Confiscation of Electronic Evidence Cyber Crime in Business and Law Collaboration After Pandemic Achieving Sustainable Legal Development

Idham Qrida Nusa(✉), Bambang Sugiri, Yuliati Yuliati, and Faizin Sulistio

Universitas Brawijaya, Malang, Indonesia
idhaman63@student.ub.ac.id

Abstract. This paper aims to find out how the confiscation of digital evidence in cybercrime cases from the perspective of the COVID-19 pandemic uses post-pandemic business and legal collaboration to encourage sustainable legal development. The analysis highlights how the use of cloud storage as a storage results in crime, in the form of ATM owner privacy data. Such as case studies that show how digital evidence, as a form of information technology advancement, allows the wearer to cross the jurisdictional boundaries of each country. Jurisdictional issues on the internet are closely related to law enforcement issues in each country. As a world without borders, applying jurisdiction on the internet is not easy. There needs to be certainty about the law that will be applied in a world without borders. The jurisdiction of a country as we know it can be developed and used in a world without borders. This study examines the subject matter through a normative juridical approach, legal approach, case approach, qualitative analysis, examines the principle of legal certainty philosophically. By analyzing the theory of criminal law and confiscation. Business and legal collaboration in the form of cloud storage service products will provide advantages and benefits for all parties. There needs to be certainty about the law that will be applied in a world without borders. The jurisdiction of a country as we know it can be developed and used in a world without borders.

Keywords: Confiscation · Cyber Crime · Cloud Storage · Electronic Evidence · Sustainable Legal Development

1 Introduction

Coronavirus disease 2019 (COVID19), has caused disruption around the world. It was discovered in December 2019, with reports stating that people were suffering from fever and respiratory problems after shopping at a seafood market in Wuhan, Hubei, China. In less than a month, cases of 2019-nCoV infection spread to several regions in Thailand, Japan, Vietnam and Singapore, Hong Kong, Taiwan, Macau. According to the monitoring of the United Nations Educational, Scientific and Cultural Organization (UNESCO), a

© The Author(s) 2023
A. Kusumaningrum and A. Liemanto (Eds.): BICoBL 2022, AEBMR 251, pp. 203–209, 2023.
https://doi.org/10.2991/978-94-6463-214-9_22

total of 39 countries have been affected with a large number of cases of 421,388,462 [1]. All are looking for other ways to keep education going because students are forced to stay at home. One way to teach students remotely is to use online learning. In light of the coronavirus crisis, the role of the cloud computing environment has emerged as an alternative way out. During this pandemic, all of the educational world has taken proactive steps to protect students, lecturers and staff from being infected with the virus, such as working from home and teaching through e-learning (distance learning). Due to these steps, the usage or demand for cloud computing service providers has increased. Facing a series of difficult challenges to provide quality services as a result of the explosive growth of cases due to the coronavirus [2]. The COVID-19 pandemic was an extraordinary and unprecedented event that changed the lives of billions of people around the world, producing what is commonly referred to as the new normal in terms of social norms and the way we live and work. In addition to the tremendous impact on society and business as a whole, the pandemic has created a unique set of cybercrime-related circumstances that also affect society and business. The increasing anxiety caused by the pandemic increases the probability of cyberattacks occurring in accordance with the increase in the number and range of cyberattacks [3]. Technology is changing how people go about their lives. Because of this, digital forensic investigations must also evolve to keep pace with technology [4]. Crimes by taking advantage of current advances. Cloud storage, as form of advances in information technology, allowing the wearer to pass jurisdictional boundaries of each country [5]. Rclone is a platform-independent software that offers a documented command line interface (CLI) to access a variety of cloud storage providers (CSPs) examples are Google Drive, Microsoft OneDrive, or Dropbox [6].

Consequently, it is important for investigators to understand how this tool is configured and what artifacts it leaves on the system. Contribution: We conduct a comprehensive forensic analysis of the rclone application and present artifacts found on the system, in memory, and the network [7].

