**BALTIC JOURNAL OF LAW & POLITICS**
A Journal of Vytautas Magnus University
VOLUME 15, NUMBER 7 (2022)
ISSN 2029-0454

Cite: *Baltic Journal of Law & Politics* 15:7 (2022): 268-279
DOI: 10.2478/bjlp-2022-007019

# Technical Guidelines Design of Using Electronic Evidence in Cybercrime Cases

**Harli Siregar**
Universitas Sumatera Utara, Medan, North Sumatera, Indonesia

**Topo Santoso**
Universitas Indonesia, Depok, Indonesia

**Alvi Syahrin**
Universitas Sumatera Utara, Medan, North Sumatera, Indonesia

**Mahmud Mulyadi**
Universitas Sumatera Utara, Medan, North Sumatera, Indonesia

Received: October 15, 2022; reviews: 2; accepted: December 28, 2022

**Abstract**

The era of globalization is marked by digitalization to further bring positive and negative impacts. The world seemed without limits with various facilities, but there were also deviations in the form of cybercrime. The Criminal Procedure Code only regulates the types of evidence of witness testimonies, expert statements, letters, instructions and statements of the accused. The existence of electronic evidence becomes a debate because it has actually happened in cyberspace. In practice it always raises questions related to chain of custody, authentication or the authenticity of evidence. This research was conducted by using the normative juridical approach (qualitative) by analyzing the concept of law in relation to real conditions is proposed. It is required standard and certified digital forensics as well as documentation in the form of minutes of every action. Stronger and more detailed regulations in the form of technical guidelines and their implementation for law enforcement officers have been prepared and tested. In addition, it is necessary to change the way of thinking that is more honest and constructive for law enforcement officials.

**Keywords**

Cybercrime, electronic evidence, technical guidelines

**JEL Classifications:** J11, F43

## 1. Introduction

The current COVID-19 pandemic has brought about changes in the order of human life, whether political, economic, social, cultural, including law. People's habits changed almost one hundred and eighty degrees. As social beings, humans always live together in social interaction by meeting or meeting face to face directly, but this pandemic has eradicated this habit and created a new habit, namely the increased use of electronic media as a communication device. Technology is something that cannot be separated from life in the era of globalization. World civilization is related to the advancement of information technology covering all elements of life. Globalization since the beginning of the 20th century, marked when there was a transportation and electronic revolution that spread and accelerated trade between nations, in addition to the increase and speed of traffic of goods and services (Mansur, 2009). This condition makes distance, space and time no longer a significant barrier in interacting. The information technology revolution began since the invention of the computer and in its development has formed a new world commonly known as cyberspace. The progress and development of technology, especially telecommunications, multi media and information technology (telematics) will ultimately change the organizational structure and social relations (Mansur, 2009).

The role of technology and information is increasingly important, massive and a necessity in the atmosphere of the COVID-19 pandemic. In this context, it raises the question of whether law as a rule is able to adapt or even lag behind, or even more sadly, the law operates independently of the development of technology and information. The phrase that says "ubi societas ibi ius" where there is a society there is a law means that the existence of law is indispensable to regulate human life. Telematics convergence is in the form of organizing an electronic system based on digital technology known as the net (Makarim, 2017). The use of internet technology other than for good purposes is also not uncommon to be misused by certain parties. The perpetrators of criminal offenses are not limited to cybercrime but are also used in conventional criminal acts. In cybercrime there are 2 (two) types, namely computer crime and computer related crime. Both are similar terms but not the same. Computer crime is a crime that uses a computer as the main tool to commit a crime such as defacement (changing the pages of a site illegally), denial distributed of service (making a system not working or not functioning properly after being flooded with data by so many computers that have been infected and become a network reboot, keylogging (recording every typing activity on the keyboard and applications that appear on the screen), identity theft (theft of important data from people who are targeted), intrusion (illegally entering into a system) while computer related crime is all kinds of traditional crime such as theft, pornography, robbery, murder, corruption, narcotics and so on (Al-Azhar, 2012).

