LEGAL BRIEF
ISSN 2722-4643 (Online) | 1979-522X (Print)
Volume 13, No. 3, 2024, pp. 960-968
Published by: IHSA Institute (Natural Resources Law Institute)

Evidence of social media accounts in the investigation process

Budi Santoso

Faculty of Communication and Informatics, University Muhammadiyah Surakarta

Abstract: This study aims to determine the position of electronic evidence in the form of social media accounts in the investigation process and parameters in determining an electronic information/document in the form of social media accounts as evidence in the investigation process. This study uses an empirical legal method with a descriptive approach, utilizing primary and secondary data. The data was collected through observation, document study, and interviews. Furthermore, data analysis is carried out qualitatively. The results of the study show that electronic evidence such as social media accounts has an important role in the investigation of cyber crimes, but it is only considered as valid preliminary evidence if it has gone through official confiscation and digital forensic examination in accordance with the ITE Law. To be accepted in court, electronic evidence must meet formal requirements, namely relevance and validity, as well as material requirements, namely authenticity without modification. Verification through digital forensics is needed to maintain the integrity of evidence, so that electronic evidence is treated as equal to physical evidence in law enforcement.

Keywords: Evidence, Social Media, Investigation.

1. Introduction

Along with the development of information and communication technology, social media has become an inseparable part of modern people's lives. Social media such as Facebook, Instagram, Twitter, and WhatsApp are not only used to interact personally, but also often become a platform to disseminate information, even used in illegal activities (Yunita, 2023), (Ummah, 2020). In its development, not a few people have stumbled upon legal cases due to the impact of the use of technology itself. Starting from fraud to defamation that often occurs (Sanjaya, Hartono, & Ardhya, 2022). Later, in the process of proof, information technology evidence has been used, namely in the form of electronic evidence. As in the proof that occurred in the case of the crime of disseminating pornographic content using social media applications, namely by uploading pornographic images in one of the Facebook accounts and to be disseminated (Kurniawan, 2020).

One of the criminal acts that often occur in the community by utilizing or abusing information technology is hate speech through social media (Sepima, Siregar, & Siregar, 2020). Like the case that occurred in Singaraja involving a housewife who was charged with insulting a lawyer through a tweet commenting on the status of *Facebook*, then there was also a case involving a Tamblang village chief who was charged with insulting a Jro Mangku with accusations through tweets on the status of *Facebook*. In this case, the defendant can be charged with multiple articles, namely article 311 of the Criminal Code which is hereinafter referred to as the Criminal Code and/or article 310 of the Criminal Code, as well as article 27 paragraph (3) of Law Number 19 of 2016 concerning amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions which is hereinafter referred to as the ITE Law (Supiyati, 2020), (Anton & Moho, 2023).

Data from the Sukoharjo Police Investigation and Crime Unit shows that the number of cases of defamation through social media in the jurisdiction of the Sukoharjo Police from 2019 to 2021 has fluctuated. In 2019, there was 1 case, which increased to 3 cases in 2020, and then decreased to 2 cases in 2021. A spike in cases in 2020 may indicate

Correspondence:
Name: *Budi Santoso*
Email: *bs143@ums.ac.id*

Received: Aug 30, 2024;
Revised: Sep 09 2024;
Accepted: Sep 23, 2024;
Published : Oct 30, 2024;

an increase in incidence or reporting, while a decline in 2021 may indicate a decrease in cases or a change in case handling. This data, taken from the Sukoharjo Police Investigation and Crime Unit, illustrates the dynamics and trends of defamation through social media in the region