Rclone as a forensic tool: From a digital forensic investigation perspective, cloud storage poses several jurisdictional and technical challenges. One of these technical challenges is the acquisition of evidence, i.e., accessing and downloading data, as there is only a limited number of forensic tools available (conventional tools have focused upon having physical access to the media that stores the data) [8]. This forces examiners to fall back on applications provided by CSPs or utilize a web interface (if available).

2 Methodology

The method of analysis of legal materials used in this study is qualitative analysis, namely analysis carried out by understanding and compiling legal materials which are collected systematically so as to obtain an overview of the problems studied.

The systematics of writing is presented in the form of a narrative description. The presentation of legal data/materials is more analytical descriptive in nature. Writing in narrative form is expected to be able to convey all normative realities related to the regulation of the confiscation of digital evidence stored in cloud storage.

In accordance with the legal problems that will be studied, the researchers examine the subject matter through a normative legal research approach, a statutory approach and

a case approach. This method emphasizes more on the concept/construct that the law can be viewed as a set of laws and regulations that are systematically arranged based on a certain order. The conceptual framework discusses normative legal theory, secondary data, qualitative analysis, normative juridical evidence, juridical research steps.

The legal materials in question include.

- Primary legal materials, including Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions, and Law Number 8 of 1981 concerning the Book of Law - Law on Criminal Procedure (KUHAP)
- Secondary legal materials, including the Denpasar District Court Decision Number: 638/Pid.Sus/2019/PN Dps dated 19 October 2020, regarding Denpasar District Court Decision
- Tertiary legal materials, namely in the form of criminal law dictionaries, encyclopedias and articles.

Legal data/materials were collected through literature study by searching locations related to Denpasar District Court Decision Number: 638/Pid.Sus/2019/PN Dps dated 19 October 2020, regarding Denpasar District Court Decision. The method of analysis of legal materials used in this research is qualitative analysis, namely the analysis is carried out by understanding and assembling legal materials that are collected systematically in order to obtain an overview of the problems studied. The data analysis was carried out qualitatively through a deductive logical study of thinking.

This study aims to determine what is the position of digital evidence in cases of cybercrime and its factors influence the occurrence of cybercrime.

This research result obtained by the author in the field, there is no proper processing of evidence procedures, digital evidence presented at trial has been explored by expert witnesses before, thus reducing the authenticity of a piece of evidence in itself, even though it is deep Law No. 11 of 2008 on Article 43 paragraph (2) has explained about the implementation investigative procedures in the field of Technology Information and Electronic Transactions. System evidence in cases of cybercrime crime by expanding the evidence in KUHAP has actually been regulated in various ways scattered laws. With such as e-mail, sound, images, access codes, symbols, and various other electronic documents have equal probative power with other evidence set forth in the Criminal Procedure Code and can and can be used as evidence Legitimate.

The writing of this legal research is arranged systematically in chapter by chapter which are interconnected. Divided into 3 (three) chapters, namely: I. Introduction, II. Methodology, III. Discussion Results, IV. Conclusion.

3 Result and Discussion

With cloud computing and cloud storage gaining popularity, the digital forensics community also started to investigate its impact on investigations and what traces can be found. Given the sheer number of publications, this section primarily discusses literature focusing on cloud storage (services) and forensics but ignores secondary literature, e.g., cloud computing in general, distributed storage technologies [9].

Electronic crime is defined as computers or computational devices being used as a tool, target, or storage device in the commission of a criminal offence [10]. Cloud-based evidence is not limited to crime or offending in the cloud environment, with much of law enforcement collection and examination of cloud data relating to data stored in the cloud, as opposed to cloud infrastructure being used as a tool or as a target of offending.

Something that is becoming more and more prolific are requests from investigators and prosecutors for in-depth analysis and specifically, reports around the duplication of key evidence across devices and storage media. These digital cross-pollination analysis requests are time-consuming and even more so when the complexity of cloud stored data is added to the mix. The source of evidential data, oftentimes duplicated across devices, is where an investigation should focus preservation and collection efforts. Discovery and analysis of data located in cloud storage and synchronized across various devices can be crucial to an investigation to tell the complete story and enable facts to be presented to a Court of law to aid decision makers [11].