In cybercrime there is evidence in the form of electronic devices such as mobile phones and computers used by perpetrators to communicate with each other or store data relating to the planning, process and outcome of the crime. Some examples of crimes that are often committed include the crime of murder, the perpetrator before killing the victim communicates via handphone sending an email or WhatsApp message before the incident. Along with technological developments in uncovering criminal cases, law enforcement officials will try to collect evidence and evidence that is considered to be able to strengthen the evidence in the trial (Al-Azhar, 2012). In the practice of the integrated criminal justice system in Indonesia, efforts to trace evidence and evidence are the authority of investigators who carry out the investigation function, the Public Prosecutor conducts prosecutions, Judges try and drop verdicts / penalties and correctional institutions carry out decisions / penalties. The flow of the law enforcement process has the same goal, namely how material truth can be obtained to realize the legal goals, namely justice, certainty, and legal benefits. The successful prosecution of criminal cases cannot be separated from the good quality of the investigation by the investigator. A case can be proven in a court of law that is inseparable from the ability of the Prosecutor as the Public Prosecutor to understand and scrutinize the results of investigating investigators. The Public Prosecutor is able to state in a good, high-quality indictment and illustrates the material actions of the criminal offender. In the trial process the prosecutor as the public prosecutor may submit any evidence and evidence presented at the hearing to convince the judge and obtain material truth.

If judging from the mode of legal thought, the integrated criminal justice system in Indonesia is part of the civil law system that is different from the common law system. The civil law starts from one general principle to another general principle while common law starts from case to case (Ferdiles, 2019). Cases are the main source of common law, while codified laws and laws are the parts that make up civil law. Common law practitioners think within the scope of certain groups and legal relationships, while civil law practitioners think within the scope of enforced regulations, which have been codified or based on laws that can be applied to the situation at hand (de Cruz, 2017). Electronic evidence becomes a global legal realism that goes into all pluralist world legal family systems. There is a main dilemma that is exposed in a pluralist perspective: the law is likely to never be fully satisfying all parties (Menski, 2017; Israhadi, 2015). Indonesian criminal constitution regulates the limitations of evidence that can be submitted before a trial and evidence outside the criminal procedure code, namely constitution of No. 11 of 2008 as amended by constitution of No. 19 of 2016 concerning the constitution of electronic information and transaction (EIT). In the general provisions of the EIT constitution, it is known that the types of electronic data such as writing, photos, sounds, images are electronic information while the types of electronic information such as text, photos, sounds, images stored on a flash disk that can be opened through a computer are electronic documents.

In its development there are many laws governing criminal procedural law which also regulate electronic evidence, although it is substantively different in its categorization. The Corruption Crimes Act, for example, categorizes electronic evidence as evidence evidence, while the Law on Money Laundering and Eradicating Terrorism places electronic evidence as stand-alone evidence. Some debates in practice about electronic evidence in cyber cases include: the problem of the existence of evidence brought by the trial regarding content while the content is in a media package such as a cellphone, which is authorized to obtain evidence, how to obtain evidence by law enforcement officials, doubt about the authorities law enforcers who play around with evidence, the availability of trusted and certified experts in reconstructing the contents of evidence, the existence of media that wraps content (when the court has declared the guilty person and the content must be executed while the content cannot stand alone outside the media) (Bakhri, 2015). All of these debates are crucial aspects related to the procedure of obtaining electronic evidence.