The development of technology that affects the emergence of cyber crimes inevitably has an impact on the legal order that applies in Indonesia (Hapsari & Pambayun, 2023). Evidence is an important thing in the evidentiary process, but Article 184 paragraph (1) of the Criminal Procedure Code is very limited, the problem that occurs is if the evidentiary process requires electronic evidence but is not regulated in Article 184 paragraph (1) of the Criminal Procedure Code (Isima, 2022), (Army, 2020). Article 184 of Law Number 8 of 1981 concerning the Criminal Procedure Law stipulates that valid evidence consists of: a. Witness statements; b. Expert testimony; c. Letter; d. Instructions; e. Defendant's statement. Referring to this article, if you look at the evidence that can be used in the evidentiary process, it is very narrow and limited, so that evidence outside the Criminal Code has emerged that cannot be used and has not received clear legality. This dilemma finally became the beginning to provide legal certainty by giving birth to a special law to contain valid evidence outside the Criminal Code.

One of the solutions to this problem is the formation of Law Number 19 of 2016 amending Law Number 11 of 2008 concerning Information and Electronic Transactions which contains electronic evidence, namely in Article 1 paragraphs (1) and (4) and Article 5 paragraphs (1) and (2). The limited evidence as regulated in the Criminal Code is not able to accommodate the development of reality in society (Hartono and Yuliartini, 2020:283). Security, comfort, and legal certainty in the use of information, media, and communication technology must be considered so that it develops optimally and does not abuse occur. However, the presence of this Law has not been able to solve all electronic crimes, so it still gives rise to various interpretations of electronic evidence by law enforcement officials, ranging from investigations to courts (Nuarta & Santhi, 2024).

In the criminal justice system, the police are the first institution to handle all criminal acts by conducting investigations, so it can be said that the success of law enforcement against defamation crimes through social media. The Police have a very important role in finding and collecting evidence, which with this evidence can shed light on a criminal act.

Regulations related to digital evidence in Indonesia, such as those regulated in the Electronic Information and Transaction Law (UU ITE), need to be continuously reviewed and updated to be able to accommodate the complexity of cases involving digital technology. Therefore, the researcher is interested in conducting research on the relevant "Social Media Account Evidence in the Investigation Process" to provide an in-depth understanding of how evidence from social media can play a role in the legal process, as well as what are the challenges faced in optimizing the evidence as a basis for achieving justice.

2. Materials and Methods

The type of research used in this study is the type of empirical law research. Definitively, it is legal research that uses the study of the application of normative law in the case of certain legal events that exist in people's lives (Permana, Arjaya, & Karma, 2021). Empirical legal research is a type of legal research that analyzes and examines the work of law in society (Benuf & Azhar, 2020).

The nature of the research used is descriptive and uses data and data sources, namely primary data and secondary data, namely primary legal materials, secondary legal materials, and tertiary legal materials, namely the Great Dictionary of Indonesian Language (Muhaimin, 2020). The researcher used three types of data collection, namely documentation study techniques, observation or observation techniques, and interview techniques. The technique of determining the research sample uses the *Non Probability Sampling* and the form is *purposive sampling.* The data obtained for this study were analyzed and processed qualitatively which drew conclusions based on logical thinking from the

results of interviews conducted by the researcher with informants and data obtained from document studies.

3. Results and Discussion

3.1. The Position of Electronic Evidence in the Form of Social Media Accounts in the Investigation Process

Unlawful acts in the ITE Law or crimes in information technology are called cybercrimes (cybercrime), which is a type of crime related to the use of information and communication technology without limits, and has strong characteristics with a technological engineering that relies on a high level of security of information conveyed and accessed by internet users (Syaefudin, Sudewo, & Rizkianto, 2021). In the examination of the crime of defamation through social media, evidence is needed for the filing process and to support the judge's judgment in sentencing the defendant who commits the crime of defamation through social media.