3.1 Usage of Cloud Storage

Chung et al. [12]. Stresses the importance to not only analyze the client application and its traces but also cookies and log files of web browsers to identify if cloud storage has been accessed. For client applications, traces may be found in general log files or the registry (Windows) [12]. Client application often also comes with a database file (maybe a text file), containing information about (successful) login attempts or synchronized files. Data volume is increasing, which causes issues for digital forensic examiners in collecting and examining data in a timely manner [13]. It is impractical to collect and preserve all data from all devices seized in an investigation due to increasing volumes of data, along with potential collection of comingling data from innocent users, and the business impact on cloud providers [14].

3.2 Arrangements for Searching Electronic Evidence

Searches are regulated in the Criminal Procedure Code, namely in Chapter V part three from Article 32 to Article 37. According to Article 32 of the Criminal Procedure Code, that for the interests of investigators, "investigators can carry out house searches or clothing searches or body searches according to the procedures specified in the law." this law" [15]. Obstacles faced by investigators when electronic evidence in the form of objects is invisible/intangible. And the place where electronic evidence is stored is not in the house, clothes or body. But stored in the cloud storage which is a cloud computing network environment.

Article 184 paragraph (1) reads (1) Legal evidence is [15]:

- Witness statement
- Expert statement
- Letter
- Instruction
- Defendant's statement

In the Constitutional Court Decision No. 20/PUU-XIV/2016, there is a dissenting opinion from Constitutional Justice Suhartoyo who agrees with the expert opinion of

the president (at that time) Dr. Edmon Makarim, S.Kom, SH., LL.M. In this case it is necessary to separate evidence and the method of obtaining it, so that all electronic information and/or electronic documents are valid evidence, while the method of obtaining them is another way. Judge Suhartoyo is of the opinion that the ITE Law has regulated how to obtain electronic information and/or documents.

3.3 Arrangements for Confiscation of Electronic Evidence

Confiscation is regulated in the Criminal Procedure Code, namely in Chapter V, the fourth part of Article 38 to Article 46 of the Criminal Procedure Code and a small part is regulated in Chapter XIV concerning confiscation as stated in Article 1 point 16 of the Criminal Procedure Code, which is a series of investigative actions to take over and or store under the control of movable objects, tangible or intangible for the purposes of evidence in investigations, prosecutions and examinations in court [15].

3.4 Data Privacy and Use of Cloud Computing

Regarding some potential problems that can arise due to misuse of privacy data management, it is very necessary to regulate what is called privacy by design. Privacy by design is an arrangement for managing privacy data through a privacy policy or privacy policy. The privacy policy must provide all the information needed by the customer regarding how the cloud computing service provider will manage the customer's personal data so that the customer knows how far the security and privacy of their personal data will be maintained, including to what extent their personal data will be used for secondary uses. Usually will be traded and distributed to other companies. Customers in this case must really understand the risks of using cloud computing services by reading and understanding carefully the terms and conditions provided by the cloud computing service provider before placing very important information and if the customer is unsure regarding the privacy security of his personal data, then you should choose another company that you feel will provide better protection. Furthermore, consumers must determine and classify which data will be stored in cloud storage services because it involves the confidentiality of very sensitive personal (company) data, for example. Then, the thing that needs to be considered and studied further is whether the cloud storage provider company has a policy that is willing to delete (take down) the proceeds of crime data stored in its cloud storage.

3.5 Jurisdiction Under the Protection Principle

Based on the principle of protection jurisdiction, a country can exercise its jurisdiction over foreign nationals who do crimes abroad that are suspected of threatening security interests, integrity and national independence. The application of this principle is justified as basis for the exercise of a state's jurisdiction. The background to this justification is national legislation in general does not regulate or not punish acts committed within a country that can threaten or interfere with the security, integrity and independence of others. For example, plotting to overthrow his government, smuggling eyes foreign money, espionage activities, or acts that violate laws his immigration.