These problems can be seen in the case on behalf of Setya Novanto (Former Chairperson of the Indonesian Parliament) and Ratna Sarumpaet (a woman figure and democracy activist). Ratna Sarumpaet has been charged by the Public Prosecutor with the following violations: First, Article 14 paragraph (1) of Law no. 1 of 1946 concerning the Criminal Law Regulations, namely broadcasting false news or news by deliberately publishing trouble among the people; or with the Second Article 28 paragraph (2) Jo 45A paragraph (2) of Law no. 19 of 2016 concerning amendments to Law no. 11 of 2008 concerning EIT, namely intentionally and without rights spreading information aimed at causing hatred or hostility to certain individuals and/or community groups based on ethnicity, religion, race and class (Sasmito, 2017). In the end, the case of Ratna Sarumpaet was prosecuted by the Public Prosecutor and by the court was convicted of spreading false news that caused trouble as stated in Article 14 paragraph (1) of Law no. 1 of 1946 and not with the EIT Law even though the person concerned spread the lie through electronic means sarana. Setya Novanto conducted a judicial review about the validity of the electronic evidence used by the prosecutor to the Constitutional Court (MK). In its decision No. 20 / PUU-XIV / 2016, the Constitutional Court decided that electronic evidence became valid evidence, its acquisition must be legally carried out in the context of law enforcement (MK RI Decision 2016). Recognition of electronic evidence as legal evidence is not only limited to the obligation of the court to realize but also constitutional rights of the people. Various studies have been carried out related to cybercrime. Computer forensics is used as a computer inquiry application and analysis technique to determine legal evidence that may be related to computer network crimes (Lubis & Siahaan, 2016). Hikmatyar et al., (2017) proposed the Integrated Digital Forensic Investigation Framework (IDFIF) method for general cybercrime investigations. The basic principles of electronic evidence taking, the process and model of cybercrime investigation, and the collection of evidence

were developed. How to detect digital data sources, the process of gathering evidence, maintaining integrity, searching for data related to crime, analyzing results, recovering data that is deleted, encrypted or damaged, and reporting recently investigated by Solak & Topaloglu (2015). To measure and assess levels interest in technology, the level and perceptions of individuals about cybercrime in terms of ethics and law have been measured using quesstionare instruments. The purpose of the research is to help interested parties to define the general level of perception of cybercrime.

The use of a fingerprint device in the form of a Run Tracker to identify unique criminal devices as legal and infallible evidence in court has been reviewed (Yogesh, 2020). This method is used as an anticipation if the attacker tries to format the system or modify device parameters. Rahman & Tomar (2020), proposed four web forensic frameworks as a frame of reference to verify crimes committed using automated bots. Evaluation of reported active and passive risk behaviors is done by predicting cyber security behavior intentions (Arend et al., 2020). The results found that the intention of cyber security behavior and actual cyber behavior significantly correlated with individual self-reported differences in passive risk behavior but not in active risk behavior. In research conducted by, it was found that technological limitations and low levels of legislative compliance were the main factors in preventing and overcoming cyber security breaches (Wang et al., 2020). Various other studies related to cybercrime have also been carried out along with the increasing need for dependence of many people on cyberspace. From the background description above raises issues such as the position and technique of collecting electronic evidence in proving cybercrime. In practice electronic evidence is always a matter of debate between the Prosecutor, Judge and Legal Counsel. This concerns the question of how to obtain (whether it is in accordance with the law or not) so that in the future it takes a special arrangement regarding the acquisition, examination, and management of evidence.

## 2. Method

Cybercriminal cases handled by the public prosecutor in the cybercrime criminal investigation unit of the National Police of Indonesia from 2016-2020 as shown in the Table 1 were used as study case in this research.

Table 1. List of cybercriminal cases (prosecutor general's criminal)

| No | Year | Number of Case | Evidence |
|---|---|---|---|
| 1. | 2016 | 13 | The data is the SPDP from the investigator to the public prosecutor |
| 2. | 2017 | 14 | |
| 3. | 2018 | 54 | |
| 4. | 2019 | 53 | |
| 5. | 2020 (June) | 28 | |

In designing technical guidelines for the use of electronic evidence in cybercrime cases, this study uses a normative juridical approach by photographing how to regulate electronic evidence in legislation to technical rules in relation to the study of literature and regulations. Qualitative research by collecting and processing data through the interview format, by asking the views of law enforcement officers in the field to test how electronic evidence can be accepted as valid evidence in court.

## 3. Results and Discussions

### 3.1 Conditions and Characteristics of Cybercrime Cases

The data in the Table 2 tries to provide an illustration of how the spread of cybercrime in terms of the action qualification and the distribution of cybercrimes from the side of the crime scene to see how far cybercrime has occurred in Indonesia.

