E-ISSN : 2723-2476
ISSN : 2723-1968
ACLJ, Vol.4, Issue 2, 2023

GUARANTEE OF INFORMATION AND COMMUNICATION TECHNOLOGY APPLICATION SECURITY IN INDONESIA: REGULATIONS AND CHALLENGES?

Nurfaika Ishak[1*]
[1*] Faculty of Syariah and Law, UIN Alauddin Makassar, Indonesia, nurfaika.ishak@gmail.com (*corresponding*).

Abstract: In this era of rapid development of science, knowledge, and technology, society is faced with a challenge related to the use of information and communication technology that can be misused by irresponsible parties and can cause harm and loss to others in the form of threats to security stability in cyberspace. This study aims to find out how to guarantee the security protection of information and communication technology applications for Indonesian citizens from the laws and regulations perspective, then how challenges and opportunities can be addressed to overcome the gaps that occur. This research is normative research with a statutory approach. The data collection technique used in this study is a literature study technique collected by reviewing scientific works, journals, laws and regulations, and other related materials related to information and communication technology, and crimes in cyberspace. The results show that the Indonesian government has issued a law on information and electronic transactions. Furthermore, several work teams were also formed under state agencies/institutions that focused on responding to information security issues such as teams under the auspices of the Ministry of Communication and Information; there were also other teams from Indonesian National Police Agency. The challenges faced are related to law enforcement on the regulations that have been set, namely how the substance of the contents in these regulations can accommodate the protection/guarantee of the security of personal information in Indonesia. In addition, this is also influenced by the apparatus's actions and the community's response.

Keywords: Security; Information and Communication; Technology; Cyberspace.

I. INTRODUCTION

Freedom to express thoughts and freedom of opinion, as well as the right to obtain information through the use and utilization of information and communication technology, is aimed at advancing public welfare, and educating the nation's life as well as providing a sense of security, justice, and legal certainty for users and administrators of electronic systems. In the life of society, nation and state, rights and freedoms through the use and utilization of information technology are carried out by taking into account the limitations stipulated by law with the sole purpose of guaranteeing recognition and respect for the rights and freedoms of others and to fulfill the demands imposed by the law. justice by considerations of morality, religious values, security, and public order in a democratic society (Junaidi et al., 2020; Syahriar, 2021).

Information technology plays a vital role in trade and national economic growth to realirealisele's welfare; the government needs to support the development of information technology through legal infrastructure and its ration so that the use of information technology is carried out safely to prevent its misuse by taking into account the religious and socio-cultural values of the Indonesian people. In 2013 Indonesia became a victim of wiretapping by Australian intelligence services based on leaked documents from a former member of the United States National Security Agency (NSA), Edward Snowden. The document contains a number severalfor tapping telephone conversations by Australia, one of which is President Susilo Bambang Yudhoyono and nine people closest to the president's circle (Setyawan, 2016). Cyberspace is also one of the sources of various threats to a country's sovereignty. The threat can come from anyone. Cyberspace can be a thrthreatenry because it can be used to steal information, propaganda, provocation, and attacks on information in various fields such as banking data, military networks and the national defense (Setiyawan et al., 2020).

Cybercrime is a crime that uses information technology and is one form of transnational crime does not recognise borderless, without violence (non-violence), there is no physical contact (no physical contact), and without name (anonomity) (Umbara & Setiawan, 2022). These characteristics of cybercrime make it challenging to track cybercrime actors and prove criminal elements, which exceeds the limitations of existing regulation (M. R. Wijaya & Arifin, 2020). The implementation of law enforcement in cyber crime currently in Indonesia has several weaknesses, namely weakness in legal regulations that have not thoroughly governed the types of cybercrime, weaknesses in enforcement, namely the lack of human resources investigators who understand cybercrime, and the lack of facilities and prelaw enforcement facilities in cybercrime (Bawono, 2019). Cybercrime prevention enencountersany difficulties, one of them in the legal arrangement because the form of cybcybercrimeways experiences the development along with the progress of information technology (Akub, 2018). Cyber crime knows no boundaries (borderless) and the time of the incident because victims and perpetrators are often in different countries. All these actions can be carried out only in front of a computer that has Internet access without fear of being known by other people/eyewitnesses, so this crime is included in Transnational Crime/crimes between countries whose disclosures often involve law enforcement from more than one country (Hartono & Hapsari, 2019).

