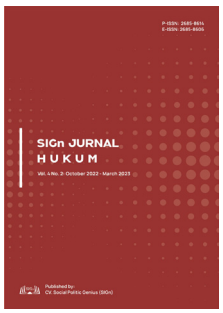

SIGn Jurnal Hukum

E-ISSN: 2685 – 8606 || P-ISSN: 2685 – 8614

https://jurnal.penerbitsign.com/index.php/sjh/article/view/v4n2-12

Volume 4 Issue 2: October 2022 – March 2023 Published Online: March 2, 2023

Article

Social Media in the Process of Evidence of Electronic Information and Transaction Crimes

Media Sosial dalam Proses Pembuktian Tindak Pidana Informasi dan Transaksi Elektronik

Rionov Oktana*
Universitas Hasanuddin || r_oktana@yahoo.com
**Corresponding Author*

Syukri Akub
Universitas Hasanuddin || syukri.akub@gmail.com

Maskun Maskun
Universitas Hasanuddin || maskun@unhas.ac.id

How to cite:

Oktana, R., Akub, S., & Maskun, M. (2023). Social Media in the Process of Evidence of Electronic Information and Transaction Crimes. *SIGn Jurnal Hukum, 4*(2), 320-331. https://doi.org/10.37276/sjh.v4i2.252

ABSTRACT

This study aims to examine and analyze social media accounts' status and seizure procedures in the evidentiary process of cybercrime. This study uses normative legal research with a statute and case approach. The collection of legal materials is carried out using a literature study technique. The collected legal material is then qualitatively analyzed to describe the problem and answer study purposes. The results show that the status of social media as legal means of proof in the evidentiary process at trial is regulated in Law No. 11 of 2008 and Law no. 8 of 1981. Electronic evidence can be categorized as proof of indication by fulfilling the formal and material requirements regulated in Law No. 11 of 2008. Meanwhile, seizure procedures of social media accounts in the evidentiary process of cybercrime are preceded by searching mobile phone communication to obtain device specifications. Social media accounts, files, documents, and applications used by cybercrime perpetrators will be found in these specifications. Seizure of social media accounts is regulated in Article 43 section (3) of Law No. 19 of 2016, while the procedure is carried out based on Law No. 8 of 1981. Therefore, it is recommended that the government and law enforcement agencies issue implementing regulations regarding seizing social media accounts as legal means of proof in the evidentiary process of electronic information and transaction crimes. In addition, collaboration between the Ministry of Communications and Informatics and social media platforms is needed to handle more accessible and more efficient cases, mainly regarding seizures of social media accounts used by cybercrime perpetrators. On the other hand, it is necessary to expand the meaning of proof of indication as regulated in Law No. 8 of 1981 in order to be able to emphasize social media proof as a legal means of proof.

Keyword: *Cybercrime; Evidentiary; Proof; Social Media.*

ABSTRAK

Penelitian ini bertujuan untuk mengkaji dan menganalisis kedudukan dan prosedur penyitaan akun media sosial dalam proses pembuktian cybercrime. Penelitian ini menggunakan penelitian hukum normatif dengan pendekatan perundang-undangan dan pendekatan kasus. Pengumpulan bahan hukum dilakukan dengan menggunakan teknik studi literatur. Bahan hukum yang terkumpul kemudian dianalisis secara kualitatif untuk mendeskripsikan masalah dan menjawab tujuan penelitian. Hasil penelitian menunjukkan bahwa kedudukan media sosial sebagai alat bukti yang sah dalam proses pembuktian di persidangan diatur dalam UU No. 11 Tahun 2008 dan UU No. 8 Tahun 1981. Bukti elektronik dapat dikategorikan sebagai alat bukti petunjuk dengan memenuhi syarat formil dan materiil yang diatur dalam UU No. 11 Tahun 2008. Sementara itu, prosedur penyitaan akun media sosial dalam proses pembuktian cybercrime didahului dengan penggeledahan handphone untuk mendapatkan spesifikasi perangkat. Akun media sosial, file, dokumen, dan aplikasi yang digunakan oleh pelaku cybercrime akan ditemukan dalam spesifikasi tersebut. Penyitaan akun media sosial diatur dalam Pasal 43 ayat (3) UU No. 19 Tahun 2016, sedangkan tata caranya dilakukan berdasarkan UU No. 8 Tahun 1981. Oleh karena itu, direkomendasikan agar pemerintah dan lembaga penegak hukum menerbitkan peraturan pelaksana mengenai prosedur penyitaan akun media sosial sebagai alat bukti yang sah dalam proses pembuktian kejahatan informasi dan transaksi elektronik. Selain itu, kolaborasi antara Kementerian Komunikasi dan Informatika dengan platform media sosial sangat diperlukan dalam penanganan kasus bisa lebih mudah dan efisien, terutama terkait penyitaan akun media sosial yang digunakan oleh pelaku cybercrime. Di sisi lain, perlu diperluas makna alat bukti petunjuk sebagaimana diatur dalam UU No. 8 Tahun 1981 agar dapat menekankan alat bukti media sosial sebagai alat bukti yang sah.

Kata Kunci: *Alat Bukti; Cybercrime; Media Sosial; Pembuktian.*

INTRODUCTION

Information and communication technology has experienced drastic developments in the era of globalization or the 4.0 era. This development has had a positive impact, namely using computer and mobile phone communication devices through the internet (Riyanto, 2020). The relationships (interactions) through information technology are no longer physical, as has been the case so far, but these interactions are virtual or cyberspace (Kantaatmadja et al., 2001).

Conversely, these developments also have a negative impact, namely cybercrime. Cybercrime perpetrators misuse this technology because users still do not

PENDAHULUAN

Teknologi informasi dan komunikasi mengalami perkembangan yang sangat drastis di era globalisasi atau era 4.0. Perkembangan ini memberikan dampak positif yaitu penggunaan perangkat komunikasi komputer dan handphone melalui internet. Hubungan (interaksi) melalui teknologi informasi tidak lagi bersifat fisik seperti yang terjadi selama ini, tetapi interaksi tersebut bersifat virtual atau dunia maya.

Sebaliknya, perkembangan tersebut juga membawa dampak negatif yaitu *cybercrime* (kejahatan dunia maya). Pelaku *cybercrime* menyalahgunakan teknologi ini karena pengguna masih belum memahami

understand the use of Information and Communication Technology properly and correctly. User understanding of using this technology will have an impact on the existence of cybercrime. On the other hand, cybercrime perpetrators using computers are called computer crime (Antoni, 2017). Meanwhile, perpetrators who use computers as tools to commit crimes are called computer-related crimes (Sulisrudatin, 2018).

On the other hand, offenses in the penal code have an abstract meaning from concrete events. In essence, the penal code is to provide protection to society and provide retaliation for the actions that the perpetrator has committed (Rivanie, 2022). In addition, as crime develops in society, the law must also develop so that its function as a provider of security can be fulfilled (Rivanie et al., 2021). Therefore, the categories of the offense must be given scientific terms and meaning and regulated in legislation (Rahmanto, 2019).