Table 2. Electronic Information and Transaction (EIT) Crime Case Data According to the Delict Qualifications

| No | Delict Qualification | 2016 | 2017 | 2018 | 2019 | 2020 |
|---|---|---|---|---|---|---|
| 1. | Immorality, Gambling, Humiliation, Extortion) | 3 | 2 | 27 | 18 | 3 |
| 2. | Fake & Misleading News, Hate and Hostile News | 2 | 10 | 20 | 28 | 17 |
| 3. | Threats of Violence and Scare | 2 | - | 1 | 3 | - |
| 4. | Unlawful acts on other party's computer access without permission | 5 | 1 | 4 | 3 | 4 |
| 5. | Wiretapping, Alteration, Loss of Electronic Information | - | 1 | - | - | - |
| 6. | Prohibition of interference with Information/ Electronic documents | 1 | - | 2 | 1 | 4 |
| | **Total** | **13** | **14** | **54** | **53** | **28** |

Based on the number of cybercrimes associated with the qualifications of the offenses, it is illustrated that the cybercrimes that have occurred have covered almost all acts regulated in the EIT law even though the dominating acts are: fake news or hoaxes, hatred and hostility, fraud, decency and illegal access. In practice, there is always a debate between law enforcement officers, there is always a debate whether something posted is an insulting news, what are the parameters, such as an act of insulting the head of state because in other countries it may not be a form of humiliation. In addition, the number of cybercrimes from year to year has increased both in terms of the number and quality of crimes. Meanwhile, judging from the distribution according to the location of the case (*locus delicti*) in Indonesia, it can be described in Table 3.

Table 3. Handled Cybercrime Case Recapitulation by Indonesian Prosecutors Year of 2016-2019

| No | High Prosecutor | 2016 | 2017 | 2018 | 2019 |
|---|---|---|---|---|---|
| 1 | Aceh | 7 | 8 | 25 | 21 |
| 2 | Sumatera Utara | 21 | 28 | 87 | 87 |
| 3 | Sumatera Barat | 7 | 5 | 4 | 3 |
| 4 | Riau | 2 | 3 | 11 | 4 |
| 5 | Kepulauan Riau | - | 7 | 11 | 11 |
| 6 | Jambi | 7 | - | 10 | 2 |
| 7 | Sumatera Selatan | - | 2 | 3 | 1 |
| 8 | Kepulauan Bangka Belitung | 6 | 2 | 8 | 3 |
| 9 | Lampung | 4 | 9 | 19 | 22 |
| 10 | Bengkulu | 1 | - | 18 | 4 |
| 11 | DKI Jakarta | 21 | 10 | 16 | 22 |
| 12 | Jawa Barat | 17 | 23 | 60 | 51 |
| 13 | Banten | 4 | 8 | 13 | 24 |
| 14 | Jawa Tengah | 13 | 10 | 51 | 25 |
| 15 | D.I. Yogyakarta | 11 | 11 | 2 | *7* |
| 16 | Jawa Timur | 26 | 45 | 71 | *58* |
| 17 | Kalimantan Barat | 2 | 7 | 24 | *28* |
| 18 | Kalimantan Tengah | 3 | 9 | 27 | *10* |
| 19 | Kalimantan Selatan | 1 | 4 | 14 | *11* |
| 20 | Kalimantan Timur | 8 | 7 | 5 | 12 |
| 21 | Sulawesi Utara | 8 | 19 | 12 | 6 |
| 22 | Gorontalo | 6 | 6 | 5 | 1 |
| 23 | Sulawesi Barat | - | - | - | - |
| 24 | Sulawesi Tengah | 9 | 14 | 11 | 7 |
| 25 | Sulawesi Tenggara | - | - | 1 | 9 |
| 26 | Sulawesi Selatan | 15 | 6 | 16 | 12 |
| 27 | Bali | 4 | 9 | 15 | 17 |
| 28 | Nusa Tenggara Barat | 16 | - | 3 | 1 |
| 29 | Nusa Tenggara Timur | 9 | 17 | 8 | 5 |
| 30 | Maluku | - | - | 4 | 7 |
| 31 | Maluku Utara | - | - | 5 | 1 |
| 32 | Papua Barat | - | - | 1 | 4 |
| 33 | Papua | 2 | 5 | 11 | 9 |
| **Total** | | **233** | **274** | **571** | **485** |

The data in the Table 2 shows that technological progress is experiencing rapid growth from the western to the eastern regions in Indonesia as evidenced by the spread of cybercrime not only in developed and heterogeneous areas but also in underdeveloped and homogeneous areas. In addition, the number of cybercrimes which tends to increase from year to year shows that people are increasingly aware or literate of the law in the field of EIT or vice versa that technology abuse tends to increase. From the side of cybercrime prevention, the above figures cannot be taken lightly because the spread of cybercrime indicates that perpetrators can commit cybercrimes from anywhere and to anyone in a different area or locus (Nasir et al., 2019).