The increasing use of technology (such as the internet) creates new challenges in protecting personal property, especially personal data, and increasing the practice of collecting, utilizing, and disseminating one's personal data (Prastini, 2018). Based on the results of national internet anomaly traffic monitoring from January to December 2018, there were 232,447,974 Cyberattacks on the Indonesian network (Aulianisa & Indirwan, 2020). The current condition of the implementation of Cybersecurity and resilience in Indonesia is still scattered among various institutions or stakeholders, each of which has governance guidelines. Various existing laws and regulations, in fact, cannot reach the problems in cyberspace (Aulianisa & Indirwan, 2020).

A new legal regime has been born, known as cyber law or telematics law. Cyberlaw or cyber law, is internationally used for legal terms related to information and communication technology (Ersya, 2017). Likewise, telematics law is a manifemanifestsgence of telecommunications law, media law, and informatics law. Other terms that are also used are information technology (law of information technology), the law of cyberspace (virtual world law), and the law of cyberspace.

E-ISSN : 2723-2476
ISSN : 2723-1968
ACLJ, Vol.4, Issue 2, 2023

These terms were born considering the activities carried out through a network of computer systems and communication systems both locally and globally (internet) by utilizing computer system-based utilizing technology which is an electronic system. Legal problems often relate to the delivery of information, communication, and/or transactandlectronically, especially in evidence and matters related to legal actions carried out through the electronic system.

Where the public is even entangled in the existence of illegal financial technology and there is a misuse of their personal data. It is true that there is an agreement that allows the debtor to access the personal data of the creditor, but whether with it immediately the debtor can misuse the customer's personal data (H. Wijaya & Herwastoeti, 2022). In 2019, the National Cyber and Crypto Agency (BSSN) reported 290 million cases of cyber attacks. This amount is 25% more than the previous year when cybercrimes caused Indonesia's US$ 34.2 billion in losses. The Covid-19 pandemic, apart from triggering a significant increase in phishing attacks, spam and ransomware malware attacks, has also increased the pressure to establish a well-functioning cybersecurity infrastructure (Anjani, 2021).

In the case of cyber threats, based on data analysis, The ID-SIRTII traffic monitoring system (Indonesia Security Incident Response Team on Internet Infrastructure) noted that the incidence of attacks in cyberspace in Indonesia reached one million incidents and will tend to increase every day due to an unknown system and application weaknesses (Chotimah, 2019). The laws and regulations in the field of information technology in force in Indonesia currently do not accommodate all cyber crimes, so several cyber crimes cannot be overcome, such as data theft through information technology which then demands a ransom of some funds. Retrieval of this data can threaten the guarantee of personal data protection which can be misused.

In an era of rapid development of science, knowledge, and technology, society is faced with a challenge related to the use of information and communication technology that can be misused by irresponsible parties and can cause harm and loss to others in the form of threats to security stability in the online world. The purpose of this study is to find out how to guarantee the security protection of the use of information and communication technology for Indonesian citizens from a review of laws and regulations and how challenges and opportunities can be addressed to overcome the gaps.

II. RESEARCH METHOD

This research is normative research that uses a statutory approach (Irwansyah, 2020). An approach that prioritizes legal materials in the form of legislation as an essential reference in conducting research. Analysis of the data used is a qualitative analysis based on material and data related to the topic of discussion (Al-Fatih, 2023). The data collection technique is the collection of primary data/ primary legal sources through direct research in the form of data collection on laws and regulations, and secondary data collection used is library research related to the problem being studied, which consists of literature. Some literature such as books, journals, reports and websites related to the topic of discussion/ information technology, communication, and cybercrime. These methods and approaches are used because they are in accordance with the research studies conducted.

III. RESULTS AND DISCUSSION

1. Regulations in Protecting the Use of Information and Communication Technology

Information globalization has placed Indonesia as part of the world's information society, thus requiring the establishment of regulations regarding the management of information and electronic transactions at the national level so that information technology development can be carried out optimally, evenly, and spread to all levels of society to educate the nation's life; the use and utilization of information technology must continue to be developed in order to maintain, and strengthen national unity and integrity based on laws and regulations for the national interest.