Internationally, legal phenomena in cyberspace already have several terms based on their field of study: cyber law, the law of information technology, and virtual world law (Ersya, 2017). These terms exist as a response to activities carried out through a network of computer and communication systems that can be viewed virtually. Likewise, telematics law is a convergence of telecommunication law, media law, and informatics law.

The Government then responded to community activities in cyberspace by forming Law No. 11 of 2008, amended by Law No. 19 of 2016. This law functions to guarantee legal certainty for people who carry out transactions electronically, encourage Indonesia's economic growth, and as one of the efforts to prevent information technology-based crimes or cybercrime.

Furthermore, content is information available through information and communication technology-based electronic media or products. Therefore, Law No. 11 of 2008 regulates the prohibition of distributing, transmitting, delivering, spreading, or making accessible the following content: violating decency; gambling; insult and/or defamation; extortion and/or threats; hoax and misleading news; causing feelings of hatred or hostility towards specific individuals and/or groups of people based on ethnicity, religion, race, and intergroup; and personal threats of violence or intimidation.

The content mentioned above is also able to qualify as electronic proof based on Article 5 section (2) of Law No. 11 of 2008, which regulates that:

penggunaan Teknologi Informasi dan Komunikasi dengan baik dan benar. Pemahaman pengguna dalam menggunakan teknologi ini akan berdampak pada adanya *cybercrime*. Di sisi lain, pelaku kejahatan dunia maya dengan menggunakan komputer disebut *computer crime*. Sedangkan pelaku yang menggunakan komputer sebagai alat untuk melakukan kejahatan disebut *computer-related crime*.

Di sisi lain, tindak pidana dalam hukum pidana memiliki makna abstrak dari peristiwa konkrit. Hakikatnya hukum pidana adalah untuk memberikan perlindungan kepada masyarakat dan memberikan pembalasan atas perbuatan yang telah dilakukan oleh pelaku. Selain itu, seiring berkembangnya kejahatan di masyarakat, hukum juga harus berkembang agar fungsinya sebagai pemberi rasa aman dapat terpenuhi. Oleh karena itu, kategori tindak pidana harus diberi istilah dan makna ilmiah dan diatur dalam peraturan perundang-undangan.

Secara internasional, fenomena hukum di dunia maya sudah memiliki beberapa istilah berdasarkan bidang kajiannya: hukum siber, hukum mayantara, hukum teknologi informasi, dan hukum dunia maya. Istilah-istilah tersebut ada sebagai respon terhadap aktivitas yang dilakukan melalui jaringan komputer dan sistem komunikasi yang dapat dilihat secara virtual. Demikian pula hukum telematika merupakan konvergensi dari hukum telekomunikasi, hukum media, dan hukum informatika.

Pemerintah kemudian merespon aktivitas masyarakat di dunia maya dengan membentuk UU No. 11 Tahun 2008 yang telah diubah dengan UU No. 19 Tahun 2016. Undang-undang ini berfungsi untuk menjamin kepastian hukum bagi masyarakat yang melakukan transaksi secara elektronik, mendorong pertumbuhan ekonomi Indonesia, dan sebagai salah satu upaya pencegahan kejahatan berbasis teknologi informasi atau *cybercrime*.

Selanjutnya, konten adalah informasi yang tersedia melalui media atau produk elektronik berbasis teknologi informasi dan komunikasi. Oleh karena itu, UU No. 11 Tahun 2008 mengatur larangan mendistribusikan, mentransmisikan, menyebarkan, mengirimkan, atau membuat dapat diaksesnya konten: melanggar kesusilaan; perjudian; penghinaan dan/atau pencemaran nama baik; pemerasan dan/atau pengancaman; berita bohong dan menyesatkan; menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antargolongan; dan ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi.

Konten tersebut di atas juga dapat dikualifikasikan sebagai alat bukti elektronik berdasarkan Pasal 5 ayat (2) UU No. 11 Tahun 2008, yang mengatur bahwa:

"Electronic Information and/or Electronic Documents and/or printouts, as referred to in section (1), are an expansion of the legal means of proof in accordance with the applicable Procedural Law in Indonesia."

In this case, Article 184 of Law No. 8 of 1981 regulates that:

"Legal means of proof are: a. the testimony of a witness; b. the testimony of an expert; c. a document; d. an indication; e. the testimony of the accused."

On the other hand, the perpetrator can remove and destroy content after committing a cybercrime. The perpetrator carried out the act to avoid criminal liability. At the same time, victims and law enforcers will find it difficult to obtain absolute truth due to the lack of proof in the evidentiary process. Therefore, law enforcers, based on Law No. 11 of 2008 and Law No. 8 of 1981, can seize computers or mobile phone communication devices used by cybercrime perpetrators.

In contrast, new problems will arise in the evidentiary process if the perpetrator commits a cybercrime using social media platforms: WhatsApp, Instagram, Facebook, and other social media. Meanwhile, computers or mobile phone communication devices used by cybercrime perpetrators are uncertain. In this case, the perpetrator replaces, exchanges, or even uses other people's devices whenever they want or after committing cybercrime.

One of the cybercrimes that can be studied in the case of fraud with the lottery club and investment mode contained in Decision No. 1808/Pid.Sus/2021/PN.Mks. In the charges process, the Public Prosecution only stated physical evidence in the form of three units of mobile phones, ten copies of bank transaction report printouts, one ATM card, and three printout screenshots of the arisanamanah_mks Instagram account. Law enforcers in Indonesia are still not accustomed to seizing social media accounts used by cybercrime perpetrators. The Judge in the decision stated that the accused had been legally and convincingly proven guilty of having committed the offense:

"As a person who commits or participates intentionally and without rights spreads hoaxes and misleading news, resulting in consumer losses in electronic transactions."

From the decision above, it can be judged that law enforcers should also seize social media accounts used by cybercrime perpetrators.

Based on the description above, this study aims to examine and analyze social media accounts' status and seizure procedures in the evidentiary process of cybercrime.

"Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya sebagaimana dimaksud pada ayat (1) merupakan perluasan dari alat bukti yang sah sesuai dengan Hukum Acara yang berlaku di Indonesia."

Dalam hal ini, Pasal 184 UU No. 8 Tahun 1981 mengatur bahwa:

"Alat bukti yang sah ialah: a. keterangan saksi; b. keterangan ahli; c. surat; d. petunjuk; e. keterangan terdakwa."

Di sisi lain, pelaku dapat menghapus dan menghancurkan konten setelah melakukan *cybercrime*. Pelaku melakukan perbuatan tersebut untuk menghindari pertanggungjawaban pidana. Pada saat yang sama, korban dan penegak hukum akan sulit mendapatkan kebenaran mutlak karena kurangnya alat bukti dalam proses pembuktian. Oleh karena itu, penegak hukum berdasarkan UU No. 11 Tahun 2008 dan UU No. 8 Tahun 1981 dapat menyita komputer atau alat komunikasi handphone yang digunakan oleh pelaku *cybercrime*.

