

Detection of Digital Law Issues and Implication for Good Governance Policy in Indonesia

Awaludin Marwan^{a,1,*}, Diana Odier-Contreras Garduño^{b,2} Fiammetta Bonfigli^{b,2}

^a Faculty of Law, Bhayangkara University, Jakarta, Indonesia.

^b Utrecht University, Netherlands Institute of Human Rights, Netherlands.

^c Faculty of Law, Universidade Federal do Espirito Santo, Brazil.

¹ awaludin.marwan@gmail.com *, ² d.i.odier-contrerasgarduno@uu.nl ² fiammettabonfigli@msn.com

* corresponding author

ARTICLE INFO

Article history

Received: July 9, 2021

Revised: June 29, 2022

Accepted: July 30, 2022

Keywords

Good Governance;

Cybercrime;

Digital Law;

E-Business;

ABSTRACT

The concept of good governance is essential to be utilized to analyze updating digital law and society. However, at the practical level, it can still be seen the lack of implementation of the principle of properness, transparency, effectiveness, accountability, participation, and human rights by the government to respond to the economic growth and criminal trend within the digital era. This study discusses good governance as a concept that can be used to analyze digital law and society. Especially in the cybercrime and e-businesses in Indonesia, the concept of good governance may utilize the social impact. This study uses socio-legal research, which combines interviews and literature review. This article will start to discuss the relevance of the study of good governance, digital law, and society in Indonesia's social and judicial context with the Electronic Information Transaction Law. This study concludes that during the growth of the digital economy, Indonesia has suffered from cyber-attacks, scams, phishing, malware injection, etc., which may need more extraordinary law enforcement. At the same time, the increasing number of e-commerce, fintech, social media, digital start-up, etc., need support from proper facilitation by the government. Good governance may provide a tool to cover the objective and balance its outcomes in the digital era.



This is an open access article under the [CC-BY 4.0](https://creativecommons.org/licenses/by/4.0/) license.



1. Introduction

Good governance is a meta-legal theory that can be applied to any legal problem. At present, I use this concept to delineate the development of digital law and society in Indonesia. Simply put, good governance is a legal concept that focuses on strengthening the norms for governments and the legal protection of citizens. This concept was developed from the doctrine of administrative law and encourages government structures for determining institutional objectives and supervising the performance of public servants based on professionalism and integrity ([Rukanova et al., 2015](#)).

Meanwhile, with digital trends using the internet in Indonesia, legal updates are needed to explain the development of digital trends in Indonesia. Indeed, more than 150 million Indonesians now have access to the internet ([Janowski & Janssen, 2015](#)). The digital market and penetration in Indonesia have increased over time. In this paper, many issues are discussed in the public sphere, such as cybercrime, financial technology, media online, e-commerce, social media, cryptocurrency,

etc. Furthermore, I will discuss some issues concerning digital law and society in Indonesia, such as the legal problems of cybercrime and e-business development in Indonesia. I analyze these legal issues from the good governance perspective (Ferrari, 2022).

At the level of international law, the concept of good governance is utilized by the various players in the field of international law. This concept is used by the United Nations Development Programme, the International Monetary Fund (IMF), the International Court of Justice (ICJ), the East African Court of Justice (EACJ), the European Court of Human Rights (ECtHR), the Inter-American Court of Human Rights (IACHR), and the World Trade Organization (WTO), the World Bank, and so on. Regarding cyber law, Henk's argumentation is beneficial in analyzing the social phenomena of digital law. Digital law seems to be something without frontiers and jurisdiction. Indeed, in the digital era, society is comprised of networks and interconnected (Castells) (Esposito, 2022).

The concept of good governance comes from an intellectual administrative law tradition. Henk Addink's thoughts are relatively similar to those of his colleagues from Utrecht University School of Law, such as Rob Widdershoven, Ben Schueler, Remco Nehmelman, Philip Langbroek, and Anoeska Buijze. However, I have seen some differences and debates at the Institute of Jurisprudence, Constitutional and Administrative Law, Utrecht University School of Law (Green, 2022). Meanwhile, I understand that Dutch and European administrative law traditions have also developed Addink's concept of good governance. He always admires the General Administrative Law Act (GALA). The Netherlands' General Administrative Law Act (GALA) (*Algemene wet resurrect of Awb*) is composed of rules for orders (*besluiten*) which are released by the administrative authorities and have encouraged legal protection. Furthermore, Addink's concept of good governance reinvented the right to good governance based on European law, especially Article 41 of the Charter of Fundamental Rights of the European Union. Article 41 may become an umbrella right to establish the right to good governance and administration (Reddick et al., 2015).