In the Industrial Era 4.0, all electronic work systems can support the concept of remote working (Putra et al., 2023). The government facilitates the use of information technology and electronic transactions by protecting the public interest from all kinds of disturbances as a result of the misuse of electronic information and electronic transactions that disrupt public order, as well as preventing the dissemination and use of electronic information and/or electronic documents containing prohibited contents. The government has the authority to terminate access and/or instruct the electronic system operator to terminate access to electronic information and/or electronic documents that have contents that violate the law.

Utilization of information technology, media, and communication has changed both the behaviour of society and human civilization globally (Raharja, 2019). Information and communication technology development has also caused world relations to become borderless and caused significant social, economic, and cultural changes to occur so quickly. Information technology is currently a double-edged sword because in addition to contributing to improving human welfare, progress, and civilization, it is also an effective means of violating the law.

In this regard, the legal world has long since expanded the interpretation of its principles and norms when dealing with intangible material issues, for example, in the case of electricity theft as a criminal act. In reality, cyber activities are no longer straightforward because they are no longer limited by the territory of a country, which can be easily accessed anytime and from anywhere. Losses can occur both to the perpetrator of the transaction and to other people who have never made a transaction, for example, the theft of credit card funds through shopping on the Internet. In addition, evidence is a significant factor, considering that electronic information is not only not comprehensively accommodated in the Indonesian procedural law system, but is also very vulnerable to change, intercept, falsification, and sending to various parts of the world as a matter of seconds. Thus, the resulting impact can be so complex and complicated (Widiastuti, 2009).

The legal basis for regulating cyber security in Indonesia is the Electronic Information and Transactions (ITE) Law Number 11 of 2008 and the revised version of the ITE Law Number 19 of 2016. This law includes rules for several violations, such as distributing illegal content, data protection violations, unauthorised access permission to computer systems to obtain information, and an illegal and unauthorised expropriation or interception of other computer or electronic systems. The ITE Law provides legal protection for electronic system content and electronic transactions. However, this law does not cover important aspects of cybersecurity, such as information and network infrastructure, and human resources with expertise in cyber security.

Several work teams were formed under state agencies/institutions that focused on responding to information security issues such as teams under the auspices of the Ministry of Communications and Information Technology, there were also other teams within the Indonesian National Police

E-ISSN : 2723-2476
ISSN : 2723-1968
ACLJ, Vol.4, Issue 2, 2023

working environment. Law enforcement is an important thing in the life of society and the state. POLRI as law enforcer who have the function, duty, and authority to realize security and public order, so strict action is needed in law enforcement against cybercrimes.

In addition to investigators of state police officers of the Republic of Indonesia, certain civil servants within the government whose scope of duties and responsibilities are in the field of information technology and electronic transactions are given special authority as investigators as referred to in the Law on Criminal Procedures to carry out investigations of criminal acts in Indonesia. information technology and electronic transactions. Investigations in the field of information technology and electronic transactions are carried out with due observance of the protection of privacy, confidentiality, the smooth running of public services, and the integrity or integrity of data by the provisions of laws and regulations. The criminal procedure law shall carry out search and/or confiscation of electronic systems related to alleged criminal acts in the field of information technology and electronic transactions. In conducting searches and/or confiscations as referred to in paragraph (3), investigators are obliged to maintain the maintenance of the interests of public services.

Civil Servant Investigators are authorized to:

a. Receive a report or complaint from someone about a criminal act in the field. Information technology and electronic transactions;
b. Summon any person or other party to be heard and examined as a suspect or witness in connection with an alleged criminal activity in the field of information technology and electronic transactions;
c. Examine the correctness of reports or information relating to criminal acts in the field of information technology and electronic transactions;
d. Conduct examinations of persons and/or business entities that are reasonably suspected of committing criminal acts in the field of information technology and electronic transactions;
e. Examine tools and/or facilities related to information technology activities suspected of being used to commit criminal acts in the field of information technology and electronic transactions;
f. Conduct searches of certain places suspected of being used as places to commit criminal acts in the field of information technology and electronic transactions;
g. Carry out sealing and confiscation of tools and/or facilities for information technology activities that are suspected to be used in a manner that deviates from the provisions of laws and regulations;
h. Make a data and/or electronic system related to criminal acts in the field of information technology and electronic transactions so that they cannot be accessed;
i. Request information contained in the electronic system or information produced by the electronic system to the electronic system operator related to criminal acts in the field of information technology and electronic transactions;
j. Request expert assistance required in the investigation of criminal acts in the field of information technology and electronic transactions; and/or
k. Stop the investigation of criminal acts in the field of information technology and electronic transactions by the provisions of the criminal procedure law.