Sebaliknya, masalah baru akan muncul dalam proses pembuktian jika pelaku melakukan *cybercrime* menggunakan platform media sosial: WhatsApp, Instagram, Facebook, dan media sosial lainnya. Sedangkan perangkat komunikasi komputer atau handphone yang digunakan oleh pelaku *cybercrime* tidak menentu. Dalam hal ini, pelaku mengganti, menukar, atau bahkan menggunakan perangkat milik orang lain kapanpun mereka mau atau setelah melakukan *cybercrime*.

Salah satu *cybercrime* yang dapat dikaji adalah kasus penipuan dengan modus arisan dan investasi yang termuat dalam Putusan No. 1808/Pid.Sus/2021/PN.Mks. Dalam proses tuntutan, Penuntut Umum hanya menyebutkan barang bukti berupa tiga unit handphone, sepuluh rangkap printout laporan transaksi bank, satu kartu ATM, dan tiga lembar printout screenshot dari akun Instagram arisanamanah_mks. Penegak hukum di Indonesia masih belum terbiasa menyita akun media sosial yang digunakan oleh pelaku *cybercrime*. Hakim dalam putusannya menyatakan bahwa terdakwa telah terbukti secara sah dan meyakinkan bersalah melakukan tindak pidana:

"Sebagai orang yang melakukan atau turut serta melakukan dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik."

Dari putusan di atas, dapat dinilai bahwa penegak hukum juga harus menyita akun media sosial yang digunakan oleh pelaku *cybercrime*.

Berdasarkan uraian di atas, penelitian ini bertujuan untuk mengkaji dan menganalisis kedudukan dan prosedur penyitaan akun media sosial dalam proses pembuktian *cybercrime*.

METHOD

This study uses normative legal research with a statute approach and a case approach (Qamar & Rezah, 2020). The legal materials used in this study include legislation, books and scientific law articles, and online materials discussing legislation forming. The collection of legal materials is carried out using a literature study technique. The collected legal material is then qualitatively analyzed to describe the problem and answer study purposes (Irwansyah, 2020).

RESULTS AND DISCUSSION

Status of Social Media in the Evidentiary Process of Cybercrime

Evidence is provisions that contain guidelines on ways justified by legislation to prove an indictment of offense to the accused (Wiredarme & Muttaqin, 2022). Evidence is also the provision governing proof based on legislation that Judges use when they want to prove an offense that will be decided later. The evidentiary process dramatically determines the outcome of the examination at the trial court against the accused. Evidence must be carried out, measured, and carefully to make an offense light and transparent.

The law of evidence in Law No. 8 of 1981 adheres to a limited law-based proof system (*negatief wettelijk bewijs theorie*). In this case, Article 183 of Law No. 8 of 1981 regulates that:

> *"A judge shall not impose a penalty upon a person except when with at least two legal means of proof he has come to the conviction that an offense has truly occurred and that it is the accused who is guilty of committing it."*

From the provisions above, it can be understood that the Judge imposing a penalty is not necessarily based solely on his conviction. However, that conviction is still based on at least two legal means of proof. This negative proof (*negative wettelijk*) is a combination of a proof system that relies on the conviction of Judges (conviction in time) and proof according to legislation (*positief wettelijk stelsel*).

Apart from that, one thing that is quite crucial is the position of physical evidence in the evidentiary system. Physical evidence is a material object. This physical evidence is not included in the proof category according to Article 184 of Law No. 8 of 1981. In principle, the legality of physical evidence also aligns with the position of proof. For example, physical evidence as a material object is worthless if not identified by the witness or accused.

METODE

Penelitian ini menggunakan penelitian hukum normatif dengan pendekatan perundang-undangan dan pendekatan kasus. Bahan hukum yang digunakan dalam penelitian ini meliputi peraturan perundang-undangan, buku dan artikel ilmiah hukum, dan bahan-bahan online yang membahas tentang pembentukan peraturan perundang-undangan. Pengumpulan bahan hukum dilakukan dengan menggunakan teknik studi literatur. Bahan hukum yang terkumpul kemudian dianalisis secara kualitatif untuk mendeskripsikan masalah dan menjawab tujuan penelitian.

HASIL DAN PEMBAHASAN

Kedudukan Media Sosial dalam Proses Pembuktian Cybercrime

Pembuktian adalah ketentuan yang memuat pedoman tentang cara-cara yang dibenarkan oleh peraturan perundang-undangan untuk membuktikan suatu dakwaan tindak pidana kepada terdakwa. Pembuktian juga merupakan ketentuan yang mengatur tentang alat bukti berdasarkan peraturan perundang-undangan yang digunakan Hakim ketika ingin membuktikan suatu delik yang akan diputus nanti. Proses pembuktian sangat menentukan hasil pemeriksaan di sidang pengadilan terhadap terdakwa. Pembuktian harus dilakukan, diukur, dan hati-hati untuk membuat tindak pidana menjadi terang dan jelas.

Hukum pembuktian dalam UU No. 8 Tahun 1981 menganut sistem pembuktian berdasarkan hukum terbatas (*negatief wettelijk bewijs theorie*). Dalam hal ini, Pasal 183 UU No. 8 Tahun 1981 mengatur bahwa:

> *"Hakim tidak boleh menjatuhkan pidana kepada seorang kecuali apabila dengan sekurang-kurangnya dua alat bukti yang sah ia memperoleh keyakinan bahwa suatu tindak pidana benar-benar terjadi dan bahwa terdakwalah yang bersalah melakukannya."*

Dari ketentuan di atas dapat dipahami bahwa Hakim yang menjatuhkan pidana tidak harus semata-mata berdasarkan keyakinannya. Namun, keyakinan itu tetap didasarkan pada setidaknya dua alat bukti yang sah. Pembuktian negatif (*negative wettelijk*) ini merupakan gabungan dari sistem pembuktian yang bersandar pada keyakinan Hakim (*conviction in time*) dan pembuktian menurut peraturan perundang-undangan (*positief wettelijk stelsel*).

Selain itu, satu hal yang cukup krusial adalah kedudukan barang bukti dalam sistem pembuktian. Barang bukti merupakan objek materiil. Barang bukti ini tidak termasuk dalam kategori alat bukti menurut Pasal 184 UU No. 8 Tahun 1981. Pada prinsipnya, keabsahan barang bukti juga selaras dengan kedudukan alat bukti. Misalnya, barang bukti sebagai objek materiil tidak bernilai jika tidak diidentifikasi oleh saksi atau terdakwa.

From a formal juridical point of view, the position of physical evidence is not categorized as legal means of proof. In contrast, physical evidence can be identified and categorized as legal means of proof in the evidentiary process at trial. In this regard, it can be understood that physical evidence and proof have critical linkages as regulated in Article 181 of Law No. 8 of 1981.