At the level of philosophy of law tradition, Addink develops the concept of good governance from natural law school. Hence, the theoretical reflections of good governance obtain its legal and philosophical background, especially when Addink mentions Dworkin and Hart. Addink is closer to Dworkin, who emphasizes moral values toward a legal regime like R. Alexy. At the same time, Hart is quite different from Austin and Kelsen, who are too positivistic (Whitacre & Rhinesmith, 2015). Hart is known for their 'soft-positivism' approach regarding social norms and customary law (Amalia, 2021). Furthermore, Dworkin concerns with the issue of political morality as collection decisions from individuals who adore democracy (Panagopoulos et al., 2022). Meanwhile, Hart also argues that the law is not only the procedural standard but also the structure of the idea of justice. Henk does not explicitly say something about political morality and the idea of justice, but he uses Hart's concept of law and Dworkin's interpretative legal concept (Wiedemann, 2022).

After discussing Hart and Dworkin, I will elaborate on the main points of Henk's concept of good governance. Henk's concept of good governance is a legal concept that developed from the concept of the rule of law and democracy. Simply put, good governance can be called the democratic rule of law (Böck et al., 2022). The concept of the rule of law is mainly defined as the separation of power into legislative, executive, and judiciary power, and is obliged to regard the mechanism of check and balances (Custers & Malgieri, 2022). By the same token, the concept of democracy is a political system whereby people participate in the governing of the state through representation. Hence, good governance plays between the rule of law and democracy to stipulate the legal principles, properness, transparency, accountability, participation, effectiveness, and human rights (Szwajdler, 2022).

Herewith, the booming digital era may be secured by the implementation of principles of good governance. For instance, how to enforce cybercrime laws based on the principles of properness, transparency, accountability, participation, effectiveness, and human rights. This may apply to other fields, such as e-commerce, financial technology, cryptocurrency, online media, etc.

2. Research Method

This study was created using socio-legal research. Combining social data and legal documents with some interviews is conducted here. A legal approach fosters the identification of legal problems between fact and norm (Koos, 2022). For instance, the legal problem of implementation concerning cybercrime is not only using the special regulations but also the criminal code in general. Furthermore, a literature review concerning the concept of good governance and digital law and society is a pivotal component of this research (Hage, M. Y., & Ningrum, P. K., 2022). Legal approach fosters to identify legal problem between fact and norm (Yudiana et al., 2022). For instance, the legal problem of implementation concerning cybercrime is not only using the special regulation but also the criminal code in general. Furthermore, literature review concerning the concept of good governance and digital law and society are pivotal component during this research (Zolotar et al., 2022).

3. Results and Discussion

Cybercrime regulation was initiated in 2008 with the name of the Electronic Information and Transaction Law (ICT Law). This law stipulates norms for protecting business transactions, whilst this law regulates various cybercrimes such as online defamation, pornography (Zolotar et al., 2022). The Institute for Digital Law and Society (Tordillas), a non-profit organization which is concerned with issues of cybercrime in Indonesia, studied court verdicts in regards to the implementation of cybercrime regulation. Tordillas has found that the most common forms of cybercrime are online defamation and hate speech/racism. From a good governance perspective, we can identify whether cybercrime regulation can be qualified as "a good regulation" or not. Good governance needs a well-thought-out system of rules that tells governments how to act in the best way (Yudiana et al., 2022).

Good governance not only covers good regulation but also provides crucial leverage in the promotion of social justice and development. Good governance may be used to encourage economic growth in the digital era. The Indonesian government, through the Financial Services Authority (OJK), has fostered the business growth of financial technology (Amalia, 2021). At least for the present, this authority has released some regulations to support financial technology trends, ranging from POJK No. 37/POJK.04/2018 concerning Fund Disbursement Services through Equity Crowdfunding, POJK No. 13/POJK.02/2018 concerning Digital Financial Innovation in the Financial Services Sector, and POJK No. 77/POJK.01/2016 concerning Online Peer to Peer Lending, etc. On April 8, 2019, the Financial Services Authority registered 106 financial technology companies. Peer-to-peer lending transactions totaled 33 trillion IDR, or \$2 billion USD (Panagopoulos et al., 2022).

In accordance with Google and Temasek's research, Indonesia will become the largest economy market in Southeast Asia. In 2018, Indonesia gained 27 trillion USD from the digital economy and will reach 100 trillion USD in 2025 (Temasek & Google, 2018). This potential digital economy must be supported by the militancy of the implementation of good governance. Indeed, the concept of good governance may become a new standard of development. Moreover, good governance can, on some occasions, be a key to economic success. In the spirit of good governance, economic policies and regulatory frameworks should follow the rule of law. This ensures fair competition, gets rid of corruption, which hurts the integrity of the market, and makes sure that the economy grows in a healthy way (Bednarz & Manwaring, 2022).

