International Journal of Sociology and Law
Volume. 1 No. 4 November 2024
e-ISSN : 3047-0692, and p-ISSN : 3047-1923, Page. 144-153
DOI : https://doi.org/10.62951/ijsl.v1i4.179
Available online at: https://international.appihi.or.id/index.php/IJSL

Legal Obligations by Companies in Mitigating the Risks of Sustainable Digital Innovation

Gilang Indra[1], Wieke Dewi Suryandari[2], Mohamad Tohari[3]
Darul Ulum Islamic Centre Sudirman GUPPI University, Indonesia[1, 2, 3]
Email : gilangindrafr44@gmail.com[1], wiekedewi11@gmail.com[2], mohamadtohari.undaris@gmail.com[3]

Abstrak : Address : Road. Student Army, Paren, Sidomulyo, Ungaran Tim. District, Semarang Regency, Central Java 50519, Indonesia
Author correspondence : gilangindrafr44@gmail.com

Abstract. Digital innovation offers myriad advantages to companies but also entails risks necessitating mitigation. To safeguard against adverse impacts on both the company and its consumers, adherence to legal obligations is imperative. Privacy and security risks pose potential economic, ethical, or legal ramifications for consumers and companies alike. The duty to safeguard personal data is shared between governmental bodies and companies, with the latter assuming primary responsibility as service providers. Ethical business conduct entails the protection of user data and transparent disclosure of data usage to users. Companies also need to consider human, technological, and environmental aspects before developing new technologies. Therefore, awareness from companies is needed to fulfill their digital social responsibility. The latest regulation is Law Number 27 of 2022 concerning Personal Data Protection. Personal data protection is one of the main focuses of Corporate Digital Responsibility (CDR) or Corporate Digital Responsibility. The CDR concept is an evolution of Corporate Social Responsibility adapted to the digital era. In CDR, companies are expected to adopt practices that consider digital culture. It can be an effective strategy to integrate business and government interests in efforts to protect digital users.

Keywords: Corporate Responsibility; Digital Innovation; Sustainability.

1 INTRODUCTION

Industry 4.0 brings significant change by shifting focus towards digital technology, artificial intelligence, and the Internet of Things (IoT), revolutionizing approaches to sustainability. These technologies bridge the physical and digital worlds, enabling more efficient solutions and real-time resource monitoring. With artificial intelligence and data analytics, decision-making becomes more precise, enhancing energy efficiency and supply chain management. In the context of intensifying competition, this inevitable shift towards digitization is known as the "digital imperative."

Digital transformation is a process driven by digital technology, which generates new business models and has the potential to disrupt markets and industries worldwide. The process disrupts organizations and has significant impacts on value creation, strategies, and organizational structures. With digital transformation in business, several management practices undergo changes, which in turn can affect organizational sustainability. The formation of digital organizations is the outcome of this transformation, with artificial intelligence and computational assets becoming primary assets that reshape growth trajectories.

Received: June 12, 2024; Revised: July 18, 2024; Accepted: August 20, 2024; Online Available: August 22, 2024;

Digital innovation offers numerous benefits to companies, but it also brings risks that need to be mitigated. To ensure that these risks do not adversely affect the company and its consumers, legal obligations must be fulfilled. The following are some legal obligations by companies in mitigating sustainable digital innovation risks:

a. Personal Data Protection

   Companies must protect consumers' data by applicable laws and regulations, such as the General Data Protection Regulation (GDPR) in Europe or the Personal Data Protection Law in Indonesia. It includes securely and transparently collecting, storing, using, and sharing data.

b. Cybersecurity and Information System Security

   Companies must implement strong cybersecurity measures to protect their information systems from hacking, data theft, and other cyber attacks. This includes using encryption, two-factor authentication, and monitoring suspicious activities.

c. Compliance with Regulations

   Companies need to comply with all applicable regulations and laws related to digital innovation, including those concerning intellectual property rights, electronic transactions, and sector-specific regulations such as financial services or healthcare.

d. Risk Management

   Companies must have a risk management system to identify, evaluate, and mitigate risks associated with digital innovation. This includes risk analysis, vulnerability assessment, and emergency response planning.

e. Transparency and Communication

   Companies must be transparent with consumers about how digital innovations are used and the potential risks involved. They must also provide clear communication for handling complaints or issues.