Meanwhile, the legal means of proof category in the evidentiary process of cybercrime is based on Article 5 section (1) of Law No. 11 of 2008, which regulates that:

> *"Electronic Information and/or Electronic Documents and/or printouts are the legal means of legal proof."*

Furthermore, Article 2 section (5) point b number 4 of Government Regulation No. 71 of 2019 regulates that:

> *"Private Electronic System Operators, as referred to in section (2) point b, include: Electronic System Operators who have portals, sites, or applications in the network via the internet that are used for: provide, manage, and/or operate communication services, including but not limited to short messages, voice calls, video calls, electronic mail, and online conversations in digital platforms, networking services, and social media."*

From the provisions above, it can be understood that social media can be categorized as a legal means of proof in the evidentiary process of cybercrime. The status of social media as a legal means of proof is followed up based on Law No. 8 of 1981.

The description regarding the status of social media as a legal means of proof is not reflected in Decision No. 1808/Pid.Sus/2021/PN.Mks. In the charges process, the Public Prosecution only stated physical evidence in the form of three units of mobile phones, ten copies of bank transaction report printouts, one ATM card, and three printout screenshots of the arisanamanah_mks Instagram account. The physical evidence has also been presented during the evidentiary process at the trial.

At the trial, the Public Prosecutor presented various physical evidence, including printout screenshots of the arisanamananah_mks Instagram account used by the Accused in committing an offense of cybercrime. Meanwhile, the Public Prosecution can present a printout screenshot if they seize the arisanamananah_mks Instagram account. Public Prosecutor in Decision No. 1808/Pid.Sus/2021/PN.Mks further categorizes these printout screenshots as proof of indications regulated in Law No. 11 of 2008 and Law No. 8 of 1981.

Electronic evidence must first meet the formal and material requirements in the evidentiary process. In this case, can it be categorized as proof or limited

Dari segi yuridis formal, kedudukan barang bukti tidak dikategorikan sebagai alat bukti yang sah. Sebaliknya, barang bukti dapat diidentifikasi dan dikategorikan sebagai alat bukti yang sah dalam proses pembuktian di persidangan. Dalam kaitan ini, dapat dipahami bahwa barang bukti dan alat bukti memiliki keterkaitan yang penting sebagaimana diatur dalam Pasal 181 UU No. 8 Tahun 1981.

Sedangkan kategori alat bukti yang sah dalam proses pembuktian *cybercrime* didasarkan pada Pasal 5 ayat (1) UU No. 11 Tahun 2008 yang mengatur bahwa:

> *"Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."*

Selanjutnya Pasal 2 ayat (5) huruf b angka 4 PP No. 71 Tahun 2019 mengatur bahwa:

> *"Penyelenggara Sistem Elektronik Lingkup Privat sebagaimana dimaksud pada ayat (2) huruf b meliputi: Penyelenggara Sistem Elektronik yang memiliki portal, situs, atau aplikasi dalam jaringan melalui internet yang dipergunakan untuk: menyediakan, mengelola, dan/atau mengoperasikan layanan komunikasi meliputi namun tidak terbatas pada pesan singkat, panggilan suara, panggilan video, surat elektronik, dan percakapan dalam jaringan dalam bentuk platform digital, layanan jejaring dan media sosial."*

Dari ketentuan di atas, dapat dipahami bahwa media sosial dapat dikategorikan sebagai alat bukti yang sah dalam proses pembuktian *cybercrime*. Kedudukan media sosial sebagai alat bukti yang sah ditindaklanjuti berdasarkan UU No. 8 Tahun 1981.

Uraian mengenai kedudukan media sosial sebagai alat bukti yang sah tidak tercermin dalam Putusan No. 1808/Pid.Sus/2021/PN.Mks. Dalam proses tuntutan, Penuntut Umum hanya menyebutkan barang bukti berupa tiga unit handphone, sepuluh rangkap printout laporan transaksi bank, satu kartu ATM, dan tiga lembar printout screenshot dari akun Instagram arisanamanah_mks. Barang bukti juga telah dihadirkan selama proses pembuktian di persidangan.

Dalam persidangan, Penuntut Umum menghadirkan berbagai barang bukti antara lain printout screenshot dari akun Instagram arisanamanah_mks yang digunakan Terdakwa melakukan *cybercrime*. Sementara itu, Penuntut Umum dapat menghadirkan satu set printout screenshot jika mereka menyita akun Instagram arisanamananah_mks. Penuntut Umum dalam Putusan No. 1808/Pid.Sus/2021/PN.Mks lebih lanjut mengkategorikan printout screenshot tersebut sebagai alat bukti petunjuk yang diatur dalam UU No. 11 Tahun 2008 dan UU No. 8 Tahun 1981.

Bukti elektronik harus terlebih dahulu memenuhi syarat formil dan materiil dalam proses pembuktian. Dalam hal ini, apakah dapat dikategorikan sebagai

to physical evidence to support proof? On the other hand, physical evidence and proof have critical linkages that cannot be separated (Pribadi, 2018). Electronic evidence can only be used if categorized as proof or limited to physical evidence (Wu & Zheng, 2020). These requirements are also the basis for the Public Prosecutor so that electronic proof can generate conviction for the Panel of Judges and simultaneously provide legal certainty for the Accused.

Formal requirements regarding electronic evidence, especially those related to social media accounts, are based on Article 5 section (4) of Law No. 11 of 2008, which regulates that:

> *"Provisions regarding Electronic Information and/or Electronic Documents, as referred to in section (1), do not apply to: a. letter according to the law must be made in written form; and b. letters and their documents which, according to the law, must be made in the form of a notary deed or a deed made by a deed-making official."*

Furthermore, Article 43 section (3) of Law No. 19 of 2016 regulates that:

> *"Searches and/or seizures of Electronic Systems related to alleged criminal acts in the field of Information Technology and Electronic Transactions are carried out in accordance with the provisions of the criminal procedural law."*

In addition, there are material requirements in determining the legality of electronic evidence as based on Article 5 section (3) of Law No. 11 of 2008, which regulates that:

> *"Electronic Information and/or Electronic Documents are declared legal when using Electronic Systems in accordance with the provisions regulated in this Law."*

Article 6 of Law No. 11 of 2008 regulates that:

> *"In the event that there are provisions other than those regulated in Article 5 section (4) which require that information must be in written form or original, Electronic Information and/or Electronic Documents are considered legal as long as the information contained therein can be accessed, displayed, guaranteed wholeness, and can be accounted for to explain a situation."*

From the formal and material requirements mentioned above, the Investigator and Public Prosecutor should have handled the case as well as possible. On the other hand, the Investigator and Public Prosecutor must also ensure that element can be accessed, displayed, guaranteed wholeness, and accounted for as regulated in Article 6 of Law No. 11 of 2008. In this case, the Investigator and Public Prosecutor must seize social

alat bukti atau terbatas pada barang bukti untuk menunjang alat bukti? Di sisi lain, barang bukti dan alat bukti memiliki keterkaitan penting yang tidak dapat dipisahkan. Bukti elektronik hanya dapat digunakan jika dikategorikan sebagai alat bukti atau terbatas pada barang bukti. Persyaratan tersebut juga menjadi dasar bagi Penuntut Umum agar alat bukti elektronik dapat menimbulkan keyakinan bagi Majelis Hakim dan sekaligus memberikan kepastian hukum bagi Terdakwa.

