INTERNATIONAL JOURNAL OF FINANCIAL ECONOMICS (IJEFE) e-ISSN: 3063-3648
Vol. 2 No. 1 July 2025, page 144-152

CHALLENGES OF ECONOMIC LAW IN THE GLOBAL AND DIGITAL ERA: ANALYSING REGULATION, DATA PROTECTION, AND CYBERSECURITY THROUGH A LITERATURE REVIEW

Loso Judijanto
IPOSS Jakarta, Indonesia
losojudijantobumn@gmail.com

Abstract

The development of the digital economy in the era of globalisation has brought significant changes to the economic legal system, particularly in relation to regulation, data protection, and cybersecurity. This research aims to analyse the challenges of economic law in Indonesia in the face of digital transformation, with a focus on the effectiveness of regulations, implementation of personal data protection, and efforts to strengthen cybersecurity. The method used is a literature study with a juridical-normative approach, examining legislation, doctrine, and previous research results. The results of the study show that although Indonesia has a number of regulations such as the Personal Data Protection Law and regulations related to cybersecurity, their implementation still faces obstacles in the form of regulatory disharmony, weak law enforcement, and low digital literacy in society. In addition, the challenges of globalisation and rapid technological development require harmonisation of regulations across countries and increased capacity of human resources in the fields of law and technology. This research recommends strengthening the legal framework, increasing cross-sector collaboration, and public education to create a safe, fair and sustainable digital economy ecosystem.

Keywords: Digital economy law, regulation, personal data protection, cybersecurity, Indonesia

Introduction

The global and digital era has brought fundamental changes in various aspects of human life, including in the economic and legal fields. The development of information and communication technology, especially the internet, has accelerated the exchange of information, expanded the reach of businesses, and created new economic models that are no longer limited by conventional geographical boundaries. Economic digitalisation enables integration between business sectors, the emergence of business model innovations, and massive changes in consumption and production patterns (Nurdin & Rahman, 2024) .

In Indonesia, the digital economy is growing rapidly along with increasing internet penetration and adoption of digital technology in various sectors. Data shows that the number of MSMEs utilising digital platforms continues to grow, reflecting the huge potential of the national digital economy. This transformation not only drives economic growth, but also opens up new employment opportunities and strengthens

the nation's competitiveness in the global arena (Kuner, 2017) . However, behind these opportunities, increasingly complex legal challenges arise. Existing regulations often lag behind the pace of technological innovation, resulting in legal uncertainty for businesses and consumers. Economic law in the digital era must be able to adapt to the rapid dynamics of technology, in order to provide certainty, protection and justice for all parties involved (DeNardis, 2014) .

One of the key issues in digital economy law is the protection of personal data. The exchange of data across national borders, whether for business or social purposes, complicates the governance of data privacy and security. States are required to oversee not only physical territory, but also cyberspace, as trade in goods, services and information flows now rely heavily on digital data. Data protection is becoming increasingly crucial as personal data is a valuable asset that is vulnerable to misuse and cybercrime (Svantesson, 2015) .

Cybersecurity is also a major concern in the digital era. The increase in economic activity and online transactions makes cyberspace more vulnerable to digital crime threats, such as data theft, hacking, and online fraud. The state and businesses must collaborate to build a reliable security system to protect data and digital transactions from various risks. In addition, the globalisation of the digital economy requires harmonisation of regulations across countries. Differences in legal standards and policies between countries often become obstacles in digital-based international trade. Therefore, efforts to formulate global and transnational regulations are needed to create a conducive and competitive digital ecosystem (Pratama . , 2024)

Digital law not only regulates aspects of business and electronic transactions, but also includes the protection of intellectual property rights, privacy, and law enforcement for offences in cyberspace. Transnational standardisation of regulation and law enforcement is a challenge, given the borderless and highly dynamic characteristics of the digital world (Sari, 2025) .

On the other hand, technological developments such as artificial intelligence, big data and cloud computing also raise new ethical and legal issues. For example, the use of data for commercial or political purposes without user consent, as well as questions regarding legal liability for decisions taken by automated systems. This calls for updating regulations and adjusting legal principles to remain relevant and effective .

The Indonesian government has taken various steps to address this challenge, including through the drafting of the Personal Data Protection Law (PDP Law) and Presidential Regulation on cybersecurity. However, the implementation of these regulations still faces various obstacles, both in terms of infrastructure, human resources, and public awareness of the importance of data protection and digital security (Firdaus, 2024) .

