

PERKEMBANGAN ALAT BUKTI ELEKTRONIK HASIL PERETASAN (HACKER) SEBAGAI ALAT BUKTI DALAM TINDAK PIDANA

Trisnawati ^{1*}, Shofia Hanifah ²

^{1*,2} Program Studi Hukum, Fakultas Ilmu Sosial dan Politik, Universitas Tidar

DOI: 10.62567/micjo.v1i3.162

Article info:

Submitted: 12/06/24

Accepted: 16/07/24

Published: 30/07/24

Abstract

One of them can prove a criminal offense through electronic evidence. A regulation that regulates the evidence used is still valid in terms of proving any crime that requires digital evidence. In its development, electronic evidence is regulated in Article 5 paragraph (1) of the ITE Law that Electronic Information and / or Electronic Documents and / or their printouts are valid legal evidence. However, regarding the expansion of the types of electronic evidence, it is not explained in detail, including evidence of wiretapping results, which is still vague, because wiretapping itself is more considered a harmful criminal act. The data used in this study were obtained from various literatures relevant to the research topic. This research is descriptive in nature, namely describing the position of electronic evidence according to Indonesian criminal law. In this research, aspects of validity and evidentiary power by using electronic evidence that is valid according to the law are reviewed. Data is obtained from various literatures relevant to this research.

Keywords : progress, wiretapping, evidence.

Abstrak

Pembuktian suatu tindak pidana salah satunya dapat melalui bukti alat elektronik. Suatu peraturan yang mengatur alat bukti yang digunakan masih berlaku dalam hal pembuktian kejahatan apapun yang membutuhkan bukti secara digital. Pada perkembangannya alat bukti elektronik diatur dalam Pasal 5 ayat (1) UU ITE bahwa Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah. Namun, terkait perluasan jenis alat bukti elektronik tidak dijelaskan secara rinci termasuk alat bukti hasil penyadapan masih samar, sebab penyadapan sendiri lebih dianggap sebagai tindakan kriminal yang merugikan. Data yang diperoleh dalam penelitian ini dikumpulkan dari berbagai sumber literatur yang berkaitan dengan tema penelitian. Penelitian ini memiliki pendekatan deskriptif yang bertujuan untuk menjelaskan posisi alat bukti elektronik dalam kerangka hukum pidana di Indonesia. Penelitian ini meneliti aspek keabsahan dan kekuatan pembuktian menggunakan alat bukti elektronik yang sah menurut hukum. Data dikumpulkan dari berbagai literatur yang relevan dengan penelitian ini.

Kata Kunci : perkembangan, penyadapan, alat bukti.

1. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah mengubah banyak hal dalam berbagai bidang kehidupan, termasuk dalam konteks hukum. Transformasi digital ini telah mempengaruhi cara-cara penegakan hukum dilakukan, khususnya dalam pengakuan dan

penggunaan alat bukti elektronik (Hengki Irawan, 2024). Alat bukti elektronik ini mencakup data yang tersimpan dalam perangkat digital, komunikasi melalui email, rekaman CCTV, hingga bukti yang diperoleh melalui peretasan (hacker)(Cahyadi, 2021). Perkembangan ini mencerminkan betapa pentingnya teknologi dalam mendukung proses hukum yang modern dan efisien.

Perkembangan alat bukti elektronik hasil peretasan (hacker) dalam proses penegakan hukum semakin meningkat seiring dengan perkembangan teknologi. Dalam beberapa tahun terakhir, pemerintah telah mengeluarkan undang-undang yang lebih ketat mengenai kejahatan *cybercrime* dan peretasan, seperti Undang-Undang Nomor 9 tahun 2016 tentang “Informasi dan Transaksi Elektronik (ITE)” (Oktaviani, 2023). Undang-undang ini memberikan dasar hukum yang lebih jelas dan efektif dalam menghadapi kejahatan *cybercrime*.

Dalam konteks penegakan hukum, bukti elektronik memiliki peran yang semakin vital. Dokumen elektronik dan bukti digital kini telah diakui memiliki kedudukan hukum yang setara dengan dokumen kertas. Misalnya, dalam kegiatan e-commerce, kontrak atau transaksi yang dilakukan secara elektronik dianggap sah dan dapat dijadikan alat bukti di pengadilan. Pengakuan ini tercermin dalam berbagai peraturan perundang-undangan di banyak negara yang mengakomodasi bukti elektronik sebagai bagian dari sistem hukum mereka. Hal ini tidak hanya mempercepat proses hukum tetapi juga mengurangi ketergantungan pada dokumen fisik yang rentan terhadap kerusakan atau pemalsuan.