Persyaratan formil mengenai bukti elektronik, khususnya yang berkaitan dengan akun media sosial, didasarkan pada Pasal 5 ayat (4) UU No. 11 Tahun 2008 yang mengatur bahwa:

> *"Ketentuan mengenai Informasi Elektronik dan/atau Dokumen Elektronik sebagaimana dimaksud pada ayat (1) tidak berlaku untuk: a. surat yang menurut Undang-Undang harus dibuat dalam bentuk tertulis; dan b. surat beserta dokumennya yang menurut Undang-Undang harus dibuat dalam bentuk akta notaril atau akta yang dibuat oleh pejabat pembuat akta."*

Selanjutnya, Pasal 43 ayat (3) UU No. 19 Tahun 2016 mengatur bahwa:

> *"Penggeledahan dan/ atau penyitaan terhadap Sistem Elektronik yang terkait dengan dugaan tindak pidana di bidang Teknologi Informasi dan Transaksi Elektronik dilakukan sesuai dengan ketentuan hukum acara pidana."*

Selain itu, terdapat syarat materiil dalam menentukan keabsahan bukti elektronik sebagaimana berdasarkan Pasal 5 ayat (3) UU No. 11 Tahun 2008, yang mengatur bahwa:

> *"Informasi Elektronik dan/atau Dokumen Elektronik dinyatakan sah apabila menggunakan Sistem Elektronik sesuai dengan ketentuan yang diatur dalam Undang-Undang ini."*

Pasal 6 UU No. 11 Tahun 2008 mengatur bahwa:

> *"Dalam hal terdapat ketentuan lain selain yang diatur dalam Pasal 5 ayat (4) yang mensyaratkan bahwa suatu informasi harus berbentuk tertulis atau asli, Informasi Elektronik dan/atau Dokumen Elektronik dianggap sah sepanjang informasi yang tercantum di dalamnya dapat diakses, ditampilkan, dijamin keutuhannya, dan dapat dipertanggungjawabkan sehingga menerangkan suatu keadaan."*

Dari syarat formil dan materiil tersebut di atas, seharusnya Penyidik dan Penuntut Umum menangani perkara tersebut dengan sebaik-baiknya. Di sisi lain, Penyidik dan Penuntut Umum juga harus memastikan bahwa unsur tersebut dapat diakses, ditampilkan, dijamin keutuhannya, dan dapat dipertanggungjawabkan sebagaimana diatur dalam Pasal 6 UU No. 11 Tahun 2008. Dalam hal ini, Penyidik dan Penuntut Umum wajib menyita akun media sosial

media accounts in order to be able to access, guarantee wholeness, and be accountable for the legality of proof.

In addition, electronic information or documents accessed directly through social media accounts can produce electronic proof in original form and with guaranteed wholeness. The quality of electronic proof in the form of wholeness or a set of printout screenshots can also be of the same value. In other words, the Public Prosecutor can use and present both or one at trial. In contrast, if the Public Prosecutor does not seize social media accounts, printout screenshots can be qualified as not legal means of proof in court.

Seizure Procedures of Social Media Accounts in the Evidentiary Process of Cybercrime

In the cybercrime law enforcement process, investigative efforts by Investigators and charges by the Public Prosecutor are needed (Arisandy, 2020). These efforts were made to make cybercrime light and clear before the Panel of Judges. Apart from that, this effort was also made to give confidence to the Panel of Judges in considering up to present a court decision that has become final and binding (*inkracht van gewijsde*).

A series of efforts to the cybercrime law enforcement process must be carried out carefully and procedurally as regulated in Law No. 11 of 2008 and Law No. 8 of 1981 to present legal means of proof and strengthen legal facts in the evidentiary process at trial. On the other hand, Investigators and Public Prosecutors will conduct various activities to obtain legal means of proof according to Law No. 11 of 2008 and Law No. 8 of 1981. The collection of proofs is done to achieve a perfect evidentiary because there is one adage: in criminal cases, the proofs ought to be more transparent than light (*in criminalibus probationes debent esse luce clariores*). Apart from that, one principle is also known as the party that makes the allegation; then, he is the one who must prove it (*actori incumbit probatio, actori onus probandi*). Therefore, the burden of the evidentiary in court based on applying this principle is the burden and duty of the Public Prosecutor.

Investigators and Public Prosecutors can seize anything related to a criminal act to collect proof. In this case, Article 1 point 16 of Law No. 8 of 1981 explains that:

> *"Seizure is a series of acts by an investigator to take possession and/or to retain under his control movable or immovable goods, whether tangible or intangible, to be used for evidentiary purposes in investigation, prosecution and adjudication."*

On the other hand, a seizure is one of the forced efforts which, in principle, must be under the provisions regulated in Law No. 8 of 1981. In contrast, Law No. 8

agar dapat mengakses, menjamin keutuhan, dan mempertanggungjawabkan keabsahan alat bukti.

Selain itu, informasi atau dokumen elektronik yang diakses langsung melalui akun media sosial dapat menghasilkan alat bukti elektronik dalam bentuk asli dan terjamin keutuhannya. Kualitas alat bukti elektronik berupa keutuhan atau satu set printout screenshot juga dapat bernilai sama. Dengan kata lain, Penuntut Umum dapat menggunakan dan menghadirkan keduanya atau salah satunya dalam persidangan. Sebaliknya, jika Penuntut Umum tidak menyita akun media sosial, printout screenshot dapat dikualifikasikan sebagai alat bukti yang tidak sah di pengadilan.

Prosedur Penyitaan Akun Media Sosial dalam Proses Pembuktian Cybercrime

Dalam proses penegakan hukum *cybercrime*, diperlukan upaya penyelidikan oleh Penyidik dan tuntutan oleh Penuntut Umum. Upaya tersebut dilakukan agar *cybercrime* menjadi terang dan jelas di hadapan Majelis Hakim. Selain itu, upaya ini juga dilakukan untuk memberikan kepercayaan kepada Majelis Hakim dalam mempertimbangkan hingga memberikan putusan pengadilan yang telah memperoleh kekuatan hukum tetap (*inkracht van gewijsde*).

Serangkaian upaya proses penegakan hukum *cybercrime* harus dilakukan secara hati-hati dan prosedural sebagaimana diatur dalam UU No. 11 Tahun 2008 dan UU No. 8 Tahun 1981 guna menghadirkan alat bukti yang sah dan memperkuat fakta hukum dalam proses pembuktian di persidangan. Di sisi lain, Penyidik dan Penuntut Umum akan melakukan berbagai kegiatan untuk memperoleh alat bukti yang sah menurut UU No.11 Tahun 2008 dan UU No.8 Tahun 1981. Pengumpulan alat bukti dilakukan untuk mencapai pembuktian yang sempurna karena terdapat satu adagium: dalam kasus pidana, alat bukti harus lebih terang daripada cahaya (*in criminalibus probationes debent esse luce clariores*). Selain itu, satu prinsip juga dikenal sebagai siapa yang mendalilkan, maka dialah yang harus membuktikannya (*actori incumbit probatio, actori onus probandi*). Oleh karena itu, beban pembuktian di pengadilan berdasarkan penerapan asas ini menjadi beban dan tugas Penuntut Umum.