In the global context, several countries have implemented progressive regulations such as the GDPR in the European Union and the Digital Privacy Consumer

Protection Act in Canada, which can be a reference for Indonesia in strengthening the legal framework of the digital economy. Case studies from these countries show the importance of a proactive and collaborative approach in formulating adaptive and responsive digital legal policies. Adjusting the law to technological developments is a must so that the law can still perform its function as a protector and regulator of people's lives. Legal principles such as fairness, openness and proportionality must be reinterpreted in the digital context, in order to respond to new challenges without hindering innovation and the growth of the digital economy (Darnia ., 2023)

This research aims to analyse the challenges of economic law in the global and digital era, focusing on aspects of regulation, data protection, and cybersecurity through a literature review. It is hoped that the results of this research can contribute to the development of digital economic law in Indonesia, as well as become a reference for policy makers, legal practitioners, and the wider community in facing a global and digital era full of challenges and opportunities.

Research Methods

The research method used in this research is a literature study with a juridical-normative approach, namely examining and analysing various legal sources such as legislation, doctrine, scientific journals, and academic literature relevant to economic law issues in the global and digital era (Eliyah & Aslan, 2025) . The data collected are primary legal materials (laws, regulations, court decisions) and secondary legal materials (books, articles, previous research results), which are then analysed qualitatively-descriptively to identify, interpret, and compare regulations, data protection, and cybersecurity in Indonesia and internationally. The analysis was conducted by reviewing the content of regulations, comparing relevant legal theories, and evaluating the implementation of legal policies in the digital economy in order to obtain a comprehensive understanding and provide constructive recommendations (Green et al., 2006) .

Results and Discussion

Challenges of Economic Law in the Global and Digital Era

The development of digital technology has fundamentally changed the economic landscape. Digitalisation is driving the birth of new business models, accelerating cross-border transactions and expanding market reach. However, these changes also bring complex legal challenges, especially in terms of regulation, data protection, and cybersecurity (Yusuf Daeng, 2023) . One of the main challenges is the speed of technological development that far outstrips the law's ability to adapt. Many regulations are still based on conventional economic paradigms, making them unable to anticipate the rapid dynamics of the digital economy. This causes a legal vacuum and uncertainty for businesses and consumers (Siregar, 2025) .

The globalisation of the digital economy also expands the scope of cross-border transactions. Differences in legal systems, regulatory standards, and policies between countries are often a barrier to enforcement. Overlapping jurisdictions and lack of regulatory harmonisation complicate international digital economy dispute resolution. Personal data protection has become a central issue in the digital era (Ramadan, 2024) . Cross-border data exchange and large-scale data processing pose risks of leakage, misuse and privacy violations. Although Indonesia already has a Personal Data Protection Law, its implementation still faces challenges such as low public awareness, limited infrastructure, and the need for harmonisation with global regulations such as GDPR (Syaputri et al., 2023) .

Cybersecurity is another crucial challenge. Increasingly sophisticated cyber attacks, such as data theft, hacking and online fraud, demand an adaptive and responsive legal system. Law enforcement against cybercrime is often hampered by the limited capacity of authorities, lack of technical expertise, and the cross-border nature of the crimes. In addition, the emergence of innovations in the digital financial sector such as fintech, e-wallets, and peer-to-peer lending also poses regulatory challenges. Many digital financial products and services are not yet fully regulated, potentially posing risks to consumers and financial system stability (Setiawan, 2024) .

Another challenge is the supervision and enforcement of anti-monopoly practices and unfair business competition in the digital realm. The dominance of large digital platforms can create imbalances in market power, hamper competition, and harm small businesses and consumers (Suari & Sarjana, 2023) .

In the context of sharia economic law, digitalisation requires regulatory adaptation to remain in accordance with sharia principles. Supervision of sharia compliance in digital transactions becomes more difficult, especially in relation to transparency, fairness, and the prohibition of usury or gharar practices (Wulandari, 2023) .

Economic law enforcement in the digital era also faces challenges in terms of evidence. Digital evidence is easily manipulated or deleted, so law enforcement officials need specialised expertise in digital forensics to ensure the validity and integrity of evidence. Limited human resource capacity in the field of law and technology is another obstacle. Law enforcement officials, regulators and businesses need to improve their digital literacy and understanding of digital economy legal issues to effectively respond to the challenges (Peng, 2024) .

The next challenge is the protection of intellectual property rights (IPR) in the digital era. The rapid and easy-to-duplicate spread of digital works demands a stronger and more adaptive IPR protection system, both at the national and international levels. Globalisation also poses a risk of legal homogenisation that could threaten national legal sovereignty. Indonesia needs to balance the adoption of global standards and the protection of national interests in formulating digital economy regulations. Cross-

sectoral and international collaboration is key in facing the legal challenges of the digital economy. The government, private sector and society must work together to build a safe, fair and sustainable digital ecosystem (Tikk et al., 2017) .

