Journal of Innovative and Creativity
Journal Homepage: https://joecy.org/index.php/joecy
e-mail: journaljoecy@gmail.com

Faculty of Education
University of Pahlawan Tuanku Tambusai
ISSN 2775-771X (Online)
ISSN 2962-570X (Printed)
6 (2) 2026, Page: 36704-36709

Pembuktian Digital Dalam Penyidikan Tindak Pidana Siber Di Indonesia

Fatimah Azzahra, Bella br Tarigan, Daffa Ananda, Nuzulsyah Romadhana, Fanny Aurellia
fira006073@gmail.com, tariganbella07@gmail.com, daffaabayadii@gmail.com, nuzulsyahramadhonalubis@gmail.com, fannyaurellia49@gmail.com

Published: June, 2026

ABSTRAK

Perkembangan teknologi informasi dan komunikasi telah mendorong meningkatnya tindak pidana siber di Indonesia. Dalam proses penegakan hukum terhadap kejahatan siber, pembuktian digital menjadi salah satu aspek penting dalam tahap penyidikan karena sebagian besar alat bukti berasal dari sistem elektronik dan data digital. Penelitian ini bertujuan untuk menganalisis pengaturan dan penerapan hukum mengenai pembuktian digital dalam proses penyidikan tindak pidana siber berdasarkan Kitab Undang-Undang Hukum Acara Pidana, Undang-Undang Informasi dan Transaksi Elektronik, dan Peraturan Pemerintah Nomor 71 Tahun 2019, serta untuk mengetahui kendala yang dihadapi penyidik dalam penggunaan alat bukti digital di Indonesia. Metode penelitian yang digunakan adalah penelitian hukum normatif dengan pendekatan perundang-undangan dan pendekatan konseptual.

Hasil penelitian menunjukkan bahwa alat bukti digital telah diakui sebagai alat bukti hukum yang sah melalui Undang-Undang Informasi dan Transaksi Elektronik sebagai perluasan alat bukti yang diatur dalam KUHAP. Selain itu, PP Nomor 71 Tahun 2019 memperkuat aspek keandalan dan keamanan sistem elektronik dalam mendukung proses pembuktian. Namun, dalam praktiknya penyidik masih menghadapi berbagai kendala, seperti keterbatasan sumber daya manusia di bidang digital forensik, keterbatasan sarana dan prasarana, kesulitan memperoleh alat bukti digital, serta hambatan yurisdiksi dalam tindak pidana siber lintas negara. Oleh karena itu, diperlukan penguatan regulasi, peningkatan kapasitas penyidik, dan pengembangan teknologi digital forensik guna meningkatkan efektivitas penegakan hukum terhadap tindak pidana siber di Indonesia.

Kata Kunci: **Pembuktian Digital, Tindak Pidana Siber, Penyidikan, Bukti Elektronik, Hukum Acara Pidana.**

Abstract

The development of information and communication technology has contributed to the increasing number of cybercrimes in Indonesia. In the process of law enforcement against cybercrime, digital evidence plays an essential role during the investigation stage because most evidence originates from electronic systems and digital data. This study aims to analyze the legal regulation and implementation of digital evidence in the investigation process of cybercrime based on the Criminal Procedure Code, the Law on Electronic Information and Transactions, and Government Regulation Number 71 of 2019, as well as to identify the obstacles faced by investigators in the use of digital evidence in Indonesia.

This research employs a normative legal research method using statutory and conceptual approaches. The results show that digital evidence has been recognized as legally valid evidence through the Law on Electronic Information and Transactions as an extension of the evidentiary system regulated under the Criminal Procedure Code. Furthermore, Government Regulation Number 71 of 2019 strengthens the reliability and security aspects of electronic systems in supporting the evidentiary process. However, investigators still encounter several challenges, including limited expertise in digital forensics, inadequate facilities and infrastructure, difficulties in obtaining digital evidence, and jurisdictional barriers in transnational cybercrime cases. Therefore, strengthening legal regulations, improving investigators' capabilities, and developing digital forensic technology are necessary to enhance the effectiveness of law enforcement against cybercrime in Indonesia.