Penyidik dan Penuntut Umum dapat menyita segala sesuatu yang berkaitan dengan tindak pidana guna mengumpulkan alat bukti. Dalam hal ini, Pasal 1 angka 16 UU No. 8 Tahun 1981 menjelaskan bahwa:

> *"Penyitaan adalah serangkaian tindakan penyidik untuk mengambil alih dan atau menyimpan di bawah penguasaannya benda bergerak atau tidak bergerak, berwujud atau tidak berwujud untuk kepentingan pembuktian dalam penyidikan, penuntutan dan peradilan."*

Di sisi lain, penyitaan merupakan salah satu upaya paksa yang pada prinsipnya harus sesuai dengan ketentuan yang diatur dalam UU No. 8 Tahun 1981. Sebaliknya, UU No. 8 Tahun 1981 juga mengatur tentang

of 1981 also provides for the possibility or exception of criminal procedural procedures that are more specific or *lex specialis*. In this case, Article 284 section (2) of Law No. 8 of 1981 regulates that:

> *"Within two years after the promulgation of this law all cases shall be subject to the provisions of this law, with temporary exception for special provisions on criminal procedure as referred to in certain laws, until they are amended and or are declared ineffective."*

From the provisions above, it can be understood that if a law regulates procedures in specific procedural law in more detail, it is possible to apply procedural law procedures in the said law. For example, Law No. 11 of 2008, amended by Law No. 19 of 2016, also forms the basis for criminal procedural law for cybercrime and other criminal acts related to Electronic Information and Transactions.

As previously described, some cybercrimes use social media as an instrument for committing offenses. Therefore, the media or instruments also need to be examined and studied to describe the offenses committed by cybercrime perpetrators. Meanwhile, electronic proof has been regulated in Article 5 of Law No. 11 of 2008, while seizures have been regulated in Article 43, section (3) and section (4) of Law No. 19 of 2016.

Logically, social media is an instrument or media used by cybercrime perpetrators in committing an offense. Social media is used within the boundless scope of cyberspace: WhatsApp, Instagram, Facebook, and other social media. In contrast, the perpetrator can remove and destroy content after committing a cybercrime. In this case, the perpetrator replaces, exchanges, or even uses other people's devices whenever they want or after committing cybercrime (Suhyana et al., 2021). The perpetrator carried out the act to avoid criminal liability. Therefore, law enforcers must seize computers, mobile phone communication devices, and social media accounts used by cybercrime perpetrators.

Even though Government Regulation No. 71 of 2019 and Law No. 11 of 2008 regulate the seizures of social media accounts, the legislation does not explicitly regulate the procedures for the seizure of social media accounts used by cybercrime perpetrators. The procedure for seizing social media accounts, as regulated in Article 43 section (3) of Law No. 19 of 2016, remains subject to the seizure procedure regulated in Law No. 8 of 1981.

While Decision No. 1808/Pid.Sus/2021/PN.Mks is impossible to provide an adequate explanation of the

kemungkinan atau pengecualian terhadap prosedur hukum acara pidana yang bersifat lebih spesifik atau *lex specialis*. Dalam hal ini, Pasal 284 ayat (2) UU No. 8 Tahun 1981 mengatur bahwa:

> *"Dalam waktu dua tahun setelah undang-undang ini diundangkan, maka terhadap semua perkara diberlakukan ketentuan undang-undang ini, dengan pengecualian untuk sementara mengenai ketentuan khusus acara pidana sebagaimana tersebut pada undang-undang tertentu, sampai ada perubahan dan atau dinyatakan tidak berlaku lagi."*

Dari ketentuan di atas, dapat dipahami bahwa apabila suatu undang-undang mengatur prosedur dalam hukum acara tertentu secara lebih rinci, maka dimungkinkan untuk menerapkan hukum acara dalam undang-undang tersebut. Misalnya, UU No. 11 Tahun 2008 yang diubah dengan UU No. 19 Tahun 2016 juga menjadi dasar hukum acara pidana untuk *cybercrime* dan tindak pidana lainnya yang berkaitan dengan Informasi dan Transaksi Elektronik.

Seperti yang telah dijelaskan sebelumnya, beberapa *cybercrime* menggunakan media sosial sebagai instrumen untuk melakukan tindak pidana. Oleh karena itu, media atau instrumen juga perlu ditelaah dan dipelajari untuk menguraikan tindak pidana yang dilakukan oleh pelaku *cybercrime*. Sementara itu, alat bukti elektronik diatur dalam Pasal 5 UU No. 11 Tahun 2008, sedangkan penyitaan diatur dalam Pasal 43 ayat (3) dan ayat (4) UU No. 19 Tahun 2016.

Secara logis, media sosial merupakan instrumen atau media yang digunakan oleh para pelaku *cybercrime* dalam melakukan kejahatan. Media sosial digunakan dalam ruang lingkup dunia maya yang tidak terbatas: WhatsApp, Instagram, Facebook, dan media sosial lainnya. Sebaliknya, pelaku dapat menghapus dan menghancurkan konten setelah melakukan *cybercrime*. Dalam hal ini, pelaku mengganti, menukar, atau bahkan menggunakan perangkat milik orang lain kapanpun mereka mau atau setelah melakukan *cybercrime*. Pelaku melakukan perbuatan tersebut untuk menghindari pertanggungjawaban pidana. Oleh karena itu, aparat penegak hukum harus menyita komputer, alat komunikasi handphone, dan akun media sosial yang digunakan oleh pelaku *cybercrime*.

Meskipun PP No. 71 Tahun 2019 dan UU No. 11 Tahun 2008 mengatur tentang penyitaan akun media sosial, namun peraturan perundang-undangan tersebut tidak mengatur secara tegas prosedur penyitaan akun media sosial yang digunakan oleh pelaku *cybercrime*. Prosedur penyitaan akun media sosial sebagaimana diatur dalam Pasal 43 ayat (3) UU No. 19 Tahun 2016 tetap tunduk pada prosedur penyitaan yang diatur dalam UU No. 8 Tahun 1981.

Sedangkan Putusan No. 1808/Pid.Sus/2021/PN.Mks tidak mungkin memberikan penjelasan yang memadai tentang prosedur penyitaan. Oleh karena

seizure procedure. Therefore, a sample court decision is needed to describe the seizure procedure adequately. In this case, Decision No. 255/Pid.Sus/2021/PN.Mks can explain the seizure procedure of social media accounts used by cybercrime perpetrators.

Investigators in Decision No. 255/Pid.Sus/2021/PN.Mks seizure of the email account and password connected to the accused's Facebook account. The seizure has obtained Court Decree No. 1723/Pen.Pid/2020/PN.Mks, as regulated in Article 38 section (1) of Law No. 8 of 1981. The seizure is also based on Seizure Warrant No. SP.Sita/142/VIII/2020/Ditrekrimsus and has been completed with the minutes of the seizure, as regulated in Article 75 section (1) point f of Law No. 8 of 1981.