Based on research conducted at the Sukoharjo Resort Police, there is 1 (one) case of social media insult that occurred in Sukoharjo Regency, where the law enforcement procedure is to take action through Restorative Justice. Then there are 5 (five) cases where the law enforcement procedure is to take penal action (criminal) before restorative justice law enforcement efforts are carried out first, but among the plaintiffs in this case there are still those who still make decisions so that the case is resolved penally (criminal) so that the Investigator of the Investigation Unit II of the Criminal Investigation Unit of the Sukoharjo Police continued the legal process of the case in accordance with the provisions of the applicable laws and regulations

In line with the results of the research at the Sukoharjo Resort Police, according to Ketut Darbawa in his interview explained that in the process of examining and confiscating social media accounts by investigators, in this case the confiscation was not carried out carelessly, it must be preceded by a permit from the chairman of the local district court.

Proof is a decisive stage in the case process, because from the results of the evidence, it can be known whether or not an indictment or demand is true or not by pointing to evidence. So that in the investigation process, the investigating police must be observant in finding and collecting existing evidence so that they can shed light on a criminal act.

As is known in the Theory of Evidentiary Law, Eddy O.S. Hiariej explained that in order for an evidence to be used as evidence in court, several conditions are needed, including the following: 1) It is allowed by law to be used as evidence. 2) Reability, that is, the evidence can be trusted for its validity (for example, it is not fake or has not been altered). 3) Necessity, that is, the evidence is indeed needed to prove a fact. 4) Relevance, that is, the evidence has relevance to the necessary facts (Salsabila, Firganefi, & Riski, 2024).

Evidence is everything that has to do with an act where with these evidence, can shed light on a criminal act. Evidence is one of the variables in the evidentiary system, so in the collection of evidence the investigator must refer to the evidence according to the Criminal Procedure Code, namely in Article 184 paragraph (1) of the Criminal Procedure Code explains that the valid evidence is: 1) Witness Statement, 2) Expert Testimony, 3) Letter, 4) Instructions, and 5) Defendant's Statement (Handrawan, Lade Sirjon, Iksan, & Sulihin, 2023).

In dealing with the problem of cybercrime, this problem of proof plays an important role, this needs to be noted because electronic evidence has become a new intermediary medium for the implementation of a crime (Lestari & Damayanti, 2018). Article 184 paragraph (1) of the Criminal Procedure Code has determined "limitatively" valid evidence according to the law, but this limitation makes it difficult for law enforcement officials to disclose the material truth of cyber crimes (cybercrime).

Then the regulation regarding evidence in cybercrime can be seen in the provisions of Law Number 19 of 2016 on the Amendment of Law Number 11 of 2008 concerning Information and Electronic Transactions. The birth of the ITE Law is a little progress in responding to and tackling the current cybercrime, especially in the law enforcement process or the litigation process. In Article 1 paragraph (1) of the ITE Law, it is stated that Electronic Information is one or a set of electronic data, including but not limited to writing, sounds, images, maps, designs, photographs, electronic data interchange (EDI), electronic mail, telegram, telex, telecopy, or the like, letters, signs, numbers, access codes, symbols, or perforations that have a meaning or meaning or can be understood by people who are able to understand them.

Meanwhile, regarding Electronic Documents as mentioned in Article 1 paragraph (4) of the ITE Law, is any Electronic Information created, transmitted, transmitted, received, or stored in analog, digital, electromagnetic, optical, or similar form, which can be seen, displayed, and/or heard through a computer or a system may be seen, displayed, and/or heard through a computer or electronic system, including but not limited to writing, sounds, images, maps, designs, photographs or the like, letters, signs, numbers, access codes, symbols or perforations that have meaning or meaning or can be understood by a person capable of understanding them.

In the investigation of cybercrime (cybercrime) There are 3 phases used by investigators, namely, first, the witness is told to tell all the information he sees and other information related to the crime. Then second, the police are looking for suspects from potential suspects. Finally, the third one, the Police asked witnesses to identify the perpetrators of a number of potential suspects owned by the police directly by showing the potential suspects (Sanjaya et al., 2022).