Namun, penggunaan bukti elektronik tidak terlepas dari berbagai tantangan, terutama terkait dengan aspek keamanan dan legalitas. Bukti elektronik yang diperoleh melalui peretasan menimbulkan dilema etis dan hukum. Di satu sisi, bukti tersebut bisa sangat relevan dan krusial dalam mengungkap kebenaran atau kejahatan tertentu. Di sisi lain, metode perolehannya yang ilegal menimbulkan pertanyaan tentang validitas dan bisa jadi melanggar hak privasi individu atau entitas yang menjadi korban peretasan. Oleh karena itu, pengadilan sering kali harus mempertimbangkan apakah bukti yang diperoleh secara ilegal dapat diterima atau tidak.

Dalam beberapa kasus, alat bukti elektronik yang diperoleh dari peretasan dapat menjadi bukti yang kuat dalam proses hukum. Misalnya, jika seorang hacker berhasil mengakses sistem komputer dan mencuri informasi pribadi, oleh karena itu alat bukti elektronik yang dimaksud bisa digunakan untuk bukti bahwa kejahatan telah terjadi. Selain itu, alat bukti elektronik juga dapat digunakan untuk mengidentifikasi pelaku kejahatan dan memantau aktivitas mereka. Namun, perkembangan alat bukti elektronik hasil peretasan juga memiliki beberapa tantangan. Salah satu tantangan adalah bagaimana memastikan keamanan dan integritas alat bukti elektronik tersebut.

Dalam penelitian ini, kita akan membahas perkembangan alat bukti elektronik hasil peretasan sebagai alat bukti dalam tindak pidana. Kita akan meneliti bagaimana alat bukti elektronik tersebut digunakan dalam proses hukum dan bagaimana tantangan yang dihadapi dalam penggunaannya. Kita juga akan membahas bagaimana undang-undang dan kebijakan yang relevan dapat membantu dalam menghadapi kejahatan *cybercrime* dan memastikan keamanan alat bukti elektronik.

2. METODE PENELITIAN

Fokus penelitian ini menggunakan hukum normatif dengan menggali doktrin dan asas hukum, termasuk pembahasan perbandingan hukum dan sejarah hukum. Peneliti bertujuan untuk memperoleh pemahaman komprehensif mengenai kedudukan peralatan elektronik dan alat bukti, dengan menggunakan pendekatan seperti pendekatan perundang-undangan dan

pendekatan sejarah. Hal ini memungkinkan dilakukannya penelaahan terhadap berbagai peraturan hukum yang menjadi tema sentral penelitian.

3. HASIL DAN PEMBAHASAN

A. Perkembangan Alat Bukti Elektronik di Indonesia

Sebelum UU ITE diberlakukan, alat bukti elektronik telah diakui dalam beberapa undang-undang, seperti UU No. 8 Tahun 1997 tentang “Dokumen Perusahaan”, UU No. 15 Tahun 2003 tentang “Pemberantasan Tindak Pidana Terorisme”, UU No. 15 Tahun 2003 tentang “Tindak Pidana Pencucian Uang”, UU No. 20 Tahun 2001 tentang “Pemberantasan Tindak Pidana Korupsi”, dan UU No. 30 Tahun 2002 tentang “Komisi Pemberantasan Korupsi”.

Perkembangan alat bukti dalam cybercrime di Indonesia telah mengalami perubahan besar sejalan dengan kemajuan teknologi informasi dan komunikasi. Dalam konteks penegakan hukum terkait kejahatan di ranah cyber, alat bukti elektronik memegang peranan penting dalam proses penyelidikan, penuntutan, dan pembuktian tindak pidana yang dilakukan secara digital. Berbagai jenis alat bukti elektronik, seperti data elektronik, pesan teks, email, rekaman suara, dan lain sebagainya, menjadi kunci dalam mengungkap dan menindak pelaku kejahatan cyber (Abdul Halim Barkatullah, 2019).

Salah satu aspek penting dalam perkembangan alat bukti di Indonesia adalah regulasi terkait penggunaan alat bukti elektronik dalam sistem peradilan. Undang-undang Informasi dan Transaksi Elektronik (ITE) menjadi pijakan hukum yang mengatur penggunaan alat bukti elektronik dalam penegakan hukum di Indonesia. Pasal 5 ayat (1) UU ITE menyatakan bahwa informasi elektronik, dokumen elektronik, dan hasil cetaknya memiliki kekuatan hukum yang sah sebagai pembuktian dalam pengadilan. Adanya dasar hukum ini, penggunaan alat bukti elektronik dalam kasus cybercrime menjadi lebih kuat dan terlindungi secara hukum¹.