Besides the contribution to the economic side, good governance also improves the condition of democracy. With the development of information and communication technology, Indonesian society seems to celebrate freedom, liberty, and extrication. Freedom of the press is a symbol which encourages the growth of online media. However, some journalists have been prosecuted through cybercrime regulation. By analysing case law, journalists can be criminalised for criminal offences such as defamation (The Court of Bau's Decision No. 158/Pid.B/2017), extortion (The Court of Pekanbaru's Decision No. 345/Pid.Sus/2018/PN Rgt), hate speech (the Court of Medan's Decision No. 8/Pid.Sus/2019/PT.MDN), and so on. Freedom and democracy are actually at risk through the misinterpretation of cyber law usage (You, 2022).

At the same time, democracy and freedom, by nature, are increasing in Indonesia due to enhancing social media. As mentioned by Hootsuite, we are social in 2019, Indonesia's most active social media platforms, ranging from Youtube 88 %, WhatsApp 83.0%, Facebook 81.0%, Instagram 80.0%, etc. The majority of the 150 million social media users are between the ages of 13 and 34 (Chatfield et al., 2015). From a good governance perspective, democracy on social media can be delineated as the growing principle of participation. People participated in the election and expressed their views through new papers. However, due to the digital era, communication can be held through an online system (Meijer, 2015). People can react to any specific policy or government's action through social media, whether they support or criticize it. On social media, it is possible to create a better space for dialogue between people and the government. In fact, the idea of participation makes a public space where the government can hear what people want (Nottingham et al., 2022).

Last but not least, with the rise of the digital era, Indonesia has seen an increase in e-commerce or e-business over the last decade. Some e-commerce companies gained a valuation of more than 1 billion USD, such as Tokopedia, Traveloka, and Bukalapak. They became the "giants of unicorn" to back up digital economic growth. One e-commerce company has already attained the status of a "decacorn," with a valuation of more than ten billion dollars. The booming of the digital era stimulates the speed of digital economic development. Not only e-commerce and e-business, but also e-money and cryptocurrency, have been growing since the last decade in Indonesia. Before, cryptocurrency such as bitcoin was prohibited. The Commodity Futures Trading Supervisory Body has released Regulation No. 5 of 2019 with technical rules for the crypto asset market. From the point of view of development, Indonesia has a lot of e-businesses, which may become an important thing to think about in terms of good governance. With good governance, economic growth can be based on the rule of law, democracy, and legal principles that are followed, whether they are written down or not (Elisabet & Dewi, 2021).

Good governance is composed of theoretical views ranging from a factual or real dimension to a critical or ideal dimension. Some problems are faced in achieving the implementation of the good governance concept, such as the fragmentation of legal norms which harms legal certainty; the risk of uncontrolled execution of governmental power; the complexity of industrial society's demands; and corruption and maladministration. Good governance may analyze the prevention and enforcement of cybercrime. In Indonesia, the Indonesian criminal procedure act may include the regime of administrative law. With this in mind, the idea of preventing and punishing cybercrime can be looked at from the point of view of administrative law, or more generally, the point of view of good governance. An administrative law approach can be used to analyze the implementation of cybercrime regulation. Law No. 11 of 2008, hereafter revised by Law No. 19 of 2016, stipulates some criminal offences such as Article 27, which contains the prohibition of defamation, gambling, pornography, and extortion; Article 28 is composed of consumer protection and banning racism; and Article 29 until 35 are about the prohibition of illegal interception, system destruction, etc. With this in mind, administrative law can be used to figure out how much law enforcers follow Indonesian Criminal Procedure when working on a cybercrime case (Belanche-Gracia et al., 2015).

Besides, cybercrime is mentioned by cybercrime regulation. The Indonesian ecosystem of ICT has known various cybercrimes, such as carding, cracking, joy computing, hacking, Trojan horse or any other computer virus, data leakage, data diddling, frustrating data communication, and illegal content. Furthermore, the Ministry of Communication and Information Technology has issued circulated letter No. 5 of 2016 concerning the limitation of responsibility or liability of platforms and merchants on e-commerce through user-generated content. According to the circulated letter, e-commerce marketplaces are not permitted to sell chemical liquids, booms, guns, alcohol, drugs, or any other "negative content or prohibited goods and services." Other cybercrimes that frequently occur in Indonesia are computer-related forgery, fraud, or phishing. A local police officer in Jakarta might get about 40 to 50 reports of phishing from customers of online stores in a month (Schellekens, 2022).

According to the research conducted by the Institute for Digital Law and Society, the implementation of cybercrime regulation consists of some findings. For instance, online defamation is the largest case of cybercrime from 2008–2019. Online defamation in accordance with Article 27 (2) of Law No. 11 of 2008 comprises 35 % of the total case law of cybercrime. Furthermore, racism

through online platforms has occupied the second largest case, here. Racism in accordance with Article 28 (2) of the same law above, composed of 20 % of the total case law of cybercrime. Meanwhile, pornography, in accordance with 27 (1) of Law No. 11 of 2008, has stayed in the third position. Pornography through online platforms accounts for 15 % of the total case law of cybercrime (Quigley et al., 2015).