Keywords: Digital Evidence, Cybercrime, Investigation, Electronic Evidence, Criminal Procedure Law.

© The Author(s). 2021 Open Access This article is licensed under a Creative Commons Atibution 4.0 International License, which permits 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 licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan yang signifikan dalam berbagai aspek kehidupan masyarakat. Pemanfaatan internet dan sistem elektronik yang semakin luas memberikan kemudahan dalam aktivitas ekonomi, pendidikan, pemerintahan, dan komunikasi. Namun, di samping memberikan manfaat, perkembangan teknologi tersebut juga memunculkan berbagai bentuk kejahatan baru yang dikenal sebagai tindak pidana siber (cybercrime).

Tindak pidana siber merupakan kejahatan yang dilakukan dengan memanfaatkan teknologi informasi, jaringan komputer, maupun sistem elektronik sebagai sarana atau sasaran tindak pidana.[1]

Perkembangan tindak pidana siber di Indonesia menunjukkan peningkatan yang cukup signifikan seiring dengan meningkatnya penggunaan teknologi digital. Berbagai bentuk tindak pidana siber yang sering terjadi antara lain penipuan daring (online fraud), peretasan (hacking), pencurian data pribadi, penyebaran informasi palsu (hoax), pencemaran nama baik melalui media elektronik, serta berbagai bentuk penyalahgunaan sistem elektronik lainnya. Karakteristik tindak pidana siber yang dilakukan melalui media elektronik menyebabkan proses pembuktian menjadi lebih kompleks dibandingkan dengan tindak pidana konvensional karena sebagian besar alat bukti yang digunakan berbentuk data elektronik atau digital.

Pembuktian merupakan salah satu unsur penting dalam proses penegakan hukum pidana. Dalam sistem hukum acara pidana Indonesia, alat bukti yang sah diatur dalam Pasal 184 ayat (1) Kitab Undang-Undang Hukum Acara Pidana (KUHAP), yaitu keterangan saksi, keterangan ahli, surat, petunjuk, dan keterangan terdakwa. Akan tetapi, perkembangan teknologi informasi menuntut adanya perluasan terhadap alat bukti yang dapat digunakan dalam proses pembuktian. Oleh karena itu, melalui Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024, Informasi Elektronik dan Dokumen Elektronik diakui sebagai alat bukti hukum yang sah.[2]

Keberadaan alat bukti digital memiliki peranan yang sangat penting dalam penyidikan tindak pidana siber karena sebagian besar aktivitas kejahatan meninggalkan jejak digital yang tersimpan dalam perangkat elektronik maupun sistem komputer. Bukti digital dapat berupa surat elektronik (email), rekaman percakapan elektronik, data transaksi elektronik, rekaman CCTV digital, hingga berbagai data yang tersimpan dalam komputer dan telepon seluler. Oleh karena itu, diperlukan metode dan prosedur khusus melalui digital forensik untuk memastikan keaslian, integritas, dan validitas alat bukti digital yang digunakan dalam proses hukum.

Selain diatur dalam Undang-Undang Informasi dan Transaksi Elektronik, pengaturan mengenai sistem elektronik dan transaksi elektronik juga diperkuat melalui Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Peraturan tersebut memberikan dasar hukum mengenai penyelenggaraan sistem elektronik yang andal dan aman sehingga dapat mendukung proses pembuktian digital dalam penegakan hukum terhadap tindak pidana siber.

Beberapa penelitian terdahulu telah membahas mengenai alat bukti elektronik dan tindak pidana siber dalam perspektif hukum pidana. Namun, sebagian besar penelitian tersebut lebih menitikberatkan pada kedudukan alat bukti elektronik dalam proses peradilan pidana secara umum. Sementara itu, kajian yang secara khusus membahas pengaturan pembuktian digital dalam tahap penyidikan berdasarkan KUHAP, Undang-Undang Informasi dan Transaksi Elektronik, serta Peraturan Pemerintah Nomor 71 Tahun 2019, beserta kendala yang dihadapi penyidik dalam penggunaannya, masih relatif terbatas. Oleh karena itu, penelitian ini penting dilakukan untuk memberikan pemahaman yang lebih komprehensif mengenai pembuktian digital dalam penyidikan tindak pidana siber di Indonesia.