Namun, perkembangan alat bukti elektronik hasil peretasan juga memiliki beberapa tantangan. Salah satu tantangan utama adalah bagaimana memastikan keamanan dan integritas alat bukti elektronik tersebut. Jika alat bukti elektronik tidak aman dan dapat disalahgunakan, maka dapat berakibat pada kegagalan proses hukum dan keadilan. Oleh karena itu, diperlukan upaya untuk mengembangkan teknologi yang lebih aman dan efektif dalam menghadapi kejahatan cybercrime.

Salah satu langkah yang bisa diambil adalah menerapkan teknik enkripsi untuk meningkatkan keamanan alat bukti elektronik. Enkripsi merupakan proses mengubah informasi menjadi kode yang tidak dapat dimengerti oleh individu atau pihak yang tidak memiliki otorisasi, sehingga dapat menjaga keamanan dan integritas data. Penerapan enkripsi bisa dilakukan pada level socket, yaitu dengan mengenkripsi data yang dikirim melalui jaringan, sehingga sulit untuk disadap atau diakses oleh pihak yang tidak berhak (Muhammad Farhan, Rajasa Syaefunaldi, Dhifa Ridho Dwiputra Hidayat, 2023).

Selain enkripsi, perkembangan teknologi forensik digital juga memegang peranan penting dalam menghadapi kejahatan cybercrime. Forensik digital melibatkan proses identifikasi, preservasi, analisis, dan presentasi data digital sebagai barang bukti yang sah secara hukum. Dengan adanya forensik digital, alat bukti elektronik dapat dianalisis dan diambil dengan cara yang tepat dan terpercaya, sehingga memastikan integritas dan keabsahan bukti tersebut di persidangan.

Dalam mendukung perkembangan alat bukti elektronik dalam kasus cybercrime, diperlukan juga peningkatan kapasitas sumber daya manusia di bidang teknologi informasi,

investigasi digital, dan penegakan hukum. Aparat penegak hukum perlu mempunyai pengetahuan serta keterampilan yang layak dalam menangani kasus cybercrime dan mengumpulkan alat bukti digital. Hal ini dapat dicapai melalui pelatihan forensik digital bagi penyidik dan aparat penegak hukum, kerjasama dengan lembaga pendidikan atau institusi terkait untuk mengembangkan kurikulum dan program pelatihan yang relevan, serta pertukaran informasi dan best practices dengan negara-negara lain dalam penanganan kasus cybercrime.

Lebih dari itu, pemerintah juga dapat meningkatkan kesadaran masyarakat tentang kejahatan cybercrime dan pentingnya mengamankan data pribadi. Dengan cara ini, masyarakat dapat lebih berhati-hati dalam menggunakan teknologi dan menghindari kejahatan cybercrime. Kampanye edukasi, sosialisasi, dan pelatihan terkait keamanan siber dapat dilakukan untuk meningkatkan kesadaran masyarakat.

Perkembangan alat bukti elektronik dalam dunia cybercrime di Indonesia juga membutuhkan kerjasama internasional yang erat. Mengingat sifat cybercrime yang lintas batas, diperlukan kerjasama dengan negara-negara lain dalam berbagi informasi, bukti, dan memfasilitasi proses hukum terkait kasus cybercrime. Indonesia telah menjalin kerjasama melalui perjanjian ekstradisi dan perjanjian bantuan hukum timbal balik merupakan dua aspek krusial dalam kerja sama internasional dalam bidang penegakan hukum.) dengan beberapa negara, yang memungkinkan negara-negara untuk saling berbagi informasi dan bukti dalam menangani kasus cybercrime (Dr. Abdul Halim Barkatullah, S.H., 2017).

Adanya perkembangan alat bukti di Indonesia dalam dunia cyber, diharapkan dapat meningkatkan efektivitas penegakan hukum, memberikan kepastian hukum, dan mengurangi dampak kejahatan siber yang semakin meningkat di era digital ini. Namun, upaya ini harus didukung oleh berbagai aspek, termasuk pengembangan teknologi yang aman, peningkatan kapasitas sumber daya manusia, kesadaran masyarakat, dan kerjasama internasional yang kuat.