Those investigating these crimes need to pay more attention too, after looking at the material law of cybercrime. Digital forensics is one of the "sexy" issues of the digital era. Digital forensics investigates forensic images of hard disk drives, memory dumps, system and application logs, and network packet captures. Then these sources are processed through the examination of files, memory structures, log records, and networks. An analyst may make a report afterwards (Burton, 2015). There are two general models and one conceptual model. DF = I, S, D, E, A, R, which may define a digital forensic as the same as letter 'I' for identification process, letter 'S' for storage of digital evidence, letter 'D' for documentation of digital evidence, letter 'E' for exploration, letter 'A' for analysis data, and letter 'R' for reporting. At the same time, the conceptual model can be described by DF = [Pi] [Tj, Lk, DE], which says DF for Digital Forensic is composed of letters "Pi" for a series of digital forensic processes; letters "Tj" for techniques, methods, approaches, systems, and tools; letters "Lk" for legal principles; and letter "DE" for Digital Evidence. Cybercrime evidence is hard to check in Indonesia because the Indonesian Criminal Procedure does not list digital evidence as one of the main types of evidence that can be used in the criminal justice system (Tylec et al., 2022).

After discussing the digital evidence, the subject is often abandoned regarding the victim. In the digital era, some sexual harassment can be found on social media and in digital footprints. Indonesia does not provide a system of right to be forgotten, which may be useful to erase the digital footprint of someone who is harmed by cybercrime. By giving criminal punishment for offences, such as imprisonment or fines, it often feels that the victims do not seem to be for fair legal protection. By the same token, in the digital era, victims may forfeit material or financial losses. Moreover, the victim may suffer from moral or psychological damage, and so on and so forth. Hence, the Indonesian cybercrime regulation needs to provide restitution and compensation for the victims. Sexual harassment on digital platforms, in particular, is a difficult problem to solve. The victim often feels traumatized and gets scared with her problem (Rana & Dwivedi, 2015).

However, the increased cybercrime in Indonesia also strengthens the prevention approach. Some popular cybercrime cases arose, such as e-banking fraud in 2001, when Steven Haryanto made a similar website to BCA Bank; the case of the General Election Commission, which was hacked in 2004 by a pseudonymous Xnuxer who changed the names and pictures of political parties; and illegal interception, which targeted Indonesian President Susilo Bambang Yudhoyono (SBY) and other ministers in 2009. Of course, strengthening cyber security is a pivotal component and a crucial one. Government agencies have periodically pushed for audits of the security of telecommunications and have used outside certifications like ISO 27001: 2003 for IT security management systems (Ooi et al., 2022).

Apart from what was discussed above, the position of the government remains to believe in the concept of good governance, which is a vital component. Law enforcement of anti-cybercrime requires compliance with the principles of good governance. At least the principle of properness is demanded herein. A commitment to the principle of properness is required to achieve great anti-cybercrime law enforcement and to strengthen cyber security, a commitment to the principle of properness is required. Addink says that there are eight main groups of (un)written principles of good administration. These include the rule against abusing power, the principle of fairness, the principle of legal certainty, the principle of legitimate expectations, the principle of trust, the principle of equality, the principle of due care, and the motivation principle (Van Mil & Quintais, 2022).

With the implementation of the principle of properness, Indonesian police and the Ministry of ICT's special investigator may not conduct misuse of power. They obey the standard of legal certainty and can provide fair procedure for criminal investigation. The problem of law enforcement is a symptom that is composed of corruption, maladministration, and abuse of power. The professionalism of police and the ministry of ICT's special investigator can be evaluated with their

acts and policies based on the principle of properness (Sittel, 2015). Moreover, the police and the Ministry of ICT's special investigator, who are the main actors in combating cybercrime, should not only adhere to the principle of properness but also other principles of good governance, such as transparency, accountability, effectiveness, participation, and human rights. The government should use the principles of properness, transparency, accountability, effectiveness, participation, and human rights to make cybersecurity stronger (Stahl et al., 2022).

The Cyber Agency and Country Password (BSSN) have the authority to intervene and oversee cyber security among governmental institutions, businesses, the media, and civil society. However, BSSN should carry on the principles of properness, which are based on the law, in doing their duty. This institution also conducts the principle of transparency to provide public information concerning cyber security. They also have to announce a public meeting and invite people to discuss their decision-making process (Bertot et al., 2015). Without transparency, BSSN may seem to be less committed to good governance. The principle of transparency requires opening up public information, public documents, public hearings or meetings and stimulating people to engage with the regulation-making process. It is the obligation of the government to provide accurate information. The aims of the principle of transparency are to provide people with a better understanding of official information. Herewith, the police, the Ministry of ICT, and BSSN should implement the principle of transparency to combat cybercrime and strengthen cyber security throughout the internet area network of Indonesia. Furthermore, these governmental institutions also have to realize other principles of accountability, effectiveness, participation, and human rights (van Loon & Toshkov, 2015).