The threat of punishment for any person who knowingly and without rights distributes and/or transmits and/or makes electronic information and/or electronic documents accessible which contain:

a. Violating decency, shall be punished with imprisonment for a maximum of 6 (six) years and/or a fine of a maximum of Rp1,000,000,000.00 (one billion rupiahs).
b. Gambling, shall be sentenced to a maximum imprisonment of 6 (six) years and/or a maximum fine of Rp1,000,000,000.00 (one billion rupiahs).
c. Insult and/or defamation, shall be sentenced to a maximum imprisonment of 4 (four) years and/or a maximum fine of Rp750,000,000.00 (seven hundred and fifty million rupiah).
d. Extortion and/or threats, shall be punished with imprisonment for a maximum of 6 (six) years and/or a fine of a maximum of Rp1,000,000,000.00 (one billion rupiahs).

In addition, any person who intentionally and without rights spreads false and misleading news that results in consumer losses in electronic transactions, as well as disseminates information intended to cause hatred or hostility to certain individuals and/or community groups based on ethnicity, religion, race, and between groups (SARA) shall be sentenced to a maximum imprisonment of 6 (six) years and/or a maximum fine of Rp. 1,000. 000,000.00 (one billion rupiahs). Any person who intentionally and without rights sends electronic information and/or electronic documents containing threats of violence or intimidation aimed at personally, shall be punished with imprisonment for a maximum of 4 (four) years and/or a fine of a maximum of Rp. 750,000,000. 00 (seven hundred and fifty million rupiah).

Utilization of information technology and electronic transactions are carried out based on:

a. The principle of legal certainty, the legal basis for the use of Information Technology and Electronic Transactions, and everything that supports its implementation, which has received legal recognition inside and outside the court.
b. Benefits, principles for using Information Technology and Electronic Transactions are sought to support the information process and improve the community's welfare.
c. Prudence, the principle for the use of Information Technology and Electronic Transactions is strived to support the information process to improve the welfare of the community.
d. In good faith, the principles used by the parties in conducting Electronic Transactions are not intended to intentionally and without rights or against the law cause harm to other parties without the knowledge of the other party.
e. Freedom to choose technology or be technology-neutral. The principle of the use of Information Technology and Electronic Transactions is not focused on using certain technologies so that they can follow developments in the future.

Utilization of information technology and electronic transactions are carried out with the aim of:

a. Educating the nation's life as part of the world's information society;
b. Develop trade and the national economy to improve the welfare of the community;
c. Improve the effectiveness and efficiency of public services;

E-ISSN : 2723-2476
ISSN : 2723-1968
ACLJ, Vol.4, Issue 2, 2023

d. Open the broadest possible opportunity for everyone to advance their thinking and abilities in the field of optimal and responsible use and utilization of information technology; and
e. Provide a sense of security, justice, and legal certainty for users and information technology providers.

Law Number 11 of 2008 concerning Information and Electronic Transactions (UU ITE) is the first law in the field of information technology and electronic transactions as a product of legislation that is very much needed and has become a pioneer in laying the basis for regulations in the field of utilizing information technology and electronic transactions. However, in reality, the implementation journey of the ITE Law has encountered problems.

2. Challenges and Opportunities to Overcome Problems in the Use of Information and Communication Technology

Nationally, there are several problems related to the development of solid cyber-security, including the weak understanding of state administrators on security related to the cyber world which requires restrictions on the use of services whose servers are located abroad and the use of secured systems is required; the absence of adequate legality for handling attacks in the cyber world; governance of cyber-security institutions nationally which is still partial and scattered and the absence of standardized coordination in handling cyber-security problems; our industry is still weak in producing and developing hardware or hardware related to information technology (Ardiyanti, 2014). Cyber law is a multidisciplinary law relating to other branches of science, such as criminal law, civil law, consumer protection, economics, and administration with technological, socio-cultural (ethical) and legal approaches (Ersya, 2017).