B. Kedudukan Alat Bukti Elektronik Hasil Penyadapan (*Hacker*) Sebagai Alat Bukti Pidana

Suatu data yang diperoleh dari teknologi informasi elektronik seseorang disadap atau digunakan secara menyimpang, maka perilaku kriminal yang diakibatkan oleh dampak negatif berkembangnya aplikasi Internet disebut cybercrime. Dengan berjalannya waktu, perkembangan teknologi tanpa batas (*borderless*) menyebabkan perubahan dalam bidang sosial, budaya, ekonomi dan cara penegakan hukum secara signifikan yang berlangsung dengan cepat. (Departemen Komunikasi dan Informatika Republik Indonesia, 2007) Salah satu hal yang digunakan dalam permasalahan hukum dihadapkan dengan proses dan cara penegakan hukum yang dilaksanakan melalui sistem elektronik.

Dari pemahaman ini, meski alat bukti pidana didapatkan dari kejahatan yang mana mencakup hal-hal yang dilakukan sebagai dampak negatif internet termasuk segalanya pola menggunakan fasilitas ini internet sebagai pencurian data. Seorang *hacker* yang melakukan pembobolan data berdasarkan keilmuan dalam sistem komputer atau di bidang IT pada dasarnya dapat mengumpulkan segala bentuk informasi, mengakses file alat bukti yang dicari. Menurut Pasal 1 Ayat 1 dalam Undang-Undang Informasi dan Transaksi Elektronik Nomor 19 Tahun 2016, informasi elektronik didefinisikan sebagai satu atau sekelompok data elektronik yang mencakup berbagai bentuk seperti teks, suara, gambar, peta, denah, foto, serta data lainnya. Ini juga mencakup metode pertukaran data seperti Pertukaran Data Elektronik (EDI), email, telegraf, teleks, dan segala bentuk komunikasi elektronik lainnya. Termasuk di dalamnya adalah huruf, lambang, angka, kode akses, simbol, atau perforasi yang memiliki

makna penting dan dapat dimengerti oleh individu yang memiliki kemampuan untuk memahaminya.

Barang bukti digital yang diperoleh melalui aktivitas penyadapan oleh pihak yang tidak berwenang, seperti peretas, sering kali dianggap kontroversial di banyak yurisdiksi. Validitas dan efektivitas bukti-bukti tersebut sering menjadi bahan perdebatan dalam sistem hukum. Di beberapa negara, bukti yang diperoleh melalui cara yang melanggar hukum atau melanggar hukum (misalnya melalui peretasan) sering kali tidak dapat diterima di pengadilan. Namun, dalam beberapa kasus dan yurisdiksi, bukti tersebut masih dapat diterima jika pengadilan menganggap bahwa penggunaannya dibenarkan demi kepentingan keadilan, atau jika ada pandangan bahwa bukti tersebut penting demi kepentingan hukum dan keadilan. Hal ini sering kali menjadi titik balik dalam litigasi, di mana pengadilan harus mempertimbangkan perlunya penegakan hukum terhadap hak individu atas privasi dan keamanan data.

Sejalan dengan dengan pesatnya kemajuan teknologi dan hukum , beberapa ahli hukum telah mengadopsi aturan dan prosedur yang lebih masuk akal untuk menangani kasus-kasus yang menggunakan kemajuan pesat tersebut elektronik. Dalam bidang teknologi dan hukum, beberapa ahli hukum telah mengadopsi peraturan dan prosedur yang lebih masuk akal untuk menangani kasus-kasus yang menggunakan tanda tangan elektronik. Hal ini dapat mencakup kebijakan saat ini kebijakan untuk mengawasi, untuk mengawasi, melestarikan, dan memanfaatkan data elektronik serta penegakan hukum yang lebih ketat terhadap mereka yang terlibat dalam perdagangan gelap .melestarikan , dan memanfaatkan data elektronik serta penegakan hukum yang lebih ketat terhadap mereka yang melakukan perdagangan gelap .

Berdasarkan Putusan Mahkamah Konstitusi Nomor 20/PUU/XIV/2016 menerangkan bahwa setiap barang bukti elektronik dapat menjadi alat bukti yang sah ketika mendapati izin dari aparat penegak hukum ataupun pihak yang berwenang. Selain itu dalam Pasal 5 Undang-Undang ITE disebutkan.