4 Conclusions and Suggestions

Legislation should encompass the collection of data available to a device at the point of execution of the warrant and subsequent to warrant execution, as oftentimes the use of cloud storage is identified during post-warrant analysis. This is commonplace when a forensic examiner is subsequently analyzing a device extract or computer image and discovers remnants of cloud storage use, such as those outlined in the related work papers. The ability to identify and collect potentially relevant cloud-stored data post-warrant in a forensically sound manner can be crucial to an effective investigation, either confirming known evidence, providing further evidence of offending, or exonerating a suspect and allowing an investigation to move forward and closer to the complete truth. The arrangement for the confiscation of electronic evidence in the form of private data stored in cloud storage that is most appropriate to be implemented in Indonesia is through a combination of legal approaches and non-legal/ business approaches in the form of business and legal collaboration towards sustainable development after the pandemic. There needs to be a revision that explains the position of electronic evidence in the Criminal Procedure Code, so that it can provide more legal certainty for justice-seekers.

Acknowledgment. I am pleased to submit an original manuscript entitled "Confiscation of Electronic Evidence Cyber Crime in Business and Law Collaboration after Pandemic Achieving Sustainable Legal Development" to be considered for publication in Journal of Atlantis Press Journals. We believed this manuscript is appropriate for publication by the Journal of Atlantis Press Journals. This manuscript has not been published and has not been followed by publication elsewhere.

References

1. Education: from school closure to recovery, https://en.unesco.org/covid19/educationresponse, last accessed 2023/01/21.
2. Al Ashhab, Z.R., Anbar, M., Singh, M.M., Alieyan, K., Ghazaleh, W.A.: Detection of HTTP flooding DDoS attack using Hadoop with MapReduce: a survey. Int. J. Adv. Trends Comput. Sci. Eng, 8(1), 71–77 (2019).
3. Lallie, H.S., Shepherd, L.A., Nurse, J.R., Erola, A., Epiphaniou, G., Maple, C., Bellekens, X.: Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Computers & Security, 105, 102248 (2021).
4. Findlay, B.: A review of thumbnail images artefacts in the Linux desktop and a methodology to add provenance to deleted files, using the thumbnail images artefact in combination with recent files history, and Trash artefacts. Forensic Science International: Digital Investigation, 44, 301498 (2023).
5. Findlay, B.: Digital policing. In Introduction to Professional Policing (pp. 193–212). Routledge, London (2020).
6. Breitinger, F., Zhang, X., Quick, D.: A forensic analysis of rclone and rclone's prospects for digital forensic investigations of cloud storage. Forensic Science International: Digital Investigation, 43, 301443 (2022).
7. Detecting rclone e an effective tool for exfiltration, https://research.nccgroup.com/2021/05/27/detecting-rclone-an-effective-tool-for-exfiltration/, last accessed 2023/04/02.
8. Quick, D., Martini, B., Choo, R.: Cloud storage forensics. Syngress, United States (2013).

9. Ricci, J., Baggili, I., Breitinger, F.: Blockchain-based distributed cloud storage digital forensics: Where's the beef?. IEEE Security & Privacy, 17(1), 34-42 (2019).
10. Electronic Crime Strategy of the Police Commissioners' Conference Electronic Crime Steering Committee, http://www.police.govt.nz/resources/2001/e-crime-strategy/e-crime-strategy.pdf, last accessed 2023/04/02.
11. Digital pollination: user impact on the document life cycle, https://thesedonaconference.org/sites/default/files/conference_papers/%5B8.2%5D%20S.%20Stawski_Digital%20Pollination%20Paper_Oct%202018.pdf, last accessed 2023/04/02.
12. Chung, H., Park, J., Lee, S., Kang, C.: Digital forensic investigation of cloud storage services. Digital investigation, 9(2), 81-95 (2012).
13. Quick, D., Choo, K.K.R.: Impacts of increasing volume of digital forensic data: A survey and future research challenges. Digital Investigation, 11(4), 273-294 (2014).
14. Almulla, S., Iraqi, Y., Jones, A.: A state-of-the-art review of cloud forensics. Journal of Digital Forensics, Security and Law, 9(4), 2 (2014).
15. Law Number 8 of 1981 concerning the Book of Law - Law on Criminal Procedure (KUHAP) (1981).

Open Access This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (http://creativecommons.org/licenses/by-nc/4.0/), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.