Berdasarkan uraian tersebut, penelitian ini bertujuan untuk menganalisis pengaturan dan penerapan hukum mengenai pembuktian digital dalam proses penyidikan tindak pidana siber berdasarkan KUHAP, Undang-Undang Informasi dan Transaksi Elektronik, dan Peraturan Pemerintah Nomor 71 Tahun 2019, serta untuk mengetahui kendala yang dihadapi penyidik dalam penggunaan alat bukti digital pada tindak pidana siber di Indonesia.

METODE PENELITIAN

Penelitian ini menggunakan metode penelitian hukum normatif dengan pendekatan perundang-undangan (statute approach) dan pendekatan konseptual (conceptual approach). Bahan hukum yang digunakan terdiri atas bahan hukum primer, yaitu Kitab Undang-Undang Hukum Acara Pidana (KUHAP), Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, serta Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Selain

itu, penelitian ini juga menggunakan bahan hukum sekunder berupa buku, jurnal ilmiah, dan hasil penelitian yang berkaitan dengan pembuktian digital dan tindak pidana siber, serta bahan hukum tersier berupa kamus hukum dan ensiklopedia hukum. Pengumpulan bahan hukum dilakukan melalui studi kepustakaan (library research), sedangkan analisis bahan hukum dilakukan secara kualitatif dengan metode deskriptif-analitis.

HASIL DAN PEMBAHASAN

Pengaturan dan penerapan hukum mengenai pembuktian digital dalam proses penyidikan tindak pidana siber berdasarkan Kitab Undang-Undang Hukum Acara Pidana, Undang-Undang Informasi dan Transaksi Elektronik, dan Peraturan Pemerintah Nomor 71 Tahun 2019 di Indonesia

Pembuktian merupakan salah satu unsur penting dalam proses peradilan pidana karena berfungsi untuk menentukan ada atau tidaknya suatu tindak pidana serta keterlibatan seseorang dalam tindak pidana tersebut. Dalam hukum acara pidana Indonesia, alat bukti yang sah diatur dalam Pasal 184 ayat (1) KUHAP yang terdiri atas keterangan saksi, keterangan ahli, surat, petunjuk, dan keterangan terdakwa.[3]Namun, KUHAP belum mengatur secara khusus mengenai alat bukti digital karena disusun pada saat perkembangan teknologi informasi belum berkembang sebagaimana saat ini.

Perkembangan teknologi informasi telah melahirkan berbagai bentuk kejahatan siber yang dilakukan melalui media elektronik. Kondisi tersebut menuntut adanya pengakuan terhadap alat bukti digital sebagai sarana pembuktian dalam proses penegakan hukum. Untuk menjawab kebutuhan tersebut, pemerintah membentuk Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024. Melalui Pasal 5 ayat (1) UU ITE ditegaskan bahwa Informasi Elektronik dan/atau Dokumen Elektronik beserta hasil cetaknya merupakan alat bukti hukum yang sah.[4]

Pengakuan terhadap alat bukti elektronik tersebut merupakan perluasan dari alat bukti yang diatur dalam KUHAP. Hal ini ditegaskan dalam Pasal 5 ayat (2) UU ITE yang menyatakan bahwa Informasi Elektronik dan/atau Dokumen Elektronik merupakan perluasan dari alat bukti yang sah sesuai dengan hukum acara yang berlaku di Indonesia.[3] Dengan demikian, alat bukti digital memiliki kekuatan pembuktian yang dapat digunakan dalam proses penyidikan, penuntutan, maupun pemeriksaan di persidangan.