The Criminal Procedure Code does not explicitly mention the definition of evidence, but in the doctrine of criminal procedure law, it can be understood that what is meant by evidence is objects that can be subject to confiscation. This is regulated in Article 39 paragraph (1) of the Criminal Procedure Code, which states that the evidence is as follows: 1) Objects or bills of the suspect or defendant that are wholly or partially suspected to have been obtained from a criminal act or as a result of a criminal act or an object that has been used directly to commit a criminal act or to prepare for it; 2) Objects used to obstruct the investigation of criminal acts; 3) Objects that are specifically made and intended to commit criminal acts; 4) Other objects that have a direct connection with the criminal act committed (Basrawi, 2023).

In the process of proving at trial, although it is not explicitly referred to as valid evidence, evidence has a very important position. This can be seen in Article 181 paragraph (1) of the Criminal Procedure Code which regulates the obligation of the presiding judge to show all evidence to the defendant and ask whether the defendant knows the evidence or not. From this, it can be seen that this shows that the position of evidence has an important function in the evidentiary system in the trial.

Based on the results of research in the field, precisely at the Sukoharjo Resort Police, according to Ketut Darbawa, of the 5 cases that have been handled by the Unit II Functional Unit of the Sukoharjo Police Criminal Investigation Unit, the position of prints or printouts (screenshots) with social media accounts is not the same, prints or printouts (screenshots) The post in the account is only preliminary evidence, to find out the truth value of the post or upload, of course, you must first confiscate and check the perpetrator's social media account. The use of social media accounts as electronic evidence will certainly make it easier for nvestigators to find the original data (server data). Then in his interview Ketut Darbawa added that social media accounts as electronic evidence can be said to be valid in the investigation process, especially in the case of criminal defamation, if the social media account has been examined and confiscated first by investigators, in this case the confiscation is not carried out carelessly, must be preceded by a permit from the chairman of the local district court.

Gede Sedana in his interview added that in order for Electronic Information and Electronic Documents in the form of social media accounts to be used as valid electronic evidence at trials, especially in the act of defamation through social media, posts on social media accounts must be open or known in general in order to fulfill the elements of Article 310 of the Criminal Code and in the Joint Decree of the Minister of Communication and Information of the Republic of Indonesia, Attorney General of the Republic of Indonesia, and Chief of the National Police of the Republic of Indonesia Number 229 of 2021, Number 154 of 2021, Number KB/2/VI/2021. Thus, in essence, in the results of the research conducted at the Sukoharjo Resort Police or more precisely in the Unit II Functional Unit of the Criminal Investigation Unit of the Sukoharjo Police through Ketut Darbawa and Gede Sedana, it is stated that social media accounts can be said to be valid as evidence if they meet the elements of the crime of defamation and have been confiscated through appropriate procedures.

This is in line with what is stated in Article 1 number 1 of Law Number 11 of 2008 concerning Electronic Information and Transactions, that social media accounts are a form of Electronic Information. So it can be concluded that social media accounts can be used as electronic evidence in accordance with Article 5 paragraphs (1) and (2) of Law Number 19 of 2016 concerning amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions, namely Electronic Information and/or Electronic Documents and/or their printouts are an extension of valid Evidence in accordance with the applicable Procedural Law in Indonesia.

3.2 Parameters in the Determination of an Electronic Information/Document in the Form of a Social Media Account as Evidence in the Investigation Process

The requirements and determination of electronic evidence must meet the requirements both formally and materially as evidence that will be declared valid and used in the trial as well as the evidence regulated in the Criminal Code (Sanjaya et al., 2022). These provisions and requirements are used to ensure legal certainty and function as a benchmark in determining the validity of evidence so as to give rise to the judge's confidence in the legal facts presented through electronic evidence. So that in this case, the investigator who is in charge of finding and collecting evidence, must be able to determine which evidence is valid to be used as evidence in the trial and can only be used as evidence (supporting evidence).