f. Employee Training and Awareness

   Companies must ensure their employees are well-trained in cybersecurity, data protection, and compliance with regulations. Employee awareness can help reduce the risk of human error.

g. Collaboration with Authorities and Third Parties

   Companies should collaborate with relevant authorities and third parties to ensure compliance with laws and regulations. It includes cooperation in investigations or audits if necessary.

h. Safe and Ethical Use of Technology

Companies must ensure that the technology they use is safe and ethical. It includes responsibly using artificial intelligence, data analytics, and other innovative technologies.

i. Handling and Resolving Issues

Companies must have clear procedures for handling and resolving issues in case of violations or incidents. It includes investigation, notification to affected parties, and necessary corrective actions.

By fulfilling these legal obligations, companies can reduce the risks of digital innovation and ensure that their activities not only comply with the law but also maintain consumer trust and security. One significant change brought about by the advancement of digital technology in the business world is the emergence of artificial intelligence that manipulates and manages user information. Additionally, digital transformation also benefits companies by simplifying various aspects of operations, from production to distribution, at lower costs. Companies can also leverage machine learning technology to analyze consumer behavior, design effective sales and marketing strategies, and predict future sales trends.[3]

With this technology, companies can collect vast amounts of public data, but this also presents its own challenges in managing and protecting such data. However, in reality, many companies are less responsible in their use of public data, often because they perceive data protection as the responsibility of others or regulators. Ethically, digital responsibility should compel companies to create value and a business image that is trustworthy by consumers and investors.

Privacy and security risks can have economic, ethical, or legal implications for consumers and companies. Legal regulations governing social responsibility are outlined in Law Number 40 of 2007 concerning Limited Liability Companies and Government Regulation Number 47 of 2012 concerning Corporate Social and Environmental Responsibility. The concept of social responsibility, or Corporate Social Responsibility (CSR), regulated in these regulations, is conventional and has not yet adapted to technological and digital developments. Data breaches caused by companies are now under scrutiny by the government, especially concerning Law Number 11 of 2008 concerning Information and Electronic Transactions, which states that the use of personal data can only be done with the consent of the individual concerned or under regulations. Furthermore, Law Number 24 of 2013 concerning Population Administration

stipulates that the publication of personal data without authorization can be punished by imprisonment for up to 2 years and a fine of IDR 25,000,000.

The responsibility to protect personal data should be shouldered by both the government and companies. Companies, as service providers, bear the greatest responsibility in this regard. They need to conduct business ethically by safeguarding user data and providing transparent explanations to users about how their data will be used. Companies should also consider human, technological, and environmental aspects before developing new technologies. Therefore, awareness from companies is necessary to fulfill their digital social responsibility. The latest law regulating personal data protection is Law Number 27 of 2022 concerning Personal Data Protection.[4]

Personal data protection is one of the main focuses of Corporate Digital Responsibility (CDR) or Corporate Digital Responsibility. The CDR concept is an evolution of Corporate Social Responsibility adapted to the digital era. In CDR, companies are expected to adopt practices that consider digital culture. It can be an effective strategy to integrate business and government interests in efforts to protect digital users.

Based on the background description above, the interesting legal issue is: What are the Legal Obligations of Companies in Mitigating Sustainable Digital Innovation Risks?

2 METHOD

Method

The research method employed in this writing is normative legal research, which involves studying library materials or secondary data. The approach used is a normative juridical approach with a descriptive-analytical nature.

Approach

The normative approach is a method used to examine issues within the context of law and legal regulations, including rules that can be used as a basis for examining issues and their legal consequences. In this case, an example is Law Number 27 of 2022 concerning Personal Data Protection. The normative approach is applied to specific regulations or written laws related to the concept of Legal Obligations by Companies in Mitigating Sustainable Digital Innovation Risks. The research describes the object being studied, focusing on regulations and legal protection concepts related to corporate responsibility in the digital era.[6]

3 RESULT AND DISCUSSION

Legal Obligations by Companies in the digital era

The application of digital technologies in various social contexts creates new opportunities, work methods, and communication mechanisms and changes the way some daily activities are carried out. Technology is now a factor that needs to be considered by both individuals and organizations, both private and government sectors. However, technology can also have negative impacts. For example, it can lead to job instability and unemployment, communication problems, or excessive social interaction. This duality of technology's impact in various social contexts has sparked debate about the use, relevance, and relationship between technology and humans in society.