Meninjau dari permasalahan yang kompleks mengenai alat bukti elektronik hasil penyadapan tanpa izin akan berantung dari jenis kasus yang dihadapi. Berdasarkan fakta lapangan terlebih dengan adanya permintaan penegak hukum agar melaporkan mengenai alat bukti termasuk dari hasil penyadapan untuk dilaporkan sehingga merubah status alat bukti elektronik hasil penyadapan menjadi alat bukti yang sah

4. KESIMPULAN

Perkembangan alat bukti digital di Indonesia diatur dalam Undang-Undang Informasi dan Transaksi Elektronik yang mengatur tentang penggunaan alat bukti elektronik dalam proses hukum. Bukti elektronik seperti aktivitas log, metadata, dan transfer bitcoin telah menjadi kunci dalam penyelidikan dan penuntutan kasus kejahatan dunia maya di Indonesia. Negara ini telah mengalami beberapa kasus kejahatan dunia maya tingkat tinggi, seperti peretasan server di Amerika Serikat dan pencurian data oleh peretas yang menyamar sebagai kurir e-niaga. Untuk mengatasi tantangan bukti digital, Indonesia telah mengembangkan undang-undang dan kebijakan, seperti perubahan Undang-Undang Informasi dan Transaksi Elektronik, untuk memberikan dasar hukum yang lebih jelas dalam menangani kejahatan dunia maya. Namun, memastikan keamanan dan integritas bukti elektronik masih merupakan tantangan yang signifikan.

Mengenai penggunaan bukti elektronik yang diperoleh dari intersepsi yang tidak sah, dapat diterimanya bukti tersebut tergantung pada keadaan spesifik dari setiap kasus dan undang-undang yang berlaku. Penggunaan alat bukti elektronik di pengadilan dapat

diperbolehkan apabila dipandang perlu demi kepentingan keadilan dan penegakan hukum. Putusan Mahkamah Konstitusi baru-baru ini telah memberikan pedoman diperbolehkannya alat bukti elektronik dalam proses hukum, dengan menekankan pentingnya mendapatkan izin dari aparat penegak hukum atau pihak yang berwenang. Kesimpulannya, pengembangan bukti elektronik dalam lanskap kejahatan dunia maya di Indonesia memerlukan pendekatan multi-sisi, termasuk peraturan hukum, perkembangan teknologi, peningkatan kapasitas, kesadaran masyarakat, dan kerja sama internasional. Seiring dengan kemajuan teknologi, penting bagi Indonesia untuk menyesuaikan undang-undang dan prosedurnya agar dapat secara efektif mengatasi tantangan kejahatan dunia maya dan memastikan proses hukum yang adil.

5. DAFTAR PUSTAKA

Buku

- Departemen Komunikasi dan Informatika Republik Indonesia. (2007). *Menuju Kepastian Hukum di Bidang : Informatika dan Transaksi Elektronik*.
- Dr. Abdul Halim Barkatullah, S.H., M. H. (2017). *Hukum Transaksi Elektronik di Indonesia: Sebagai Pedoman dalam Menghadapi Era Digital Bisnis e-Commerce di Indonesia* (M. H. Dr. Mulyani Zulaeha, S.H. (ed.); 1st ed.). Nusa Media.
- Abdul Halim Barkatullah. (2019). *Hukum Transaksi Elektronik di Indonesia: Sebagai Pedoman Dalam Menghadapi Era Digital Bisnis e-Commerce di Indonesia*. Nusamedia.
- Cahyadi, R. A. (2021). *Apa yang Harus Ditanyakan kepada Ahli Digital Forensics? (Panduan bagi Praktisi Hukum* (1st ed.). Deepublish.

Jurnal

- Hukum: Tren Dan Inovasi Di Era Digital. *Inovatif: Jurnal Penelitian Ilmu Sosial*, 4(2), 4. <https://doi.org/https://doi.org/10.31004/innovative.v4i2.9732>
- Muhammad Farhan, Rajasa Syaefunaldi, Dhifa Ridho Dwiputra Hidayat, A. U. H. (2023). Penerapan Hukum Dalam Menanggulangi Kejahatan Siber Penegakan Hukum Terhadap Tindak Pidana Siber. *Kultura: Jurnal Ilmu Hukum, Sosial, Dan Humaniora*, 1(6), 5. <https://doi.org/https://doi.org/10.572349/kultura.v1i6.569>
- Oktaviani, A. (2023). Alternatif Pidana Bagi Pelaku Tindak Pidana Peretasan Di Indonesia Dalam Undang-Undang Informasi Dan Transaksi Elektronik. *Novum: Jurnal Hukum*, 0(0), 4. <https://doi.org/https://doi.org/10.2674/novum.v0i0.50394>
- Takasya Angela Tanauw Khristanto. (2020). Kedudukan Hukum CCTV Sebagai Alat Bukti Elektronik Setelah Terbitnya Putusan Mahkamah Konstitusi Nomor 20/PUU-XIV/2016 Tanggal 07 September 2016. *Jurnal Hukum To-Ra*, 6(2), 55.