Good governance may have various functions in different fields, such as education, health care, financial services, development issues, economic markets, and the environment. The concept of good governance can also be used to analyze the digital economy trend in Indonesia. I do believe digital economic growth may be enhanced over time with the support of the implementation of good governance, the rule of law, and democracy. In particular, economic growth may be constrained within stability when the principles of good governance such as properness, transparency, accountability, participation, effectiveness, and human rights can be realized (Basukie et al., 2020). Addink says that, in general, good governance can help with economic analysis, especially when it comes to how goods and services are made, distributed, and used. Furthermore, good governance can be used to analyze political economy, which includes microeconomics and macroeconomics. The idea of good governance can be used to look at how basic parts of the economy behave, such as the role of households, firms, and markets, and how they interact within specific economic clusters. It can also be used to look at unemployment, inflation, and economic growth, as well as monetary and fiscal policy (Koussouris et al., 2015).

Herewith, I will discuss the development of e-commerce or e-business in Indonesia from a good governance perspective, which may be useful to have a better understanding of the current situation of the digital economy in Indonesia, its problems, and solutions. As we know above, Indonesia's digital economy is the largest in the region of Southeast Asia. In 2018, the total Gross Merchandise Value (GMV) of Southeast Asia's internet economy reached \$72 billion across online travel, e-commerce, online media, and ride hailing. Google and Temasek predict it will reach \$ 240 billion in 2025. And, Indonesia is called in this Google and Temasek research as a "digital archipelago" with the largest and fastest growing internet economy in the region (Yudiana et al., 2022).

Indonesia, with its GDP of over \$ 1 trillion, 67.6% productive age, and more than 54.4% of the population online, has become the biggest digital market within the region. A lot of popular apps and games are famous and consumed in Indonesia. Online apps like WhatsApp, Facebook, Instagram, ShareIt, Line, Facebook Messenger, Gojek, and games like Mobile Legends, PUBG Mobile, Clash of Clans, Helix Jump, Ludo King, and others have a million users in Indonesia. The digital market in Indonesia is huge. The government requires the concept of good governance to be implemented to determine and supervise the development of the digital economy (Yudiana et al., 2022).

Unfortunately, in the field of e-commerce, the government seems to have a lack of good governance due to "almost zero" regulation concerning this subject. The government also seems to not provide a supply of taxation. In other words, there is no record in regards to taxation and total

transactions related to e-commerce and digital platforms (Sabani et al., 2019). Moreover, the Indonesian government does not have any data on total transactions regarding e-commerce. The lack of data about e-commerce and digital platforms makes the government nervous about producing its policy. Without sufficient data, the government cannot make great public policy. The Indonesian Central Bureau of Statistics also does not have data on e-commerce and digital platform penetration. People know Gojek becomes a unicorn, and some e-commerce sites such as Tokopedia, Bukalapak, and Traveloka turn into unicorns. Furthermore, consumer protection in the e-commerce ecosystem is fraught with peril (Zolotar et al., 2022).

The lack of regulation in the field of e-commerce may encourage economic risk. From a good governance perspective, this may not suit the principle of properness, especially the principle of legal certainty. Addink argues that the principle of legal certainty obliges all activities and exercises to be based on existing law. More information about the spirit of legal certainty can be seen at Article 4: 23 and Article 5:22 of the General Administrative Law Act (GALA). This principle can also be seen in Article 10a of the Indonesian Government Administration Act No. 30 of 2014. The principle of legal certainty is an essential one. Douzinis says that the way textual language is put together is a key part of creating legal order. Hence, the written law is an important thing to guarantee the principle of legal certainty (Suryono et al., 2021).

Regulation concerning e-commerce is not adequate to secure this trend and the legal protection of citizens (customers). Rules concerning e-commerce are mentioned in Articles 65 and 66 of Law No. 7 of 2014 concerning trade. Moreover, this regulation creates a government regulation, which is until now still in debate. The bill of government regulation concerning e-commerce is still delayed by the Coordinating Ministry for Economic Affairs. Actually, this bill might have been issued last August due to controversial debate regarding the legal substance. The only regulation concerning e-commerce is the President's Regulation No. 74 of 2017 concerning road map e-commerce for 2017–2019 (González-Gallego & Pérez-Cárceles, 2021). However, this regulation is too broad to cover the problem of e-commerce. Once a 'substantial and technical' regulation was issued by the Ministry of Finance concerning e-commerce taxation No. 2010 of 2018. The Indonesian Association of E-commerce (Idea) protested against this regulation. This regulation was quickly withdrawn by the Ministry of Finance. In this case, the Indonesian government does not seem to follow the principle of accountability and effectiveness. The lack of regulation and the government's limited role in supervising e-commerce demonstrate that the government cannot create social and political accountability, and their actions are less effective. The Indonesian government is less open because there isn't enough public information about e-commerce for them to make rules and policies about it before they do (Suryono et al., 2021).