Finally, new ethical and legal challenges arise as technologies such as artificial intelligence, big data and blockchain evolve. Issues of legal liability for automated decisions, use of data for commercial purposes without consent, and the potential discrimination of algorithms are important concerns that must be anticipated in future regulations.

Thus, facing these challenges requires regulatory updates, increased law enforcement capacity, public education, and strengthened international cooperation. Only with strategic and collaborative measures can the economic legal system remain relevant and effective in the evolving global and digital era.

Regulatory Effectiveness, Data Protection, and Cybersecurity in Indonesia

The development of the digital economy in Indonesia has encouraged the government to strengthen regulations in the fields of digital economy, personal data protection, and cybersecurity. Regulation is an important foundation in overseeing the growth of the digital economy, protecting consumers, and maintaining the stability and security of the national digital ecosystem. However, the effectiveness of these regulations still faces various complex challenges (Zarsky, 2017) .

Digital economy regulation in Indonesia has progressed with the issuance of a number of regulations, such as OJK Regulation on fintech, Government Regulation on electronic transactions, and Personal Data Protection Law (PDP Law). However, existing regulations are often unable to keep up with the dynamics and speed of digital technology innovation. This has led to disharmony between institutions, weak law enforcement, and low digital literacy among the public and business actors (Putra, 2023).

The effectiveness of digital economy regulations is also affected by the inequality of digital infrastructure in Indonesia. In urban areas, digital technology adoption and compliance with regulations tend to be better compared to rural areas which still face limited internet access and other supporting infrastructure. This inequality has an impact on the uneven implementation of regulations and legal protection throughout Indonesia (Sahputra ., 2022)

In the context of personal data protection, Indonesia already has a PDP Law that provides a clear and comprehensive legal framework regarding the rights and obligations of owners and managers of personal data. However, the effectiveness of the PDP Law is still constrained by weak law enforcement, low business compliance, and lack of effective supervision. Cases of personal data leaks still occur frequently, both in the public and private sectors, signalling the need to strengthen supervision and stronger sanctions (Greenleaf, 2021) .

One of the main challenges in data protection is the low awareness of the public and businesses on the importance of personal data protection. Many businesses, especially MSMEs, do not fully understand the legal obligations related to personal data management. The government needs to increase education and socialisation on the PDP Law so that compliance and data protection can run optimally. In addition, the establishment of an independent and strong data protection supervisory institution is key to the effectiveness of the PDP Law (Sulaiman, 2024) . To date, the supervisory institution mandated by the PDP Law has not been fully established and functioning optimally. Without strict and transparent oversight, the implementation of the PDP Law risks becoming a mere formality with no real power to protect citizens' privacy rights (Bygrave, 2017) .

Cybersecurity is becoming an increasingly crucial issue as digital economic activities and online transactions increase. The government has established the National Cyber and Crypto Agency (BSSN) and issued a number of regulations to strengthen national cyber security. However, the effectiveness of these efforts still faces obstacles, such as a lack of experts, limited digital forensic technology, and weak coordination between law enforcement agencies (Chander & Sun, 2015) .

Law enforcement against cybercrime in Indonesia is also still not optimal. Many cybercrime cases are difficult to uncover and handle due to the limited capacity of law enforcement officials, complicated judicial processes, and lack of coordination between relevant agencies. To improve the effectiveness of law enforcement, specialised training, increased budgets, and the provision of more sophisticated technology are needed for law enforcement officials (Moerel ., 2013)

Cybersecurity audits in Indonesian companies show that audit effectiveness has a positive effect on the maturity level of cybersecurity risk management. However, there are still many companies that do not have an adequate cybersecurity audit system, making them vulnerable to attacks and data leaks. Improving audit and risk management is an important step in strengthening national cybersecurity (Kaffah & Badriyah, 2024) .

Cross-sector and international collaboration is also urgently needed to deal with cyber threats that cross national borders. Indonesia needs to strengthen public-private partnerships, increase participation in regional cybersecurity initiatives such as ASEAN, and adopt international standards to strengthen the national cybersecurity ecosystem. Another challenge faced is the low level of digital literacy in society. Many internet users in Indonesia do not understand cybersecurity risks and the importance of personal data protection (Nurdin & Rahman, 2024) . Digital education and literacy must be prioritised so that people can participate safely and responsibly in the digital ecosystem. The digital divide between urban and rural areas also worsens the effectiveness of regulation and legal protection. The government needs to expand digital infrastructure, improve

internet access, and provide technical support to MSMEs to optimally comply with regulations and protect consumer data (Kuner, 2017) .