Initially, investigators first searched the mobile phone communication device used by the cybercrime accused. A seizure is needed to obtain the specifications of the device used by cybercrime perpetrators (Riskiyadi, 2020). IMEI and serial number are essential in tracing the device's usage history, even if the file, document, or application has been deleted.

Furthermore, the investigator seized the accused's email account. The investigator changes the account password to expedite the investigation process's interests. Changes to the account password are also accompanied by Minutes of Changes in Email Address Password Codes.

On the other hand, investigators have devices to search and extract files, documents, or applications used on mobile phones. The results of the operation of these devices are needed for investigative purposes (Mualfah et al., 2023). This search will be able to open the files, documents, and applications needed to be accessed and can find the history of social media use that was used by the cybercrime accused.

In contrast, investigators can report directly to the platform to take down the cybercrime perpetrator's social media accounts for a specific incident that does not require seizure attempts because they result in conditions that are not conducive. The Public Prosecutor can also set aside a specific incident using the opportunity principle (Akub & Sutiawati, 2018). Law enforcers make these efforts to maintain security conditions, especially in cyberspace which is the public's attention.

CONCLUSIONS AND SUGGESTIONS

Based on the results and discussion above, it can be concluded that the status of social media as legal means of proof in the evidentiary process at trial is regulated in Law No. 11 of 2008 and Law No. 8 of 1981. Electronic evidence can be categorized as physical evidence to support proof. It can also be categorized as proof of indication by fulfilling the formal and material requirements regulated in Law No. 11 of 2008. Proof of indication must also align with other proofs presented

itu, diperlukan contoh putusan pengadilan yang dapat menggambarkan prosedur penyitaan secara memadai. Dalam hal ini, Putusan No. 255/Pid.Sus/2021/PN.Mks dapat menjelaskan prosedur penyitaan akun media sosial yang digunakan oleh pelaku *cybercrime*.

Penyidik dalam Putusan No. 255/Pid.Sus/2021/PN.Mks menyita akun email dan password yang terhubung dengan akun Facebook terdakwa. Penyitaan tersebut telah mendapatkan Penetapan Pengadilan No. 1723/Pen.Pid/2020/PN.Mks, sebagaimana diatur dalam Pasal 38 ayat (1) UU No. 8 Tahun 1981. Penyitaan tersebut juga berdasarkan Surat Perintah Penyitaan No. SP.Sita /142/VIII/2020/Ditrekrimsus dan telah dilengkapi berita acara penyitaan sebagaimana diatur dalam Pasal 75 ayat (1) huruf f UU No. 8 Tahun 1981.

Awalnya, penyidik terlebih dahulu menggeledah alat komunikasi handphone yang digunakan terdakwa *cybercrime*. Penyitaan diperlukan untuk mendapatkan spesifikasi perangkat yang digunakan pelaku *cybercrime*. IMEI dan nomor seri sangat penting dalam melacak riwayat penggunaan perangkat, meskipun file, dokumen, atau aplikasi telah dihapus.

Selanjutnya, penyidik menyita akun email tersangka. Penyelidik mengubah kata sandi akun untuk mempercepat kepentingan proses penyelidikan. Perubahan password akun juga disertai Berita Acara Perubahan Kode Password Alamat Email.

Di sisi lain, penyidik memiliki perangkat untuk mencari dan mengekstrak file, dokumen, atau aplikasi yang digunakan di handphone. Hasil pengoperasian perangkat ini diperlukan untuk tujuan investigasi. Pencarian ini akan dapat membuka file, dokumen, dan aplikasi yang diperlukan untuk diakses dan dapat menemukan riwayat penggunaan media sosial yang digunakan oleh terdakwa *cybercrime*.

Sebaliknya, penyidik dapat melaporkan langsung ke platform untuk melakukan pencopotan akun media sosial pelaku *cybercrime* atas kejadian tertentu yang tidak memerlukan upaya penyitaan karena mengakibatkan kondisi yang tidak kondusif. Penuntut Umum juga dapat mengesampingkan suatu kejadian tertentu dengan menggunakan asas oportunitas. Upaya tersebut dilakukan oleh aparat penegak hukum untuk menjaga kondisi keamanan, khususnya di dunia maya yang menjadi atensi publik.

KESIMPULAN DAN SARAN

Berdasarkan hasil dan pembahasan di atas, dapat disimpulkan bahwa kedudukan media sosial sebagai alat bukti yang sah dalam proses pembuktian di persidangan diatur dalam UU No. 11 Tahun 2008 dan UU No. 8 Tahun 1981. Bukti elektronik dapat dikategorikan sebagai barang bukti untuk mendukung alat bukti. Hal itu juga dapat dikategorikan sebagai alat bukti petunjuk dengan memenuhi syarat formil dan materiil yang diatur dalam UU No. 11 Tahun 2008. Alat bukti

at trial. Meanwhile, seizure procedures of social media accounts in the evidentiary process of cybercrime are preceded by searching mobile phone communication to obtain device specifications. Social media accounts, files, documents, and applications used by cybercrime perpetrators will be found in these specifications. Seizure of social media accounts is regulated in Article 43 section (3) of Law No. 19 of 2016, while the procedure is carried out based on Law No. 8 of 1981. Based on the description of these conclusions, it is recommended that the government and law enforcement agencies issue implementing regulations regarding the procedure for seizing social media accounts as legal means of proof in the evidentiary process of electronic information and transaction crimes. In addition, the collaboration between the Ministry of Communications and Informatics and social media platforms is needed in preventing and handling cases of electronic information and transaction crimes. In this case, coordination in handling cases can be easier and more efficient, especially regarding seizures of social media accounts used by cybercrime perpetrators. On the other hand, it is necessary to expand the meaning of proof of indication as regulated in Law No. 8 of 1981 in order to be able to emphasize social media proof as a legal means of proof. In this case, a judicial review is carried out through a Constitutional Court Decision, which regulates social media as proof of indication, as has been done in several legal discovery efforts.

petunjuk juga harus sejalan dengan alat bukti lain yang dihadirkan di persidangan. Sementara itu, prosedur penyitaan akun media sosial dalam proses pembuktian *cybercrime* didahului dengan penggeledahan handphone untuk mendapatkan spesifikasi perangkat. Akun media sosial, file, dokumen, dan aplikasi yang digunakan oleh pelaku *cybercrime* akan ditemukan dalam spesifikasi tersebut. Penyitaan akun media sosial diatur dalam Pasal 43 ayat (3) UU No. 19 Tahun 2016, sedangkan tata caranya dilakukan berdasarkan UU No. 8 Tahun 1981. Berdasarkan uraian kesimpulan tersebut, direkomendasikan agar pemerintah dan lembaga penegak hukum menerbitkan peraturan pelaksana mengenai prosedur penyitaan akun media sosial sebagai alat bukti yang sah dalam proses pembuktian kejahatan informasi dan transaksi elektronik. Selain itu, kolaborasi antara Kementerian Komunikasi dan Informatika dengan platform media sosial sangat diperlukan dalam pencegahan dan penanganan kasus kejahatan informasi dan transaksi elektronik. Dalam hal ini, koordinasi dalam penanganan kasus bisa lebih mudah dan efisien, terutama terkait penyitaan akun media sosial yang digunakan oleh pelaku *cybercrime*. Di sisi lain, perlu diperluas makna alat bukti petunjuk sebagaimana diatur dalam UU No. 8 Tahun 1981 agar dapat menekankan alat bukti media sosial sebagai alat bukti yang sah. Dalam hal ini, uji materi dilakukan melalui Putusan Mahkamah Konstitusi yang mengatur media sosial sebagai alat bukti petunjuk, sebagaimana telah dilakukan dalam beberapa upaya penemuan hukum.