The development of digital technology has created a variety of systems with extraordinary capabilities. Currently, we are witnessing a transition towards artificial intelligence (AI) systems and Machine Learning Data technology which plays an important role in various industries around the world. This digital transformation makes it easier for companies to carry out various activities, from production to distribution, more efficiently and at lower costs. Companies can also utilize machine learning data technology to analyze consumer behavior, design effective sales and marketing strategies, and even predict future sales trends.

Digital transformation also brings convenience to consumers, from the ordering and payment process until the goods reach their hands, making the use of digital technology increasingly widespread and massive. The use of digital technology is now increasingly intensive. Currently, many activities are carried out online, without direct human interaction. This condition allows companies to obtain and manage large amounts of public data through digital technology, which in turn creates challenges for companies in managing this data and ensuring its security.

Many companies consider that the responsibility for protecting consumer data is the government's job, so they often do not have clear internal guidelines or policies regarding consumer data protection. This has led to an increase in cybercrime related to consumer data breaches. Although Law Number 27 of 2022 concerning Personal Data Protection requires data managers, including companies, to comply with laws and regulations related to data protection, the problem is not only about legal compliance but also about ethical aspects. The law does not provide clear ethical obligations for companies in managing consumers' data, only providing

administrative and criminal sanctions. Existing data protection policies are often ineffective, and as a result, companies do not feel they have much responsibility in managing and using consumer data, because they consider data protection to be the government's responsibility.

Companies that continue to innovate in technology to face the future must not forget the values that underlie the vision of the future they want to create. If they forget this, the company's social vision can be neglected. Thus, the issue of costs and benefits of technology can become a social issue. In the laws and regulations governing corporate ethical responsibilities, there are no specific obligations that require companies that use digital technology to comply with certain ethical standards. In particular, there is no obligation for companies, developers, individual designers, or corporate actors who use digital technologies or data processing to be aware that the activities they undertake or the data they collect and process may give rise to ethical responsibilities for them.

Corporate responsibility in using digital technology, including data management, cyber security, and the impact of technology on society and the environment, is the focus of Corporate Digital Responsibility (CDR). CDR covers various aspects related to a company's digital activities and aims to ensure that the use of technology has a positive impact or is at least not harmful. This is an expansion of the concept of Corporate Social Responsibility (CSR) which specifically addresses digital issues. CDR is becoming increasingly important along with the digitalization of companies today, where activities from production to distribution are carried out digitally. Therefore, companies need to be responsible for the impacts of digitalization, including protecting consumer data and other actions related to their digital activities.

In recent years, Indonesia has experienced several cybercrime incidents affecting various entities, including state-owned companies, private companies, and government agencies. However, the response from companies and government agencies is often seen as lacking the ability to build public trust, and sometimes data security does not appear to be taken seriously. Even though laws governing data security already exist, being responsible and implementing good practices remains an important factor in overcoming this problem. The concept of Corporate Digital Responsibility (CDR) is still relatively new and requires further study before it is widely implemented in Indonesia. Nevertheless, the potential utility of this concept for corporations and governmental bodies in upholding the security and confidentiality of individuals' data remains conspicuous. Through the adoption of Corporate Digital Responsibility (CDR), these entities can foster a culture of responsibility and proactivity,

thereby adeptly addressing challenges stemming from advancements in digital technology, particularly those concerning data safeguarding.

By implementing the concept of Corporate Digital Responsibility (CDR), companies and government agencies can build a better work culture, increase awareness of digital security, and take proactive steps to protect user data. This approach can help create an environment where data security is a top priority, and ensure that every action taken by companies or government agencies reflects their responsibility to society and service users. Through CDR, companies and government agencies are expected to be able to integrate data security and digital ethics into every aspect of their operations, providing more trust to consumers, and contributing to overall digital security.