Selain itu, Pasal 44 UU ITE juga mengatur bahwa alat bukti dalam penyidikan, penuntutan, dan pemeriksaan perkara di bidang teknologi informasi dapat berupa alat bukti sebagaimana diatur dalam peraturan perundang-undangan serta alat bukti elektronik berupa Informasi Elektronik dan/atau Dokumen Elektronik.[4] Ketentuan tersebut menunjukkan bahwa alat bukti digital memiliki kedudukan yang penting dalam pengungkapan tindak pidana siber karena sebagian besar aktivitas pelaku meninggalkan jejak elektronik yang dapat digunakan sebagai sarana pembuktian.

Pengaturan mengenai pembuktian digital juga diperkuat melalui Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Peraturan ini mengatur penyelenggaraan sistem elektronik yang andal, aman, dan bertanggung jawab sehingga dapat menjamin keutuhan, keaslian, serta ketersediaan data elektronik yang digunakan sebagai alat bukti dalam proses hukum.[5] Keandalan sistem elektronik menjadi aspek penting karena validitas alat bukti digital sangat bergantung pada integritas data yang diperoleh.

Dalam praktik penyidikan tindak pidana siber, pembuktian digital dilakukan melalui proses digital forensik. Digital forensik merupakan metode ilmiah yang digunakan untuk memperoleh, mengamankan, memeriksa, menganalisis, dan menyajikan data elektronik agar dapat digunakan sebagai alat bukti yang sah di hadapan hukum.[6] Melalui proses tersebut, penyidik dapat mengidentifikasi jejak digital pelaku, mengungkap modus operandi kejahatan, serta memperoleh informasi yang relevan untuk membuktikan terjadinya tindak pidana siber.

Penerapan pembuktian digital dalam penyidikan tindak pidana siber umumnya dilakukan melalui pemeriksaan perangkat elektronik seperti komputer, telepon seluler, media penyimpanan data, surat elektronik (email), rekaman CCTV digital, riwayat transaksi elektronik, maupun aktivitas dalam jaringan internet. Hasil pemeriksaan tersebut kemudian dianalisis oleh penyidik dan dapat

diperkuat dengan keterangan ahli digital forensik untuk menjamin keabsahan alat bukti yang digunakan dalam proses peradilan pidana.

Berdasarkan uraian tersebut, dapat diketahui bahwa pembuktian digital memiliki kedudukan yang sangat penting dalam penyidikan tindak pidana siber. Keberadaan UU ITE dan PP Nomor 71 Tahun 2019 telah memberikan dasar hukum yang kuat bagi penggunaan alat bukti digital sebagai sarana pembuktian. Dengan demikian, pembuktian digital menjadi instrumen yang sangat penting dalam mendukung efektivitas penegakan hukum terhadap tindak pidana siber di Indonesia.

Kendala yang Dihadapi Penyidik dalam Penggunaan Alat Bukti Digital pada Tindak Pidana Siber di Indonesia

Perkembangan teknologi informasi telah mendorong peningkatan tindak pidana siber dengan berbagai modus operandi yang semakin kompleks. Kondisi tersebut menuntut penyidik untuk mampu memperoleh, mengolah, dan menganalisis alat bukti digital secara efektif. Namun, dalam praktiknya penggunaan alat bukti digital pada penyidikan tindak pidana siber masih menghadapi berbagai kendala yang mempengaruhi efektivitas penegakan hukum. Kendala tersebut berasal dari faktor internal maupun eksternal yang berkaitan dengan kemampuan sumber daya manusia, sarana pendukung, regulasi hukum, hingga karakteristik tindak pidana siber yang bersifat lintas batas negara.[5]

1. Kendala Internal Penyidikan
2. Keterbatasan kemampuan penyidik di bidang teknologi informasi dan digital forensik

Salah satu hambatan utama dalam penyidikan tindak pidana siber adalah keterbatasan kemampuan penyidik dalam memahami teknologi informasi dan digital forensik. Tidak semua penyidik memiliki kompetensi teknis terkait identifikasi, pengamanan, ekstraksi, maupun analisis alat bukti digital. Padahal, penanganan alat bukti elektronik memerlukan prosedur khusus agar keaslian dan integritas data tetap terjaga selama proses penyidikan berlangsung. Kurangnya kemampuan teknis tersebut berpotensi menyebabkan kesalahan dalam pengelolaan alat bukti sehingga mempengaruhi nilai pembuktian di proses hukum.