REFERENCES

Akub, S., & Sutiawati, S. (2018). *Keadilan Restoratif*. CV. Litera.

Antoni, A. (2017). Kejahatan Dunia Maya (Cyber Crime) dalam Simak Online. *Nurani: Jurnal Kajian Syari`ah dan Masyarakat, 17*(2), 261-274. https://doi.org/10.19109/nurani.v17i2.1192

Arisandy, Y. O. (2020). Penegakan Hukum terhadap Cyber Crime Hacker. *Indonesian Journal of Criminal Law and Criminology (IJCLC), 1*(3), 162-169. https://doi.org/10.18196/ijclc.v1i3.11264

Decision of the District Court of Makassar Number 1808/Pid.Sus/2021/PN Mks. http://sipp.pn-makassar.go.id/show_detil/S2FLbHBJUk1rdVZYVW5VNWs5a2g2THIydVByRGZlYVJPeG8zY0RBMjE3Y1V0b3AySXU5SlhqcWRIaEtUZURBMnZWRVk4NUFNM1VnenkvWlhXZXNVdGc9PQ==

Decision of the District Court of Makassar Number 255/Pid.Sus/2021/PN Mks. http://sipp.pn-makassar.go.id/show_detil/bktLd2hOVENKT29LZGE1ZDE5VlRjeGNFUjJBYm0rU3FtbWhrMWhQQ2UwaTFvbGRRNHR4NWtzdFIvaHdacE5Gbi9IRXNGZkZ3ZWZuREozdE1jSXhuTlE9PQ==

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

Government Regulation of the Republic of Indonesia Number 71 of 2019 on Organization of Electronic Systems and Transactions (State Gazette of the Republic of Indonesia of 2019 Number 185, Supplement to the State Gazette of the Republic of Indonesia Number 6400). https://peraturan.go.id/peraturan/view.html?id=8bbe35c2d0c1d71527ff135120c6825e

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

Kantaatmadja, M. K., Wiradipraja, E. S., Sastrawidjaja, M. S., Ramli, A. M., Saefulah, T. S., Hawkins, C., Dewi, S., Ikhwansyah, I., Abubakar, L., Latipulhayat, A., Gultom, E., Budhijanto, D., Imamulhadi, I., & Siswadi, A. G. C. (2001). *CyberLaw: Suatu Pengantar*. ELIPS Project.

Law of the Republic of Indonesia Number 8 of 1981 on the Code of Criminal Procedure (State Gazette of the Republic of Indonesia of 1981 Number 76, Supplement to the State Gazette of the Republic of Indonesia Number 3209). https://www.dpr.go.id/jdih/index/id/755

Law of the Republic of Indonesia Number 11 of 2008 on Electronic Information and Transactions (State Gazette of the Republic of Indonesia of 2008 Number 58, Supplement to the State Gazette of the Republic of Indonesia Number 4843). https://www.dpr.go.id/jdih/index/id/138

Law of the Republic of Indonesia Number 19 of 2016 on Amendment to Law Number 11 of 2008 on Electronic Information and Transactions (State Gazette of the Republic of Indonesia of 2016 Number 251, Supplement to the State Gazette of the Republic of Indonesia Number 5952). https://www.dpr.go.id/jdih/index/id/1683

Mualfah, D., Viransa, A., & Amran, H. F. a. (2023). Akuisisi Bukti Digital pada Aplikasi Tamtam Messenger Menggunakan Metode National Institute of Justice. *Journal of Software Engineering and Information System, 3*(1), 7-16. https://doi.org/10.37859/seis.v3i1.4548

Pribadi, I. (2018). Legalitas Alat Bukti Elektronik dalam Sistem Peradilan Pidana. *Lex Renaissance, 3*(1), 109-124. https://doi.org/10.20885/JLR.vol3.iss1.art4

Qamar, N., & Rezah, F. S. (2020). *Metode Penelitian Hukum: Doktrinal dan Non-Doktrinal*. CV. Social Politic Genius (SIGn).

Rahmanto, T. Y. (2019). Penegakan Hukum terhadap Tindak Pidana Penipuan Berbasis Transaksi Elektronik. *Jurnal Penelitian Hukum de Jure, 19*(1), 31-52. http://dx.doi.org/10.30641/dejure.2019.V19.31-52

Riskiyadi, M. (2020). Investigasi Forensik terhadap Bukti Digital dalam Mengungkap Cybercrime. *Cyber Security dan Forensik Digital, 3*(2), 12-21. https://doi.org/10.14421/csecurity.2020.3.2.2144

Rivanie, S. S. (2022). *Hukum Pidana Terorisme: Hakikat Sanksi dan Pengaturan Terorisme di Indonesia*. Penerbit KBM Indonesia.

Rivanie, S. S., Komuna, A. P., Putra, A. A., Utama, P. F., & Muzakkir, A. K. (2021). Protection of Children as Perpetrators of Criminal Act Stimulated by Pornography Based on Indonesian Laws. *Musamus Law Review, 4*(1), 1-15. https://doi.org/10.35724/mularev.v4i1.3759

Riyanto, H. R. B. (2020). Pembaruan Hukum Nasional Era 4.0. *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional, 9*(2), 161-181. http://dx.doi.org/10.33331/rechtsvinding.v9i2.455

Suhyana, F. A., Suseno, S., & Ramli, T. S. (2021). Transaksi Ilegal Menggunakan Kartu ATM Milik Orang Lain. *SIGn Jurnal Hukum, 2*(2), 138-156. https://doi.org/10.37276/sjh.v2i2.92

Sulisrudatin, N. (2018). Analisa Kasus Cybercrime Bidang Perbankan Berupa Modus Pencurian Data Kartu Kredit. *Jurnal Ilmiah Hukum Dirgantara, 9*(1), 26-39. https://doi.org/10.35968/jh.v9i1.296

Wiredarme, W., & Muttaqin, M. Z. (2022). Challenges and Strategies to Minimize Campaign Violations of Regional Head Election. *SIGn Jurnal Hukum, 4*(1), 58-71. https://doi.org/10.37276/sjh.v4i1.168

Wu, H., & Zheng, G. (2020). Electronic Evidence in the Blockchain Era: New Rules on Authenticity and Integrity. *Computer Law & Security Review, 36*, 1-12. https://doi.org/10.1016/j.clsr.2020.105401