Cybercrime is a dark side of the advancement of information and communication technology, which brings enormous implications in all areas of life especially closely related to economic crime (Jhon, 2018). Therefore, there are several approaches to maintaining security in cyberspace: legal, technological, social, cultural, and ethical. The legal approach is absolute to overcome security disturbances in the operation of electronic systems because without legal certainty, the problem of using information technology is not optimal.

The challenges faced relating to law enforcement on the regulations that have been set, namely how the substance of the contents in these regulations is. Some decisions of the Constitutional Court state that criminal acts of insult and defamation in the field of electronic information and electronic transactions are not merely a general crime, but a complaint offense. The affirmation of the complaint offense is intended to be in line with the principles of legal certainty and a sense of community justice.

The provisions regarding searches, confiscations, arrests, and detentions regulated in the ITE Law create problems for investigators because criminal acts in the field of information technology and electronic transactions are so fast and perpetrators can easily obscure crimes or evidence of a crime. The characteristics of cyberspace virtual allow illegal content such as information and/or electronic documents that have content that violates decency, gambling, insults or defamation, extortion and/or threats, spreading false and misleading news resulting in consumer losses in electronic transactions, and acts of spreading hatred or hostility based on ethnicity, religion, race, and class, and sending threats of violence or intimidation aimed at personally can be accessed, distributed, transmitted, copied, stored for re-dissemination from anywhere and anytime.

The use of any information through media or electronic systems concerning a person's personal data must be carried out with the consent of the person concerned. For this reason, it is necessary to guarantee the fulfil of personal protection by requiring each electronic system operator to delete irrelevant electronic information and/or electronic documents under their control at the request of the person concerned based on a court order. In addition, the public can play a role in increasing the use of information technology through the use and operation of electronic systems and electronic transactions by the provisions of the law. The role of the community can be carried out through institutions formed by the community.

Therefore, the government as a party is obliged to provide security by accommodating the protection of the use of technology and information by reforming legislation in the field of information and communication technology. Cooperation between countries can also be a reference for the government considering the extent of the cyber world which is a threat to the security of the use of information and communication.

IV. CONCLUSION

The results of the research show that the Indonesian government has issued a law on electronic information and transactions. Furthermore, several work teams have been formed under state agencies/institutions that focus on responding to information security issues, such as a team under the auspices of the Ministry of Communication and Information Technology, there are also other teams within the Polri work environment. The challenges faced are related to law enforcement against regulations that have been stipulated, namely how the substance of the contents of these regulations can accommodate the protection/guarantee of information and technology security in Indonesia which continues to develop so that it requires updating of laws and regulations. In addition, the government's responsiveness and responsiveness supported by human resource capabilities, facilities and infrastructure are also factors in the success of guaranteeing the security protection of the use of information and communication technology, which can be accompanied by cooperation between countries.

REFERENCES

Akub, M. S. (2018). *Pengaturan Tindak Pidana Mayantara (Cyber Crime) dalam Sistem Hukum Indonesia*. *21*(2), 85–93. https://doi.org/10.33096/aijih.v21i2.19

Al-Fatih, S. (2023). *Perkembangan Metode Penelitian Hukum di Indonesia* (1st ed.). UMM Press.

Anjani, N. H. (2021). Perlindungan Keamanan Siber di Indonesia. In *CIPS* (pp. 1–12). CIPS: Center for Indonesian Policy Studies.

Ardiyanti, H. (2014). Cyber-Security Dan Tantangan Pengembangannya Di Indonesia. *Jurnal Politicia*, *5*(1), 95–110. https://doi.org/10.22212/jp.v5i1.336

Aulianisa, S. S., & Indirwan, I. (2020). Critical Review of the Urgency of Strengthening the Implementation of Cyber Security and Resilience in Indonesia. *Lex Scientia Law Review*, *4*(1), 33–48. https://doi.org/10.15294/lesrev.v4i1.38197

Bawono, B. T. (2019). Reformation of Law Enforcement of Cyber Crime in Indonesia. *Jurnal Pembaruan Hukum*, *6*(3), 332–349. https://doi.org/10.26532/jph.v6i3.9633

E-ISSN : 2723-2476
ISSN : 2723-1968
ACLJ, Vol.4, Issue 2, 2023

Chotimah, H. C. (2019). Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara [Cyber Security Governance and Indonesian Cyber Diplomacy by National Cyber and Encryption Agency]. *Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional*, *10*(2), 113–128. https://doi.org/10.22212/jp.v10i2.1447