Besides the issues of e-commerce, the digital economy from a good governance perspective in Indonesia has glimpsed a bit of a problem, especially from the principle of participation and protection of human rights in the field of financial technology. Addink argues that the principle of participation is needed to enhance the capacity of people and how the administrative authority responds to it. The channel of participation within financial technology is limited (Bakker & Ritts, 2018). The Financial Services Authority does not have any adequate mechanism to receive a complaint and how to respond to it. Of course, people can submit a complaint, especially regarding financial technology services through an online platform. Unfortunately, people do not have any information on what exactly the numbers of reports are and how these complaints are taken care of by the Financial Services Authority. Furthermore, in March 2019, the Financial Services Authority blocked 803 financial technology companies. From the principle of participation, this policy of the Financial Services Authority may be analyzed to what extent the public or stakeholders or financial technology companies have been invited to dialogue. Participation before a decision has been taken is really essential (Valdivia & Balcell, 2022).

However, the Financial Services Authority may try to establish legal protection for citizens. Many complaints about 'illegal' financial technology companies. Thousands of complaints were received by the Financial Services Authority, the Association for Financial Technology Companies, and Legal Aid Institutions (Thomas et al., 2018). Even though the complaints are large, people or customers have suffered damage such as extortion, super-high interest loans, and infringement of privacy rights. The principle of human rights must be recognized in the field of customer protection, especially in the sector of financial technology services. Hence, the Financial Services Authority and

the Ministry of ICT, as well as the Cyber Directory of National Police, must be aware of the prioritizing of legal protection of citizens. To get social justice in a country, good governance puts the legal protection of citizens at the top of the list (Lestantri et al., 2021).

4. Conclusion

The concept of good governance is essential to be analyze the updating of digital law and society. As I mentioned above, Henk's concept of good governance is useful to oversee the regulation, policy, and action by the government with regard to the development of digital law and society. On some occasions, it can still be seen the lack of implementation of the principles of properness, transparency, effectiveness, accountability, participation, and human rights by the government to respond to the economic growth and criminal trend within the digital era. But there are still many ways to change the digital law and society system in Indonesia for the better. At the practical level, in the digital era, good governance can be used as a concept or approach to handle cybercrime and e-business. Good governance emphasized proper procedure in accordance with the principles of legal certainty, carefulness, reasonability, and so on. These principles of good governance may foster the handling of cybercrime based on the democratic rule of law. Hence, the law enforcement of cybercrime can be challenged by avoiding arbitrariness, misuses of power, mismanagement, or maladministration. Furthermore, as it can be used to strengthen the law enforcement of cybercrime, good governance may be utilized to boost the digital economy with adequate regulation and supervision over e-commerce, fintech, and other e-businesses. With good governance, the role of government agencies can be seen by the whole society and provide more customer protection as well as give legal certainty for direct or indirect investment in the technological area.

References

- Amalia, P. (2021). Multinational Corporation 's Investments made through its Subsidiary under The Latest Generation of Investment Treaties Latest Generation Of Investment Treaties. *Indonesian Journal of International Law*, 19(1). <https://doi.org/10.17304/ijil.vol19.1.5>
- Bakker, K., & Ritts, M. (2018). Smart Earth: A meta-review and implications for environmental governance. *Global Environmental Change*, 52(March), 201–211. <https://doi.org/10.1016/j.gloenvcha.2018.07.011>
- Basukie, J., Wang, Y., & Li, S. (2020). Big data governance and algorithmic management in sharing economy platforms: A case of ridesharing in emerging markets. *Technological Forecasting and Social Change*, 161(September), 120310. <https://doi.org/10.1016/j.techfore.2020.120310>
- Bednarz, Z., & Manwaring, K. (2022). Hidden depths: The effects of extrinsic data collection on consumer insurance contracts. *Computer Law and Security Review*, 45(1), 105667. <https://doi.org/10.1016/j.clsr.2022.105667>
- Belanche-Gracia, D., Casaló-Ariño, L. V., & Pérez-Rueda, A. (2015). Determinants of multi-service smartcard success for smart cities development: A study based on citizens' privacy and security perceptions. *Government Information Quarterly*, 32(2), 154–163. <https://doi.org/10.1016/j.giq.2014.12.004>
- Bertot, J. C., Seifert, J., & Jaeger, P. (2015). Securing the homeland in the digital age: Issues and implications for policy and governance. *Government Information Quarterly*, 32(2), 105–107. <https://doi.org/10.1016/j.giq.2015.04.001>
- Böck, L., Fejrskov, M., Demetzou, K., Karuppayah, S., Mühlhäuser, M., & Vasilomanolakis, E. (2022). Processing of botnet tracking data under the GDPR. *Computer Law and Security Review*, 45, 105652. <https://doi.org/10.1016/j.clsr.2021.105652>
- Burton, D. L. (2015). Digital Dilemmas: Power, Resistance and the Internet. *Government Information Quarterly*, 32(2), 218–219. <https://doi.org/10.1016/j.giq.2015.02.003>