Selain itu, perkembangan teknologi yang cepat menuntut penyidik untuk terus memperbarui kemampuan dan pengetahuan terkait metode kejahatan siber yang semakin kompleks. Oleh karena itu, pelatihan berkelanjutan di bidang digital forensik menjadi kebutuhan penting bagi aparat penegak hukum.

a. Tingginya beban kerja penyidik

Banyaknya perkara yang ditangani menyebabkan penyidik tidak dapat fokus pada penanganan tindak pidana siber. Dalam praktiknya, penyidik sering menangani berbagai jenis perkara di luar kejahatan siber sehingga proses pengumpulan dan analisis alat bukti digital menjadi kurang optimal. Tingginya beban kerja tersebut berdampak pada lambatnya proses penyidikan dan berpotensi menghambat pengungkapan tindak pidana.[6]

b. Keterbatasan sarana dan infrastruktur teknologi

Penyidikan tindak pidana siber membutuhkan perangkat teknologi dan alat forensik digital yang memadai. Namun, keterbatasan fasilitas pendukung menyebabkan proses pelacakan dan analisis bukti digital sering dilakukan secara manual. Kondisi ini berpotensi memperlambat penyidikan serta meningkatkan risiko hilangnya data penting yang dibutuhkan dalam pembuktian.

Keterbatasan perangkat lunak forensik, sistem pengolahan data, dan jaringan komunikasi yang mendukung pertukaran informasi juga menjadi hambatan dalam penanganan kasus siber. Oleh karena itu, peningkatan infrastruktur teknologi menjadi aspek penting dalam memperkuat efektivitas penyidikan tindak pidana siber.

3. Kendala Eksternal Penyidikan

a. Kesulitan memperoleh dan mempertahankan alat bukti digital

Bukti digital memiliki karakteristik yang mudah berubah, dihapus, dipindahkan, maupun dimanipulasi. Kondisi tersebut menyebabkan penyidik mengalami kesulitan memperoleh bukti yang cukup untuk mendukung proses pembuktian. Apabila bukti yang diperoleh tidak memenuhi standar

pembuktian, maka proses penyidikan dapat mengalami hambatan bahkan dihentikan.

Selain itu, sifat bukti digital yang sementara (*volatile data*) mengharuskan penyidik melakukan tindakan cepat karena keterlambatan dapat menyebabkan hilangnya informasi penting.

c. Kurangnya koordinasi antar lembaga penegak hukum

Penyidikan tindak pidana siber memerlukan kerja sama berbagai lembaga seperti Polri, Kominfo, BSSN, dan instansi terkait lainnya. Namun, koordinasi antarlembaga masih menghadapi kendala berupa belum adanya sistem kerja terpadu, tumpang tindih kewenangan, dan kurangnya protokol operasional yang baku. Kondisi tersebut menyebabkan proses pertukaran data dan penanganan kasus berjalan kurang efektif sehingga memperlambat proses penyidikan.

d. Perbedaan yurisdiksi hukum antar negara

Tindak pidana siber sering melibatkan pelaku, korban, server, atau infrastruktur digital yang berada di berbagai negara. Hal ini menimbulkan hambatan terkait yurisdiksi hukum dan kerja sama internasional. Perbedaan pengaturan hukum antar negara dapat menyulitkan proses ekstradisi pelaku maupun permintaan data dari otoritas asing. Indonesia masih menghadapi kendala dalam mekanisme *Mutual Legal Assistance (MLA)* yang membutuhkan waktu relatif lama sehingga memperlambat proses pengumpulan alat bukti digital lintas negara.