In tracing the handling of cybercriminal cases as depicted in the Table 1, it turns out that from the view of the public prosecutors and law enforcement officers

handling cases in court. It was found various problems or difficulties encountered both related to proof, evidence, administration and other issues. Criminal offenses in the EIT sector were more emphasized on digital / electronic evidence so that public prosecutors must seriously pay attention to the results of digital forensic laboratory examinations made by the National Police Headquarters or the Ministry of Communication and Information to ensure the locus and tempus delicti.

In criminal acts in the EIT field, there were usually no witnesses who witness the event directly but emphasizes the compatibility between the results of digital forensic laboratories with the electronic evidence obtained (cellphones, laptops, etc.) so that the suspect / defendant will be identified, for this reason the prosecutor must seriously examine the suitability. The existence of expert testimony in cases in the EIT field was urgently needed especially digital forensic and linguist experts to strengthen the description of the elements of the alleged article by ensuring their presence in court because expert testimony, especially digital forensics, is very instrumental in explaining the flow of deviations perpetrated by suspects / defendants.

There was still an opinion difference whether the investigator attaches enough captures or the alleged content in the case file or must do digital forensics (digital forensic laboratorium does not yet exist in the region). The public prosecutor must ensure that the evidence (cellphones, laptops, etc. that are electronic) was obtained by the investigator in a manner consistent with confiscation rules to avoid complaints or rebuttal that the evidence does not belong to the suspect / defendant and ensure the contents are in accordance with alleged. Electronic evidence obtained in stage II or in a trial before requesting the testimony of digital forensic experts must be ensured not to be opened or tampered with either by the public prosecutor or the evidence officer. This aims to avoid any changes in the content or data that are alleged but sufficient with the minutes of receipt of electronic evidence from the investigator as is (sterile) until the digital forensic expert explains the trial.

Administrative arrangements on how to destroy electronic evidence including restrictions if it relates to content in the form of e-mail, facebook, etc., it is enough to just destroy the contents or also include the packaging. There are still difficulties in the field related to vendors affiliated or domiciled abroad such as Yahoo or Gmail who do not want to open access related to criminal acts such as hate speech (statements of hatred / animosity). They consider that this is part of freedom of expression through social media facilities unless it is related to certain crimes such as terrorism.

### 3.2 Position of electronic evidence in proving cybercrime

The EIT law regulates two major parts, namely regulation of information and electronic transactions and of prohibited conduct. The EIT law confirms new evidence in the form of electronic information and documents along with printouts

as legal evidence which is commonly called electronic evidence. Electronic evidence is an extension of the evidence set out in the criminal procedure code.

The EIT law explains that electronic information and / or electronic documents and / or printouts are valid evidence. Electronic information is one or a collection of electronic data, including but not limited to text, sound, images, maps, designs, photographs, electronic data interchange (EDI), electronic mail, telegram, telex, telecopy or the like, letters, signs, numbers, access codes, symbols, or processed perforations that have meaning or can be understood by people who are able to understand them. Electronic documents are any electronic information created, forwarded, sent, received, or stored in analog, digital, electromagnetic, optical, or the like, which can be seen, displayed and / or heard through a computer or electronic system, including but not limited to in writing, sound, pictures, maps, designs, photographs or the like, letters, signs, numbers, access codes, symbols or perforations that have meaning or meaning or can be understood by people who are able to understand it (law No. 11 of 2008 concerning EIT).

Thus, electronic information can be distinguished but cannot be separated with electronic documents. Electronic information is data or data collection in various forms while electronic documents are containers or packages of electronic information. For example, music files in the form of mp3, then all information or music that comes out of the file is electronic information while the electronic documents from the file are mp3.