- Chatfield, A. T., Reddick, C. G., & Brajawidagda, U. (2015). Government surveillance disclosures, bilateral trust and Indonesia-Australia cross-border security cooperation: Social network analysis of Twitter data. *Government Information Quarterly*, 32(2), 118–128. <https://doi.org/10.1016/j.giq.2015.01.002>
- Custers, B., & Malgieri, G. (2022). Priceless data: why the EU fundamental right to data protection is at odds with trade in personal data. *Computer Law and Security Review*, 45, 105683. <https://doi.org/10.1016/j.clsr.2022.105683>
- Elisabet, M., & Dewi, Y. K. (2021). Digital Services Tax Regulation and Wto Non-Discrimination Principle: Is the Deck Stacked? *Indonesian Journal of International Law*, 19(1). <https://doi.org/10.17304/ijil.vol19.1.2>
- Esposito, F. (2022). The GDPR enshrines the right to the impersonal price. *Computer Law and Security Review*, 45, 105660. <https://doi.org/10.1016/j.clsr.2022.105660>
- Ferrari, M. V. (2022). The platformisation of digital payments: The fabrication of consumer interest in the EU FinTech agenda. *Computer Law and Security Review*, 45, 105687. <https://doi.org/10.1016/j.clsr.2022.105687>
- González-Gallego, N., & Pérez-Cárceles, M. C. (2021). Cryptocurrencies and illicit practices: The role of governance. *Economic Analysis and Policy*, 72, 203–212. <https://doi.org/10.1016/j.eap.2021.08.003>
- Green, B. (2022). The flaws of policies requiring human oversight of government algorithms. *Computer Law and Security Review*, 45, 105681. <https://doi.org/10.1016/j.clsr.2022.105681>
- Hage, M. Y., & Ningrum, P. K. (2022). Corrective Justice and Its Significance on the Private Law. *JILS (Journal of Indonesian Legal Studies)*, 7(1), 1-30. <https://doi.org/10.15294/jils.v7i1.46691>
- Janowski, T., & Janssen, M. (2015). Tribute to John Bertot and message from the incoming. *Government Information Quarterly*, 32(2), 103–104. <https://doi.org/10.1016/j.giq.2015.03.004>
- Koos, S. (2022). Digital Globalization and Law. *Lex Scientia Law Review*, 6(1), 33–68. <https://doi.org/10.15294/lesrev.v6i1.55092>
- Koussouris, S., Lampathaki, F., Kokkinakos, P., Askounis, D., & Misuraca, G. (2015). Accelerating Policy Making 2.0: Innovation directions and research perspectives as distilled from four standout cases. *Government Information Quarterly*, 32(2), 142–153. <https://doi.org/10.1016/j.giq.2015.03.001>
- Lestantri, I. D., Janom, N. B., Aris, R. S., & Husni, Y. (2021). The perceptions towards the digital sharing economy among SMEs: Preliminary findings. *Procedia Computer Science*, 197(2021), 82–91. <https://doi.org/10.1016/j.procs.2021.12.121>
- Meijer, A. (2015). E-governance innovation: Barriers and strategies. *Government Information Quarterly*, 32(2), 198–206. <https://doi.org/10.1016/j.giq.2015.01.001>
- Nottingham, E., Stockman, C., & Burke, M. (2022). Education in a datafied world: Balancing children’s rights and school’s responsibilities in the age of Covid 19. *Computer Law and Security Review*, 45, 105664. <https://doi.org/10.1016/j.clsr.2022.105664>
- Ooi, V., Kian Peng, S., & Soh, J. (2022). Blockchain land transfers: Technology, promises, and perils. *Computer Law and Security Review*, 45, 105672. <https://doi.org/10.1016/j.clsr.2022.105672>
- Panagopoulos, A., Minssen, T., Sideri, K., Yu, H., & Compagnucci, M. C. (2022). Incentivizing the sharing of healthcare data in the AI Era. *Computer Law and Security Review*, 45, 105670. <https://doi.org/10.1016/j.clsr.2022.105670>
- Quigley, K., Burns, C., & Stallard, K. (2015). “Cyber Gurus”: A rhetorical analysis of the language of cybersecurity specialists and the implications for security policy and critical infrastructure protection. *Government Information Quarterly*, 32(2), 108–117.