Despite progress in regulation and data protection, Indonesia still faces major challenges in implementation and enforcement. Legal reforms, capacity building, and adaptive regulatory updates are urgently needed to keep pace with technological advancements and the evolving dynamics of cyber threats (DeNardis, 2014) .

Overall, the effectiveness of regulation, data protection, and cybersecurity in Indonesia relies heavily on the synergy between the government, businesses, and the public. Joint efforts in strengthening regulations, improving digital literacy, and building a resilient cybersecurity ecosystem will be the key to Indonesia's success in facing the challenges of the digital economy in the global and digital era.

Conclusion

The challenges of economic law in the global and digital era are complex and multidimensional. The rapid development of digital technology has changed the pattern of economic transactions, expanded market reach, and created new business models that are often not fully accommodated by existing regulations. Legal lag in keeping up with technological innovation, jurisdictional differences between countries, as well as difficulties in proof and law enforcement are the main obstacles in creating a fair and safe digital economic ecosystem.

The effectiveness of regulations in Indonesia, especially those related to personal data protection and cybersecurity, still faces various challenges. Despite the issuance of a number of regulations such as the Personal Data Protection Law and the strengthening of the cybersecurity legal framework, their implementation is often not optimal due to weak law enforcement, lack of digital literacy, and limited infrastructure and human resources. The increasing cases of data leaks and cyberattacks show the need to strengthen supervision, cross-sector collaboration, and update regulations that are adaptive to the dynamics of digital threats.

Overall, adjusting the law to technological developments is a must so that the law remains relevant and effective in protecting people's rights and encouraging digital economic innovation. Synergy between the government, business actors, and the community is needed to strengthen regulations, improve digital literacy, and build a robust cybersecurity ecosystem. With strategic and collaborative steps, Indonesia can optimally utilise the opportunities of the digital economy without neglecting aspects of legal protection and security.

References

Bygrave, L. A. (2017). Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements. *Oslo Law Review*, *4*(2), 105–120. https://doi.org/10.5617/oslaw2760

Chander, A., & Sun, H. (2015). Data Nationalism. *Emory Law Journal*, *64*(3), 677–739. https://doi.org/10.2139/ssrn.2412352

Darnia, M. E. (2023). Perlindungan Hak Kekayaan Intelektual di Era Digital. *JERUMI: Journal of Education Religion Humanities and Multidiciplinary*, *1*(2), 411–419. https://doi.org/10.57235/jerumi.v1i2.1378

DeNardis, L. (2014). The Global War for Internet Governance. *Yale University Press*. https://doi.org/10.12987/yale/9780300181357.001.0001

Eliyah, E., & Aslan, A. (2025). STAKE'S EVALUATION MODEL: METODE PENELITIAN. *Prosiding Seminar Nasional Indonesia*, *3*(2), Article 2.

Firdaus, R. A. (2024). Perlindungan Hukum dan Pencegahan Kejahatan Siber di Era Digital dalam Sistem Hukum di Indonesia. *Staatsrecht: Jurnal Hukum Kenegaraan Dan Politik Islam*, *4*(1), 80–94. https://doi.org/10.38043/jah.v6i1.4484

Green, B. N., Johnson, C. D., & Adams, A. (2006). Writing Narrative Literature Reviews for Peer-Reviewed Journals. *Chiropractic & Manual Therapies*, 52–57.

Greenleaf, G. (2021). Global Data Privacy Laws 2021: Despite COVID Delays, 145 Laws Show GDPR Dominance. *Privacy Laws & Business International Report*, *170*, 10–13. https://doi.org/10.2139/ssrn.3786754

Kaffah, A. F., & Badriyah, S. M. (2024). Aspek Hukum Dalam Perlindungan Bisnis Era Digital Di Indonesia. *Lex Renaissance*, *9*(1), 203–228. https://doi.org/10.20885/JLR.vol9.iss1.art10

Kuner, C. (2017). The Internet and the Global Reach of EU Law. *International Data Privacy Law*, *7*(2), 73–76. https://doi.org/10.1093/idpl/ipx008

Moerel, L. (2013). Big Data Protection: How to Make the Draft EU Regulation on Data Protection Future Proof. *International Data Privacy Law*, *3*(2), 74–84. https://doi.org/10.1093/idpl/ipt007

Nurdin, M., & Rahman, A. (2024). Zakat dan Transformasi Digital: Tantangan dan Peluang Pengelolaan Zakat Era Modern Berdasarkan Perspektif Hukum Syariah. *Jurnal Hukum Ekonomi Syariah*, *4*(1). https://doi.org/10.24239/jhes.v4i1.11217