e. Penggunaan teknologi anonimisasi oleh pelaku

Pelaku tindak pidana siber umumnya menggunakan teknologi seperti *Virtual Private Network* (VPN), enkripsi, akun anonim, maupun identitas palsu untuk menyembunyikan jejak digital. Teknologi tersebut menyebabkan proses pelacakan identitas pelaku menjadi lebih sulit dilakukan oleh penyidik.

f. Keterbatasan regulasi hukum terhadap perkembangan teknologi

Perkembangan teknologi informasi berlangsung lebih cepat dibandingkan perkembangan regulasi hukum. Meskipun UU ITE telah memberikan dasar hukum mengenai alat bukti elektronik, pengaturan tersebut dinilai belum sepenuhnya mampu mengakomodasi perkembangan kejahatan siber modern seperti *ransomware, deepfake,* maupun teknologi berbasis *blockchain.*

KESIMPULAN

Berdasarkan hasil penelitian, dapat disimpulkan bahwa pengaturan mengenai pembuktian digital dalam proses penyidikan tindak pidana siber di Indonesia telah memiliki dasar hukum yang cukup kuat melalui Kitab Undang-Undang Hukum Acara Pidana (KUHAP), Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, serta Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Informasi Elektronik dan Dokumen Elektronik telah diakui sebagai alat bukti hukum yang sah dan merupakan perluasan dari alat bukti yang diatur dalam KUHAP. Dalam praktik penyidikan tindak pidana siber, pembuktian digital dilakukan melalui proses digital forensik untuk menjamin keaslian, integritas, dan keabsahan alat bukti elektronik yang digunakan dalam proses peradilan pidana.

Selain itu, penyidik masih menghadapi berbagai kendala dalam penggunaan alat bukti digital, baik yang berasal dari faktor internal maupun eksternal. Kendala internal meliputi keterbatasan kemampuan penyidik di bidang teknologi informasi dan digital forensik, tingginya beban kerja, serta keterbatasan sarana dan prasarana pendukung. Sementara itu, kendala eksternal meliputi kesulitan memperoleh dan mempertahankan alat bukti digital, kurangnya koordinasi antar lembaga, perbedaan yurisdiksi hukum antar negara, penggunaan teknologi anonimisasi oleh pelaku, serta perkembangan teknologi yang lebih cepat dibandingkan regulasi hukum. Oleh karena itu, diperlukan peningkatan kapasitas sumber daya manusia, penguatan regulasi, pengembangan teknologi digital forensik, dan peningkatan kerja sama antar lembaga maupun antar negara guna mendukung efektivitas penegakan hukum terhadap tindak pidana siber di Indonesia.

DAFTAR PUSTAKA

Arief, Barda Nawawi. *Tindak Pidana Mayantara (Cyber Crime): Perkembangan Kajian Cyber Crime di Indonesia.* Jakarta: RajaGrafindo Persada, 2006.

Makarim, Edmon. *Pengantar Hukum Telematika*. Jakarta: Rajawali Pers, 2005. Mansur, Didik M. Arief dan Elisatris Gultom. Cyber Law: *Aspek Hukum Teknologi Informasi. Bandung*: Refika Aditama, 2009.

Maskun. *Kejahatan Siber (Cyber Crime):* Suatu Pengantar. Jakarta: Kencana, 2013. Muthmainnah. *Kendala-Kendala Penyidikan dalam Memperoleh Alat Bukti Tindak Pidana Perjudian Bola Melalui Internet* (Studi di Polrestabes Surabaya). Malang: Fakultas Hukum Universitas Brawijaya, 2014.

Sitompul, Josua. *Cyberspace, Cybercrimes, Cyberlaw: Tinjauan Aspek Hukum Pidana.* Jakarta: PT Tatanusa, 2012.

Wibowo, Muhammad Singgih Imam, Akhmad Munawar, dan Hidayatullah. *"Kendala Teknis dan Hukum dalam Proses Penyidikan Tindak Pidana Siber di Indonesia."* Rewang Rencang: Jurnal Hukum Lex Generalis, Vol. 5, No. 7, 2024.

Indonesia. Kitab Undang-Undang Hukum Acara Pidana.

Indonesia. Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Indonesia. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.