Electronic evidence has a wide scope and diverse types, such as *email, websites, short message service (SMS),* videos, digital photos, including printouts of Information or other Electronic Documents (Wijaya, Muaja, & Prayogo, 2023). Each type of electronic evidence has technical characteristics and requires its own handling in determining its legal validity. Therefore, there needs to be an understanding among law enforcement officials, in this case investigators regarding the collection, analysis, and presentation of various electronic evidence. In the necessary right, more specific regulations and decisions can be applied that are used as guidelines in examining electronic evidence at the investigation level.

The regulation or benchmark can be through the formation of regulations under the law, legal interpretation (*wet interpretatie*) and legal discovery (*rechtsvinding*) by the judge (Sanjaya et al., 2022). The regulation in question can also be in the form of joint regulations between law enforcement agencies that are used as guidelines both at the central and regional levels throughout Indonesia. This is in line with the results of research that has been carried out at the Sukoharjo Resort Police.

The results of the study show that the Investigator of Unit II of the Sukoharjo Resort Police Criminal Investigation Unit, used the Joint Decree of the Minister of Communication and Information of the Republic of Indonesia, the Attorney General of the Republic of Indonesia, and the Chief of the National Police of the Republic of Indonesia Number 229 of 2021, Number 154 of 2021, Number KB/2/VI/2021 as a benchmark in determining *cybercrime (cybercrime*) especially the crime of defamation through social media as a ref-

erence in carrying out his duties and authorities. Especially in the investigation, Gede Sedana as the Investigator of Unit II of the Sukoharjo Police Criminal Investigation Unit explained that in the joint decree, in essence, social media accounts that contain posts that are derogatory, degrading, and defamatory, must meet the criteria of "publicly known" to the general public or the public itself is interpreted as a collection of people who mostly do not know each other. The criteria for "publicly known" can be posts on social media accounts with publicly accessible settings.

As mentioned earlier, one of the requirements for electronic evidence can be accepted in court with the fulfillment of formal and material requirements. This also applies in the investigation process, in this case with the fulfillment of the formal and material requirements, electronic evidence in the form of originals and printed results has the same value (Ariana, 2022). Thus, to ensure the fulfillment of the requirements in question, a scientific method that supports special technology is needed to examine electronic evidence.

The method of proof of electronic evidence requires the role of digital forensics which is briefly applied to collect, process, and present electronic evidence for the benefit of law enforcement. Given the breadth of digital forensics in investigations, this section is only limited to the principles in digital forensics.

The formal requirements regarding electronic evidence, especially social media accounts, are regulated in Article 5 paragraph (4) and Article 43 of Law Number 19 of 2016 which states that: 1) The information or Electronic Document is not a letter according to the law must be made in written form, and the letter and its documents which according to the law must be made in the form of a notary deed or a deed made by the deed making official; 2) The search or seizure of the electronic system must be carried out with the permission of the chairman of the local district court; 3) The search or seizure of electronic systems must maintain the interests of public services (Dewantara & Suartha, 2022).

This is in line with the results of research that has been carried out at the Sukoharjo Resort Police. The results of the study show that according to Gede Sedana, the investigator will forcibly take over or known as *taking down* the account in this case related to the crime of defamation if an examination has been carried out on the original data (*server data*), after which the data obtained by the investigator must not result in changes or damage to the data so that it can be accepted in court. Ketut Darbawa in his interview added that social media accounts as electronic evidence can be said to be valid in the investigation process if the social media account has been examined and confiscated first by investigators, in this case the confiscation is not carried out carelessly, must be preceded by a permit from the chairman of the local district court.