There are two views about the position of electronic evidence. The first view states that electronic evidence is separate evidence that is separate from the evidence in the criminal procedure code, while the second view states that electronic evidence is included in the categorization of evidence that already exists or does not stand alone. For example, Law No. 8 of 1997 concerning Company Documents categorizing electronic evidence as an extension of documentary evidence in the criminal procedure code. While electronic documents are part of company documents and company documents referred to are part of the evidence of letters (Ismail, 2017).

Related to the position of electronic evidence, among academics there are two opinions. The first opinion, Ismail (2017) said that electronic evidence in the form of electronic information and electronic documents as well as printed results is an expansion of evidence from the criminal procedure code so that there is no need to dispute whether electronic evidence is an extension of letter evidence. Basically, electronic evidence is the addition of new evidence in addition to those in the criminal procedure code. The evidence of criminal cases currently consists of 5 (five) pieces of evidence as witnesses' statements, expert statements, letters, instructions, defendant's information and electronic information, and electronic documents and / or printouts. The second opinion stated that the position of electronic evidence must be further explored in substance or content. Electronic information evidence and electronic documents can be categorized as an expansion of letter and evidence evidence (Ismail, 2017).

Although there are differences of views among academics, in practice, the existence of electronic evidence has been recognized and applied. Therefore, for evidence in trial of cybercriminal cases, the Public Prosecutor may use electronic evidence as independent evidence.

### 3.3 Electronic evidence collection techniques to ensure the validity of evidence of cybercrime

Although the existence of electronic evidence has been recognized, but there are challenges in obtaining it. Confiscation of digital evidence is different from non-digital. As an example of a criminal offense, investigators can immediately confiscate related physical items such as payment receipts, proof of transfer, etc. but differ from digital evidence where due to the characteristics of the evidence it has a storage place or media so it allows information that is not related to the crime such as personal photos, videos, will be confiscated.

Another problem is the possibility of erasing existing data in digital evidence that can be done remotely or because of incorrectly entering the security code and the lack of understanding of the investigator to confiscate digital evidence at the scene of the case. Another challenge is that state jurisdiction such as digital evidence is not at the scene of the case because the server is in another country. The United States requires internet service providers (Internet Service Providers) to comply with the Electronic Communications Privacy Act (ECPA). This condition will be difficult when the server of the company is in another country, so a mutual legal assistant (MLA) mechanism is needed that requires a long time.

Digital evidence that will be used as evidence must have certain conditions. By its nature, digital evidence cannot be directly used as evidence for the trial process, so a standard is needed so that all digital evidence can be used as evidence:

- Acceptable, that is data must be able to be accepted and used by law starting from the interests of the investigation to the interests of the court;
- Original, i.e., the evidence must be related to the incident / case that occurred and not fabricated;
- Complete, i.e., the evidence can be said to be good and complete if there are many clues in it that can help the investigation;
- Trustworthy, i.e., the evidence can say things that happened behind it if the evidence can be trusted then the investigation process will be easier and the condition is a must.

The standard mentioned above turns out that in the EIT Law the minimum digital evidence requirements have been determined that they are able to re-display information and / or electronic documents in full in accordance with the retention period stipulated by statutory regulations; protect the availability, integrity, authenticity, confidentiality and accessibility of electronic information in

the operation of the electronic system; operate in accordance with procedures or instructions in the operation of the electronic system; were equipped with procedures or instructions announced in language, information or symbols that can be understood by the parties concerned with the operation of the electronic system; and, have a sustainable mechanism to maintain the novelty, clarity and accountability of procedures or instructions (Gema, 2008).

In addition to the quality of electronic evidence obtained, it is also important to determine the location of the crime case (locus delicti) of cybercrime. There are several methods that can be applied in Indonesia by taking into account the theories that apply in the United States by Darrel Menthe. Theory of the uploader and the downloader which emphasizes that in the cyber world there are two main things, the uploader (the party that provides information into cyber space) and the downloader (the party that accesses information). Theory of law of the server where the investigator treats servers where web pages are physically located and where they are recorded or stored as electronic data. Theory of International Space explains that cyber space is considered as a separate legal environment from conventional law where every country has the same sovereignty. Related to the above requirements, digital forensic is needed for the digital evidence. Digital forensic is an absolute requirement that must be done so that electronic information and documents can be used as evidence both at the level of investigation, investigation, prosecution and trial. Without going through digital forensic, an electronic device cannot be made as evidence because it cannot be guaranteed validity.