Peng, S. (2024). International Economic Law in the Era of Datafication. *International Journal of Law and Information Technology*, *33*, eaae031. https://doi.org/10.1093/ijlit/eaae031

Pratama, A. (2024). Studi dokumentasi pada kebijakan ekonomi Indonesia dalam menghadapi ketidakpastian global. *COSTING: Journal of Economic, Business and Accounting*, *7*(6). https://doi.org/10.31539/costing.v7i6.13424

Putra, A. (2023). Analisis Dampak Kerjasama Indonesia Chile CEPA Terhadap Neraca Perdagangan. *Jurnal Ekonomi Dan Bisnis*, *11*. https://doi.org/10.31258/jeb.11.1.15

Rahmawati, D. (2024). Relevansi dan Tantangan Penerapan Prinsip Ekonomi Syariah dalam Pengembangan Ekonomi Syariah di Era Digital. *Jurnal Rumpun Manajemen Dan Ekonomi*, *1*(3), 143–156.

Ramadhan, F. (2024). Peran Hukum Ekonomi dalam Menjamin Keberlanjutan Bisnis dan Stabilitas Pasar di Era Digital. *Jurnal Ilmiah Ekonomi Syariah Dan Pasar Modal*, *3*(2), 224–229. https://doi.org/10.54180/jiesp.2024.3.2.224-229

Sahputra, A. (2022). Harmonization of Digital Laws and Adaptation Strategies in the Era of Globalization. *Innovative: Journal Of Social Science Research*, *3*(6), 2880–2897. https://doi.org/10.37253/innovative.v3i6.8240

Sari, D. (2025). Konsep dasar ekonomi internasional dan teori perdagangan internasional. *Socius: Jurnal Pendidikan Dan Pembelajaran Ilmu Pengetahuan Sosial*, *2*(10), 116–122. https://doi.org/10.5281/zenodo.15387779

Setiawan, B. (2024). Model Penanganan Kejahatan Teknologi Finansial (Fintech) di Era Digital 4.0. *Positum: Jurnal Hukum*, *8*(1).

Siregar, R. (2025). Perdagangan Internasional di Era Digital: Tantangan dan Peluang. *Jurnal Inovasi Manajemen, Kewirausahaan, Bisnis Dan Digital*, *2*(1), 71–93. https://doi.org/10.61132/jimakebidi.v2i1.457

Suari, K. R. A., & Sarjana, I. M. (2023). Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia. *Jurnal Analisis Hukum*, *6*(1), 132–142. https://doi.org/10.38043/jah.v6i1.4484

Sulaiman, A. (2024). Ekonomi Islam di Era Digital: Peluang dan Tantangan dalam Dunia Bisnis Modern. *Ekonomis: Journal of Economics and Business*, *8*(2).

Svantesson, D. J. B. (2015). The Extraterritoriality of EU Data Privacy Law – Its Theoretical Justification and Its Practical Effect on Global Business. *International Data Privacy Law*, *5*(4), 246–262. https://doi.org/10.1093/idpl/ipv021

Syaputri, D., Azzahra, F. R., Vidia A.Z, S., Raihan, M., Prestianto, V. A., Fadilah, Z. R., & Mustaqim. (2023). Pengaruh Digitalisasi dalam Pembangunan Hukum Ekonomi di Indonesia. *Jurnal Pendidikan Tambusai*, *7*(3), 31414–31421. https://doi.org/10.31004/jptam.v7i3.12127

Tikk, E., Kaska, K., & Vihul, L. (2017). International Cyber Norms: Legal, Policy & Industry Perspectives. *NATO Cooperative Cyber Defence Centre of Excellence*. https://doi.org/10.2139/ssrn.2949845

Wulandari, S. (2023). Literasi Hukum Ekonomi Syariah di Era Digital dan Kontribusinya bagi Penguatan Ekonomi Syariah di Indonesia. *Al-Huquq: Jurnal Studi Hukum Ekonomi Syariah*, *5*(1). https://doi.org/10.19105/alhuquq.v5i1.5729

Yusuf Daeng. (2023). Perlindungan Data Pribadi dalam Era Digital: Tinjauan Terhadap Kerangka Hukum Perlindungan Privasi. *Innovative: Journal Of Social Science Research*, *3*(6), 2898–2905. https://doi.org/10.37253/innovative.v3i6.8240

Zarsky, T. Z. (2017). Incompatible: The GDPR in the Age of Big Data. *Seton Hall Law Review*, *47*(4), 995–1020. https://doi.org/10.2139/ssrn.2992766