The material requirements for electronic evidence are regulated in Article 5 paragraph (3) of the ITE Law, namely information or electronic documents are declared valid if they use the Electronic System in accordance with the provisions stipulated in the ITE Law. Furthermore, it is regulated in Article 15 and Article 16 of the ITE Law which can obtain more detailed requirements, namely that the Electronic System must: (1) Be reliable, safe, and responsible for the operation of the Electronic System. Reliable means that the Electronic System has the ability to suit the needs of its use. Safe means that the system protects both physically and non-physically. While being responsible for the operation of the Electronic System means that the Electronic System has the ability in accordance with its specifications. (2) Able to display the Information or Electronic Documents in their entirety. (3) It can protect the availability, integrity, authenticity, confidentiality and accessibility of Electronic Information. (4) Equipped with procedures or instructions and able to operate in accordance with the procedures or instructions that have been set.

In addition, Article 6 of the ITE Law also provides material requirements regarding the validity of electronic evidence, namely that Information or Electronic Documents are considered valid as long as the information contained in them can be accessed, displayed, guaranteed to be intact, and can be accounted for so as to explain a situation.

This is in line with the results of research that has been carried out at the Sukoharjo Resort Police. The results of the study show that according to Ketut Darbawa to determine the parameters of an information or electronic document in the form of confiscation of the account is carried out so that the social media account can be accessed, which is meant by "accessed" is that the social media account can only be accessed by someone who has the competence to do so, which means that not all investigators can access the account and must be able to provide an explanation of its relevance his actions on the data and the consequences of his actions, then the authenticity is guaranteed in this case which is meant by "authenticity", namely the data is in accordance with the original data (server data) or in other words in accordance with the original data without the slightest alteration, so that the account can be displayed in front of the court.

In the event that the Electronic System used has met these requirements, the quality of electronic evidence in its original form (Electronic Information or Electronic Documents) and printed results of Information or Electronic Documents are the same (Efendi, 2024). In other words, the investigating police can use both or one of them. However, it should be remembered that in certain cases there are times when the use of electronic evidence is more appropriate than the use of printed results of the Information or Electronic Documents because the Information or Electronic Documents may provide information that cannot be provided if the Information or Electronic Documents are printed. As with the robbery case recorded by CCTV (*Closed Circuit Television*), then electronic documents recorded by CCTV should be presented in their original form.

This is in line with the results of research conducted at the Sukoharjo Resort Police. According to Ketut Darbawa, in the case of criminal defamation through social media, the printed results (*screenshots*) are only preliminary evidence, to find out the truth value of the post or upload, of course, it is necessary to confiscate and check the perpetrator's social media account first. The use of social media accounts as electronic evidence will certainly make it easier for investigators to find the original data (server data).

Thus, in order for an electronic evidence to be used as evidence in the investigation process or in a trial, it must meet the formal requirements and material requirements as explained above, namely the formal requirements are regulated in Article 5 paragraph (4) of the ITE Law, namely that Information or Electronic Documents are not documents or letters that according to the law must be in written form. Meanwhile, the material requirements are regulated in Article 6, Article 15, Article 16 of the ITE Law, which in essence Information or Electronic Documents must be guaranteed, their authenticity, integrity, and availability.

Based on the results of the research and analysis described above, the researcher concludes that the parameters or benchmarks for social media accounts (electronic evidence) to be used as valid evidence in investigations are as follows: (1) Admissible, i.e. the data must be able to be accepted and used for the sake of the law ranging from the interests of the investigation to the interests of the examination in court; (2) Original or Authentic, i.e. the electronic evidence must be related to the incident/criminal act that occurred and not fabricated. So if the social media account can be trusted, then the verification process will be easier; (3) Complete, that is, the social media account must be said to be complete if there is a lot of electronic information or electronic documents and instructions that can help the needs of the examination.

4. Conclusions

Electronic evidence such as social media accounts has an important position in the investigation process of cyber crimes, including defamation. However, evidence in the form of social media accounts, such as screenshots, is only considered preliminary evidence. In order to be legally used in court, the evidence must go through an official seizure process with court permission and digital forensic examination. Based on the rules stipulated in the ITE Law, new electronic evidence can be accepted if it meets certain legal requirements.