- <https://doi.org/10.1016/j.giq.2015.02.001>
- Rana, N. P., & Dwivedi, Y. K. (2015). Citizen's adoption of an e-government system: Validating extended social cognitive theory (SCT). *Government Information Quarterly*, 32(2), 172–181. <https://doi.org/10.1016/j.giq.2015.02.002>
- Reddick, C. G., Chatfield, A. T., & Jaramillo, P. A. (2015). Public opinion on National Security Agency surveillance programs: A multi-method approach. *Government Information Quarterly*, 32(2), 129–141. <https://doi.org/10.1016/j.giq.2015.01.003>
- Rukanova, B., Wigand, R. T., van Stijn, E., & Tan, Y. H. (2015). Understanding transnational information systems with supranational governance: A multi-level conflict management perspective. *Government Information Quarterly*, 32(2), 182–197. <https://doi.org/10.1016/j.giq.2014.12.003>
- Sabani, A., Farah, M. H., & Sari Dewi, D. R. (2019). Indonesia in the spotlight: Combating corruption through ICT enabled governance. *Procedia Computer Science*, 161, 324–332. <https://doi.org/10.1016/j.procs.2019.11.130>
- Schellekens, M. (2022). Data from connected cars for the public cause. *Computer Law and Security Review*, 45(December 2020), 105671. <https://doi.org/10.1016/j.clsr.2022.105671>
- Sittel, R. (2015). Public Libraries, Public Policies, and Political Processes: Serving and Transforming Communities in Times of Economic and Political Constraint. *Government Information Quarterly*, 32(2), 219–220. <https://doi.org/10.1016/j.giq.2015.02.005>
- Stahl, B. C., Rodrigues, R., Santiago, N., & Macnish, K. (2022). A European Agency for Artificial Intelligence: Protecting fundamental rights and ethical values. *Computer Law and Security Review*, 45, 105661. <https://doi.org/10.1016/j.clsr.2022.105661>
- Suryono, R. R., Budi, I., & Purwandari, B. (2021). Detection of fintech P2P lending issues in Indonesia. *Heliyon*, 7(4), e06782. <https://doi.org/10.1016/j.heliyon.2021.e06782>
- Szwajdler, P. (2022). Limitations of the Freedom of Hyperlinking in the Fields of Copyright Law, Trademark Law and Unfair Competition Law: Is Case-by-case Approach Sufficient? *Computer Law and Security Review*, 45(April 2016), 1–16. <https://doi.org/10.1016/j.clsr.2022.105692>
- Thomas, S., Richter, M., Lestari, W., Prabawaningtyas, S., Anggoro, Y., & Kuntoadji, I. (2018). Transdisciplinary research methods in community energy development and governance in Indonesia: Insights for sustainability science. *Energy Research and Social Science*, 45(June), 184–194. <https://doi.org/10.1016/j.erss.2018.06.021>
- Tylec, G., Maćkowska, K., & Kwiecień, S. (2022). Copyright trolling as threat to internet users' legal and economic security: Comments in light of EU and US legislations. *Computer Law and Security Review*, 45. <https://doi.org/10.1016/j.clsr.2022.105688>
- Valdivia, A. D., & Balcell, M. P. (2022). Connecting the grids: A review of blockchain governance in distributed energy transitions. *Energy Research and Social Science*, 84(October 2021), 102383. <https://doi.org/10.1016/j.erss.2021.102383>
- Van Loon, A., & Toshkov, D. (2015). Adopting open source software in public administration: The importance of boundary spanners and political commitment. *Government Information Quarterly*, 32(2), 207–215. <https://doi.org/10.1016/j.giq.2015.01.004>
- Van Mil, J., & Quintais, J. P. (2022). A Matter of (Joint) control? Virtual assistants and the general data protection regulation. *Computer Law & Security Review*, 45(February), 105689. <https://doi.org/10.1016/j.clsr.2022.105689>
- Whitacre, B., & Rhinesmith, C. (2015). Public libraries and residential broadband adoption: Do more computers lead to higher rates? *Government Information Quarterly*, 32(2), 164–171. <https://doi.org/10.1016/j.giq.2015.02.007>

-
- Wiedemann, K. (2022). Profiling and (automated) decision-making under the GDPR: A two-step approach. *Computer Law and Security Review*, 45, 105662. <https://doi.org/10.1016/j.clsr.2022.105662>
- You, C. (2022). Half a loaf is better than none: The new data protection regime for China's platform economy. *Computer Law and Security Review*, 45, 105668. <https://doi.org/10.1016/j.clsr.2022.105668>
- Yudiana, T. C., Rosadi, S. D., & Priowirjanto, E. S. (2022). The Urgency of Doxing on Social Media Regulation and the Implementation of Right to Be Forgotten on Related Content for the Optimization of Data Privacy Protection in Indonesia. *Padjadjaran Jurnal Ilmu Hukum*, 9(1), 24–45. <https://doi.org/10.22304/pjih.v9n1.a2>
- Zolotar, O. O., Zaitsev, M. M., Topolnitskyi, V. V., Bieliakov, K. I., & Koropatnik, I. M. (2022). Prospects and Current Status of Defence Information Security in Ukraine. *Hasanuddin Law Review*, 8(1), 18–29. <https://doi.org/10.20956/halrev.v8i1.3582>