Ersya, M. P. (2017). Permasalahan Hukum dalam Menanggulangi Cyber Crime di Indonesia. *Journal of Moral and Civic Education*, *1*(1), 50–62. https://doi.org/10.24036/8851412020171112

Hartono, B., & Hapsari, R. A. (2019). Mutual Legal Assistance Pada pemberantasan Cyber Crime Lintas Yurisdiksi di Indonesia. *Sasi*, *25*(1), 59. https://doi.org/10.47268/sasi.v25i1.136

Irwansyah. (2020). *Penelitian Hukum: Pilihan Metode & Praktik Penulisan Artikel* (A. Yunus (ed.)). Mirra Buana Media.

Jhon, R. M. (2018). Existence of Criminal Law on Dealing Cyber Crime in Indonesia. *Indonesian Journal of Criminal Law Studies*, *3*(1), 25–34. https://doi.org/10.15294/ijcls.v3i1.16945

Junaidi, M., Sukarna, K., & Sadono, B. (2020). PEMAHAMAN TINDAK PIDANA TRANSAKSI ELEKTRONIK DALAM UNDANG-UNDANG NO 19 TAHUN 2016 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK. *BUDIMAS : JURNAL PENGABDIAN MASYARAKAT*, *2*(2). https://doi.org/10.29040/budimas.v2i2.1355

Prastini, E. (2018). Kebijakan Kriminal Pemerintah terhadap Kejahatan Dunia Maya (Cyber Crime) di Indonesia. *Jurnal Surya Kencana Dua: Dinamika Masalah Hukum Dan Keadilan*, *5*(2), 594–610. https://doi.org/10.32493/SKD.v5i2.y2018.2341

Putra, A. M. A., Isrok, M., & Hidayah, N. P. (2023). Legal Protection of Remote Working Workers in Particular Time Employment Agreements. *Audito Comparative Law Journal (ACLJ)*, *4*(1), 22–30. https://doi.org/10.22219/aclj.v4i1.24033

Raharja, I. F. (2019). Bijak Menggunakan Media Sosial di Kalangan Pelajar Menurut Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik. *Jurnal Selat*, *6*(2), 235–246. https://doi.org/10.31629/selat.v6i2.1437

Setiyawan, W. B. M., Churniawan, E., & Faried, F. S. (2020). Information Technology Regulatory Efforts in Dealing With Cyber Attack To Preserve State. *Jurnal USM Law Review*, *3*(2), 275–295. https://doi.org/10.26623/julr.v3i2.2773

Setyawan, D. P. S. A. D. W. (2016). Diplomasi Pertahanan Indonesia dalam Pencapaian CyberSecurity Melalui ASEAN Regional Forum On CyberSecurity Initiative. *Jurnal Penelitian Politik*, *13*(1), 1–13. https://doi.org/10.14203/jpp.v13i1.250

Syahriar, I. (2021). Revisi Undang-Undang Informasi Dan Transaksi Elektronik Dalam Dimensi Politik Hukum. *The Juris*, *5*(1), 6–14. https://doi.org/10.56301/juris.v5i1.183

Umbara, A., & Setiawan, D. A. (2022). Analisis Kriminologis Terhadap Peningkatan Kejahatan Siber di Masa Pandemi Covid-19. *Jurnal Riset Ilmu Hukum*, 81–88. https://doi.org/10.29313/jrih.v2i2.1324

Widiastuti, T. W. (2009). Peranan Perubahan Sosial terhadap Macam Alat Bukti dalam RUU KUHAP. *Wacana Hukum*, *8*(1). https://doi.org/10.33061/1.jwh.2009.8.1.319

Wijaya, H., & Herwastoeti, H. (2022). Criminal & Civil Liability Related to Misuse of Illegal

Fintech Customer Data During The Covid-19 Pandemic. *Audito Comparative Law Journal (ACLJ)*, *3*(1), 1–9. https://doi.org/10.22219/aclj.v3i1.19873

Wijaya, M. R., & Arifin, R. (2020). Cyber Crime in International Legal Instrument: How Indonesia and International Deal with This Crime? *IJCLS (Indonesian Journal of Criminal Law Studies)*, *5*(1), 63–74. https://doi.org/10.15294/ijcls.v5i1.23273