To be accepted as evidence, information or electronic documents in the form of social media accounts must meet two main parameters: formal requirements and material requirements. Formal requirements ensure that the evidence is relevant and valid, while material requirements ensure that the evidence is original and unmodified. The authenticity of the data must be verified through digital forensics, which plays an important role in maintaining the integrity of the evidence. This process ensures that electronic evidence is treated as important as physical evidence in law enforcement.

The suggestions that can be given are as follows: (1) The Police need to immediately build a digital forensic laboratory along with sufficient knowledge and tools to meet the needs in the process of investigating and investigating cyber crimes, especially in determining and collecting electronic evidence. It is even hoped that a division will be formed immediately that specifically fights cybercrime; (2) The public is expected to always be able to use and utilize social media wisely and intelligently in order to avoid a legal problem. In addition, the public is also expected not to be afraid of being asked for information as witnesses by law enforcement officials, this is because there are provisions of laws and regulations that provide protection to witnesses; (3) The government that has the authority to make laws and regulations is expected to make clear regulations and specifically regulate electronic evidence, in terms of handling and collecting electronic evidence and the position of electronic evidence itself. In the Law on Cybercrime Countermeasures, criminal law has limitations, in order to be effective, it needs to be consistent with the norms that are lived and obeyed by users, such as netizens. And the most important thing is that it is hoped that the government will immediately include Cyber Crime in the Criminal Code in order to fill the legal vacuum/legal loophole that has been an obstacle, so that a new interpretation of the Criminal Code norms is needed to be adjusted to the current context

References

Anton, R. Y., & Moho, A. (2023). PERTANGGUNGJAWABAN PIDANA TERHADAP PELAKU TINDAK PIDANA PENCEMARAN NAMA BAIK DAN PENGHINAAN TERHADAP PEJABAT NEGARA MELALUI MEDIA SOSIAL. *IUS FACTI: Jurnal Berkala Fakultas Hukum Universitas Bung Karno*, *1*(2 Desember), 180–196.

Ariana, I. N. (2022). Tinjauan Yuridis Terhadap Kedudukan Alat Bukti Elektronik Berdasarkan Putusan MK Nomor 20/PUU-XIV/2016. *UNES Law Review*, *5*(1), 1–19. https://doi.org/10.31933/unesrev.v5i1.277

Army, E. (2020). *Bukti Elektronik Dalam Praktik Peradilan*. Sinar Grafika.

Basrawi. (2023). Tinjauan Yuridis Eksekusi Barang Sitaan Berstatus Sewa Menyewa Perkara Tindak Pidana pada Putusan Pengadilan yang Telah Inkracht Menurut Sistem Peradilan Pidana di Indonesia. *Jurnal Kewarganegaraan*, *7*(1), 540–547. https://doi.org/10.31316/jk.v7i1.4840

Benuf, K., & Azhar, M. (2020). Metodologi penelitian hukum sebagai instrumen mengurai permasalahan hukum kontemporer. Gema Keadilan, 7 (1), 20–33.

Dewantara, D. M. D., & Suartha, I. D. M. (2022). Legalitas Alat Bukti Elektronik Sebagai Alat Bukti Dalam Hukum Acara Pidana. *Kertha Desa*, *10*(8), 660–669.

Efendi, M. R. (2024). Pemeriksaan Alat Bukti Elektronik Dalam Persidangan Peradilan Perdata Melalui E-Court. *Jurnal Hukum Bisnis*, *8*(3), 1389–1402. https://doi.org/10.33121/hukumbisnis.v8i3.2821

Handrawan, Lade Sirjon, Iksan, & Sulihin, L. O. M. (2023). Penerapan Alat Bukti Petunjuk di Tingkat Penyidikan dalam Penetapan Tersangka Pada Tindak Pidana Kekerasan Seksual. *Lakidende Law Review*, *2*(2), 432–441. https://doi.org/10.47353/delarev.v2i2.51

Hapsari, R. D., & Pambayun, K. G. (2023). Ancaman Cybercrime di Indonesia: Sebuah Tinjauan Pustaka Sistematis. *Jurnal Konstituen*, *5*(1), 1–17. https://doi.org/10.33701/jk.v5i1.3208

Isima, N. (2022). Kedudukan alat bukti elektronik dalam pembuktian perkara pidana. *Gorontalo Law Review*, *5*(1), 179–189.