Efforts to Mitigate the Risks of Digital Innovation in Companies

The development of technology and digital systems has penetrated various sectors of life, from trade, finance, government, and tourism, to transportation. This interaction involves various stages, from storage, processing, data collection, and delivery, to production between industry and society. In this context, access to personal data becomes very important to ensure smoothness and efficiency in every transaction. Personal data is now considered a valuable asset that has high economic value in the big data era, making it vulnerable to being targeted by parties seeking profit alone. Attempts to make unauthorized use of personal data can involve a range of actions, including theft, dissemination, sale, and use of the data without the permission of the owner.[9]

Personal data protection was first stated in the 1945 Constitution, Article 28G, which states that every person has the right to personal protection, family, honor, dignity, and property under his or her control, and has the right to a sense of security and protection from the threat of fear of do or not do something that is a human right. Personal data protection is a fundamental task for the Indonesian government to produce legal protection regulations and maximize the role of law enforcement officials to guarantee the constitutional rights of all citizens.

Personal data protection also involves the Company's responsibility in collecting people's personal information, both online and offline. In addition, every company is required to have an internal policy regarding the protection of personal data as a preventive measure against potential misuse in their operations. However, the facts on the ground show that a lot of users' digital data is traded without permission or used illegally, even stolen by third parties. This

misuse of personal data shows that there are weaknesses in the system, both in terms of public legal awareness, regulatory effectiveness, less strict supervision, and less effective law enforcement, which ultimately harms the individuals concerned.

Legal products as protectors of the public regarding data privacy are regulated in Law Number 27 of 2022 concerning the protection of Personal Data, then there is Law Number 24 of 2013 concerning Amendments to Law Number 23 of 2006 concerning Population Administration, there are also Laws Law Number 11 of 2008 concerning Electronic Transaction Information, and Regulation of the Minister of Communication and Information Technology Number 20 of 2015 concerning Protection of Personal Data in Electronic Systems.

Article 1 number 1 of Minister of Communication and Information Regulation Nmor. 20 of 2016 concerning the Protection of Personal Data states that Personal Data is certain individual data that is stored, maintained, and maintained as true and protected confidentially, then in Law Number 27 of 2022 concerning Protection of Personal Data states that data about natural persons who are identified or can be identified individually or in combination with other information either directly or indirectly through electronic or non-electronic systems. Furthermore, in Law Number 27 of 2022 concerning Personal Data Protection, Article 4 states that personal data consists of specific personal data and general personal data.

The Constitutional Court in Decision No. 5/PUU-VIII/2010 stated that the right to privacy is part of the concept of Human Rights, including the right to privacy of information. Furthermore, the right to personal communication is categorized as a derogable right because restrictions can be imposed on its implementation. On the other hand, after the amendment to the 1945 Constitution, the protection of personal data is recognized as a constitutional right. Rules governing personal data can be found in the Civil Code and Law Number 11 Year 2008 concerning Electronic Information and Transactions. Article 3 of Law Number 11 of 2008 concerning Information and Electronic Transactions stipulates that the principles applied in the use of information technology and electronic transactions are based on the principles of legal certainty, utility, prudence, good faith, and freedom to choose. The Constitutional Court in that decision affirmed that the right to privacy is a component of human rights, including the right to privacy of information. However, this right may be subject to limitations.

Furthermore, in Article 15 paragraph (1) of Law Number 11 of 2008 concerning Electronic Information and Transactions, it is stated that every electronic system organizer must operate the electronic system reliably and securely and be responsible for the operation of the electronic

system. If viewed in that article, then personal data within the scope of technology must be protected for the common interest. Law Number 11 of 2008 concerning Electronic Information and Transactions also regulates several other provisions related to prohibited actions in the field of information and electronic transactions, ranging from Article 27 to Article 37. In essence, these articles prohibit any unauthorized actions intentionally abusing various electronic information and potentially harming the data owner. Law Number 11 of 2008 concerning Electronic Information and Transactions also imposes criminal sanctions on perpetrators proven to violate the concept of personal data protection and cause harm to the data owner, with a maximum penalty of 12 years imprisonment and/or a maximum fine of Rp 12,000,000,000.00.

4 CONCLUSION

Digital transformation is a process driven by digital technology, which generates new business models and has the potential to disrupt markets and industries worldwide. This process creates disruptions within organizations and has significant impacts on value creation, strategies, and organizational structures. With digital transformation in business, several management practices undergo changes, which in turn can affect organizational sustainability. The formation of digital organizations is a result of this transformation, with artificial intelligence and computer capital becoming key assets that change the direction of growth.

