. 5–8, Mei 2010, doi: 10.1016/S1361-3723(10)70051-8.

D. Maher, "Can Artificial Intelligence Help in the War on Cybercrime?," Comput. Fraud Secur., vol. 2017, no. 8, hal. 7–9, Agu 2017, doi: 10.1016/S1361-3723(17)30069-6.

B. Walker-Munro, "Cyber-Systemics, Systemic Governance and Disruption of the Criminal Law," Univ. Qld. Law J., vol. 39, no. 2, hal. 225–252, Agu 2020, doi: 10.38127/UQLJ.V39I2.5023.

J. Clough, "Principles of Cybercrime," Princ. Cybercrime, hal. 1–449, Jan 2010, doi: 10.1017/CBO9780511845123.

G. Gogolin dan J. Jones, "Law Enforcement's Ability to Deal with Digital Crime and the Implications for Business," J. Digit. Forensic Pract., vol. 3, no. 2–4, hal. 131–139, Des 2010, doi: 10.1080/15567281.2010.536737.

A. I. Cerezo, J. Lopez, dan A. Patel, “International Cooperation to Fight Transnational Cybercrime,” Work. Digit. Forensics Incid. Anal. Int., hal. 13–27, Agu 2007, doi: 10.1109/WDFIA.2007.7.

C. Campbell, K. Plangger, S. Sands, dan J. Kietzmann, “Preparing for an Era of Deepfakes and AI-Generated Ads: A Framework for Understanding Responses to Manipulated Advertising,” J. Advert., vol. 51, no. 1, hal. 22–38, Jan 2022, doi: 10.1080/00913367.2021.1909515.

M. C. Huda, “Strengthening Pancasila As National Ideology to Implementate The Balancing Values to Improve Law’s Application In Indonesia,” J. Pembaharuan Huk., vol. 5, no. 1, hal. 1–12, 2018.

F. Indra dan A. Budianto, “The Position of Pancasila as Legal Ideals and Source of All Legal Sources in Indonesia,” Proc. 1st Int. Conf. Law, Soc. Sci. Econ. Educ., hal. 1–9, 2021, doi: 10.4108/eai.6-3-2021.2306200.

Zico Junius Fernando et al, “Preventing Bribery in the Private Sector Through Legal Reform Based on Pancasila,” Cogent Soc. Sci., vol. 8, no. 1, hal. 4, 2022, doi: 10.1080/23311886.2022.2138906.