Kurniawan, D. W. (2020). Kekuatan Pembuktian Cetakan Media Sosial dalam Menyebarluaskan Konten Pornografi Sebagai Tindak

Pidana di Bidang Informasi dan Transaksi Elektronik. *Verstek*, *8*(1), 71–79. https://doi.org/10.20961/jv.v8i1.39612

Lestari, A. D., & Damayanti, M. (2018). Cakupan Alat Bukti Sebagai Upaya Pemberantasan Kejahatan Siber. *Al-Ahkam Jurnal Ilmu Syari'ah Dan Hukum*, *3*(1), 47–68. https://doi.org/10.22515/al-ahkam.v3i1.1341

Muhaimin. (2020). *Metode Penelitian Hukum*. Mataram: Mataram University Press.

Nuarta, I. N., & Santhi, N. N. P. P. (2024). Pengaturan Persidangan Pidana Secara Elektronik dalam Perspektif Peradilan Modern. *Kertha Wicaksana*, *18*(1), 37–45. https://doi.org/10.22225/kw.18.1.2024.37-45

Permana, I. P. A., Arjaya, I. M., & Karma, N. M. S. (2021). Peranan Alat Bukti Elektronik dalam Tindak Pidana Pencemaran Nama Baik. *Jurnal Interpretasi Hukum*, *2*(2), 422–428. https://doi.org/10.22225/juinhum.2.2.3452.422-428

Salsabila, L. A., Firganefi, & Riski, S. (2024). Faktor-Faktor Yang Menempatkan Media Sosial Sebagai Alat Bukti Elektronik Pada Tindak Pidana Penganiayaan. *Syariah: Jurnal Ilmu Hukum*, *1*(4), 110–118. https://doi.org/10.62017/syariah.v1i4.1499

Sanjaya, A. A., Hartono, M. S., & Ardhya, S. N. (2022). Penggunaan Akun Media Sosial Sebagai Alat Bukti Elektronik dalam Proses Penyidikan. *Jurnal Komunitas Yustisia*, *5*(2), 482–499. https://doi.org/10.23887/jatayu.v5i2.51665

Sepima, A., Siregar, G. T. P., & Siregar, S. A. (2020). Penegakan Hukum Ujaran Kebencian di Republik Indonesia. *Jurnal Retentum*, *2*(2), 108–116. https://doi.org/10.46930/retentum.v2i2.908

Supiyati, S. (2020). Penerapan Pasal 27 Ayat 3 Undang-undang No 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik Terhadap Tindak Pidana Pencemaran NAMA Baik Melalui Internet Sebagai Cybercrime Di Hubungkan Dengan Kebebasan Berekspresi. *Pamulang Law Review*, *2*(1), 23–36.

Syaefudin, M. A. F., Sudewo, F. A., & Rizkianto, K. (2021). *Hukum Siber (Perbandingan Indonesia dan Malaysia)*. Pekalongan: PT. Nasya Expanding Management.

Ummah, A. H. (2020). Dakwah digital dan generasi milenial (menelisik strategi dakwah komunitas arus informasi santri nusantara). *Tasâmuh*, *18*(1), 54–78.

Wijaya, M. F., Muaja, H. S. M., & Prayogo, P. (2023). Kedudukan Dan Status Dokumen Elektronik Menurut Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik. *Lex Privatum*, *12*(3), 1–11.

Yunita, F. (2023). Aspek Hukum Penggunaan Media Sosial Berbasis Internet. *Jurnal Notarius*, *2*(1).