Digital innovation provides numerous benefits for companies but also brings risks that need to be mitigated. To ensure that these risks do not adversely affect the company and its consumers, legal obligations must be fulfilled. Risks to privacy and security can have economic, ethical, or legal implications for consumers and companies. The responsibility to protect personal data must be borne by both the government and companies. Companies, as service providers, have the greatest responsibility in this regard. They need to conduct business ethically by safeguarding user data and providing transparent explanations to users about how their data will be used. Companies also need to consider human, technological, and environmental aspects before developing new technologies. Therefore, corporate awareness is required to fulfill their digital social responsibilities. The latest law governing personal data protection is Law Number 27 of 2022 concerning Personal Data Protection. Personal data protection is one of the main focuses of Corporate Digital Responsibility (CDR) or Corporate Digital Responsibility. The concept of CDR is an evolution of Corporate Social Responsibility tailored to the digital era. In CDR, companies are expected to adopt practices that consider

digital culture. It can be an effective strategy to integrate business and government interests in efforts to protect digital users.

REFERENCES

R. H. Sumitro, *Metodologi Penelitian Hukum dan Jurimetri*, 4th Print. Jakarta: Ghalia Indonesia, 1990.

P. Soerjowinoto, *Buku Pedoman Metode Penelitian Karya Hukum dan Skripsi*. Semarang: Fakultas Hukum Unika Soegijapranata, 2006.

Moch. M. Taufiqurrohman, Z. Priambudi, and A. N. Octavia, "MENGATUR PETISI DI DALAM PERATURAN PERUNDANG-UNDANGAN: UPAYA PENGUATAN POSISI MASYARAKAT TERHADAP NEGARA DALAM KERANGKA PERLINDUNGAN KEBEBASAN BERPENDAPAT," *Jurnal Legislasi Indonesia*, vol. 18, no. 1, p. 1, Mar. 2021, doi: 10.54629/jli.v18i1.750.

Moch. M. Taufiqurrohman, M. T. Fahri, R. K. Wijaya, and I. G. P. Wiranata, "MENINJAU PERANG SIBER: DAPATKAH KONVENSI-KONVENSI HUKUM HUMANITER INTERNASIONAL MENINJAU FENOMENA INI?," *Jurnal Kawruh Abiyasa*, vol. 1, no. 2, pp. 145–165, Jan. 2022, doi: 10.59301/jka.v1i2.21.

M. Suchacka, "Corporate Digital Responsibility - A New Dimension of the Human - Technology Relations," *System Safety: Human - Technical Facility - Environment*, vol. 2, no. 1, pp. 1–8, Mar. 2020, doi: 10.2478/czoto-2020-0001.

M. H. Hisbulloh, "Urgensi Rancangan Undang-Undang (RUU) Perlindungan Data Pribadi," *Jurnal Hukum*, vol. 37, no. 2, p. 119, Dec. 2021, doi: 10.26532/jh.v37i2.16272.

I. Guandalini, "Sustainability through digital transformation: A systematic literature review for research guidance," *J Bus Res*, vol. 148, pp. 456–471, Sep. 2022, doi: 10.1016/j.jbusres.2022.05.003.

H. B. Setiawan and F. U. Najicha, "Perlindungan Data Pribadi Warga Negara Indonesia Terkait Dengan Kebocoran Data," *Jurnal Kewarganegaraan*, vol. 6, no. 1, pp. 976–982, 2022, Accessed: Apr. 25, 2024. [Online]. Available: https://journal.upy.ac.id/index.php/pkn/article/view/2657

F. Kurniawan, Moch. M. Taufiqurrohman, and X. Nugraha, "Legal Protection of Trade Secrets over the Potential Disposal of Trade Secrets Under the Re-Engineering Precautions," *Jurnal Ilmiah Kebijakan Hukum*, vol. 16, no. 2, p. 267, Jul. 2022, doi: 10.30641/kebijakan.2022.V16.267-282.

A. K. Feroz, H. Zo, and A. Chiravuri, "Digital Transformation and Environmental Sustainability: A Review and Research Agenda," *Sustainability*, vol. 13, no. 3, p. 1530, Feb. 2021, doi: 10.3390/su13031530.