## 4. Conclusions

Placing electronic evidence in law enforcement of cybercrime as evidence that stands alone in practice is inseparable from other evidence such as experts or letters that explain their existence. Digital forensics with quality standards and certification are the right step in determining and testing the validity of electronic evidence.

The need for regulation of derivative regulations from clear and decomposed laws governing the procedures and standard mechanisms for collecting electronic evidence to ensure validity in proving cybercrime. Efforts should be made to build a culture of culture (culture set) of law enforcement officials in the framework of law enforcement of cybercrime that is more qualified and responsible.

## References

Al-Azhar, M. N. (2012). *Digital Forensik (Panduan Praktis Investigasi Komputer)*. Jakarta: Salemba.

Arend, I., Shabtai, A., Idan, T., Keinan, R., & Bereby-Meyer, Y. (2020). Passive- and not active-risk tendencies predict cyber security behavior. *Computers & Security*, *97*, 101964.

Bakhri, S. (2015). Nasionalisasi Hukum Pidana Dan Hukum Acara Pidana Dan Keharusan Peradaban. *Lex Publica*, *1*(2).

de Cruz, P. (2017). *Perbandingan Sistem Hukum, Common Law, Civil Law and Socialist Law (Terjemahkan Narulita Yusron)*. Bandung: Penerbit Nusa Media.

Ferdiles, L. (2019). Reformasi Hukum dalam Penerapan Restorative Justice dalam Sistem Pidana Nasional. *Lex Publica*, *6*(1), 25–31.

Gema, A. J. (2008). *Apakah Dokumen Elektronik Dapat Menjadi Alat Bukti yang Sah*?. Available at: http://arijuliano.blogspot.com/2008/04/apakah-dokumen-elektronik-dapat-menjadi.html.

Hikmatyar, M., Prayudi, Y., & Riadi, I. (2017). Network forensics framework development using interactive planning approach. *International Journal of Computer Applications*, *161*(10), 41-48.

Israhadi, E. I. (2015). Pembangunan Hukum Dan Sistem Hukum. *Lex Publica*, *2*(1).

Lubis, A., & Siahaan, A. P. U. (2016). Network forensic application in general cases. *IOSR J. Comput. Eng*, *18*(6), 41-44.

Makarim, E. (2017). *Pengantar Hukum Telematika, Suatu Kompilasi Kajian*. Jakarta: PT. RajaGrafindo Persada.

Mansur, D. M. A. (2009). *Cyber Law Aspek Hukum Teknologi Informasi*. Bandung: Aditama.

Menski, W. (2017). *Perbandingan Hukum dalam Konteks Global: Sistem Eropa, Asia dan Afrika*. Bandung: Penerbit Nusa Media.

Nasir, G. A., Dimyati, K., & Absori, A. (2019). Jaminan Hukum atas Pengakuan dan Eksistensi Hak Ulayat pada Masyarakat Hukum Adat. *Lex Publica*, *6*(1), 32–40.

Rahman, R. U., & Tomar, D. S. (2020). A new web forensic framework for bot crime investigation. *Forensic Science International: Digital Investigation*, *33*, 300943.

Sasmito, J. (2017). Application of the Retroactive Principle in Criminal Law on Gross Human Rights Violations. *Lex Publica*, *4*(2), 775–781.

Solak, D., & Topaloglu, M. (2015). The perception analysis of cyber crimes in view of computer science students. *Procedia-Social and Behavioral Sciences*, *182*, 590-595.

Wang, V., Nnaji, H., & Jung, J. (2020). Internet banking in Nigeria: Cyber security breaches, practices and capability. *International Journal of Law, Crime and Justice*, *62*, 100415.

Yogesh, P. R. (2020). Backtracking tool root-tracker to identify true source of cyber crime. *Procedia Computer Science*, *171*, 1120-1128.