RISET :
Jurnal Ilmiah Multidisiplin Ilmu
Published by PT. Ahlal Publisher Nusantara, Indonesia
Volume 1 No 3 April 2026 E-ISSN : 3123-8475
Journal Homepage: https://jurnalriset.com/index.php/riset/index

Analisis Hukum Terhadap Penyalahgunaan Artificial Intelligence Dalam Kejahatan Siber

Auzahra Yusveralda Juinko Cinta Prasgita[1], M. Rian Adam Pratama[2], Satrya Hutama Alaniani T[3], Steven Fancius Simanjuntak[4], Rakha Valiant Mardinata[5], Wahyu Dwi Anggraeni Putri[6]

[1,2,3,4,5,6]Ilmu Hukum, Universitas Bhayangkara Surabaya, Jalan Ahmad Yani No. 114, Surabaya, Jawa Timur, Indonesia

Email : Wahyudwianggraeniputri@gmail.com

Article Info

Corresponding Author:
Penulis Korespondensi
✉Wahyudwianggraeniputri@gmail.com

History:
Submitted: 17-04-2026
Revised: 18-04-2026
Accepted: 20-04-2026

Keywords: Artificial Intelligence; Cybercrime; Legal Responsibility; Information Technology; Law.

Kata Kunci: Artificial Intelligence; Kejahatan Siber; Pertanggungjawaban Hukum; Teknologi Informasi; Hukum.

https://doi.org

Abstract

The development of information technology in the digital era has led to various innovations, one of which is Artificial Intelligence that provides convenience in many aspects of human life. However, the advancement of this technology also creates new legal problems, particularly in the form of increasingly complex cybercrime. The use of artificial intelligence enables system hacking, data theft, information manipulation, and digital fraud carried out automatically, which causes difficulties in law enforcement. The existing legal regulations in Indonesia have generally governed cybercrime through the Law on Electronic Information and Transactions and other related regulations, but they have not specifically regulated the misuse of Artificial Intelligence as a means of committing criminal acts. The purpose of this study is to analyze the legal regulation of the misuse of Artificial Intelligence in cybercrime and to examine the form of legal responsibility for perpetrators who use such technology. This research uses normative legal research with statutory, conceptual, and case approaches. The results show that the development of artificial intelligence technology creates complexity in law enforcement because the system can operate automatically and involve multiple parties. In principle, legal responsibility remains imposed on humans as perpetrators, either as developers, users, or parties who benefit from the use of the technology. Therefore, more adaptive legal regulations, stronger law enforcement, and improved digital literacy are needed in order to prevent the misuse of Artificial Intelligence in cybercrime and to ensure legal certainty for society.

Abstrak

Perkembangan teknologi informasi pada era digital telah melahirkan berbagai inovasi, salah satunya Artificial Intelligence yang memberikan kemudahan dalam berbagai bidang kehidupan. Namun, di sisi lain perkembangan teknologi tersebut juga menimbulkan permasalahan hukum baru, terutama dalam bentuk kejahatan siber yang semakin kompleks. Penggunaan kecerdasan buatan memungkinkan terjadinya peretasan sistem, pencurian data, manipulasi informasi, serta penipuan digital yang dilakukan secara otomatis sehingga menimbulkan kesulitan dalam penegakan hukum. Pengaturan hukum yang berlaku di Indonesia pada dasarnya telah mengatur mengenai kejahatan siber melalui Undang-Undang Informasi dan Transaksi Elektronik serta peraturan terkait lainnya, namun belum secara khusus mengatur mengenai penyalahgunaan Artificial Intelligence sebagai sarana dalam melakukan tindak pidana. Tujuan dari penulisan ini adalah untuk menganalisis pengaturan hukum terhadap penyalahgunaan Artificial Intelligence dalam kejahatan siber, serta untuk mengetahui bentuk pertanggungjawaban hukum terhadap pelaku yang menggunakan teknologi tersebut. Metode penelitian yang digunakan adalah penelitian hukum normatif dengan pendekatan perundang-undangan, konseptual, dan kasus. Hasil pembahasan menunjukkan bahwa perkembangan teknologi kecerdasan buatan menimbulkan kompleksitas dalam penegakan hukum karena sistem dapat bekerja secara otomatis dan melibatkan banyak pihak. Dalam hal ini, pertanggungjawaban hukum pada prinsipnya tetap dibebankan kepada manusia sebagai pelaku, baik sebagai pembuat, pengguna, maupun pihak yang memperoleh keuntungan dari penggunaan teknologi tersebut. Oleh karena itu, diperlukan pembaruan regulasi yang lebih adaptif, penguatan penegakan hukum, serta peningkatan literasi digital masyarakat agar penyalahgunaan Artificial Intelligence dalam kejahatan siber dapat dicegah dan kepastian hukum dapat terwujud.

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi pada era digital telah membawa perubahan besar dalam kehidupan masyarakat, termasuk dalam bidang hukum. Salah satu perkembangan teknologi yang paling pesat adalah Artificial Intelligence (AI), yaitu teknologi yang memungkinkan sistem komputer melakukan proses analisis, pembelajaran, dan pengambilan keputusan secara otomatis. Kemajuan teknologi ini memberikan manfaat dalam berbagai bidang, namun juga menimbulkan risiko baru dalam bentuk kejahatan siber (cybercrime) yang semakin kompleks. Cybercrime merupakan tindak pidana yang dilakukan dengan menggunakan komputer atau jaringan internet sebagai sarana maupun sasaran kejahatan, sehingga menimbulkan tantangan baru dalam penegakan hukum, terutama karena sifatnya yang lintas negara dan sulit dilacak (Widodo, 2019).

Perkembangan teknologi digital menyebabkan kejahatan tidak lagi terbatas pada ruang fisik, tetapi juga terjadi di ruang siber yang memerlukan pengaturan hukum yang lebih adaptif agar mampu memberikan kepastian hukum bagi masyarakat.

Widodo (2019) menjelaskan bahwa perkembangan teknologi informasi menyebabkan munculnya bentuk kejahatan baru yang tidak sepenuhnya dapat dijangkau oleh hukum pidana konvensional. Oleh karena itu, kebijakan hukum pidana harus terus diperbarui agar mampu mengantisipasi perkembangan teknologi yang semakin cepat. Hal ini menunjukkan bahwa hukum harus bersifat dinamis dan responsif terhadap perubahan sosial, termasuk dalam menghadapi perkembangan Artificial Intelligence yang semakin luas digunakan dalam kehidupan sehari-hari.

Perkembangan Artificial Intelligence juga meningkatkan risiko penyalahgunaan teknologi dalam kejahatan siber, seperti peretasan sistem, pencurian data pribadi, manipulasi informasi, dan penyebaran berita palsu. Teknologi kecerdasan buatan memungkinkan suatu sistem bekerja secara otomatis tanpa pengawasan langsung dari manusia, sehingga menimbulkan persoalan baru dalam penegakan hukum. Menurut penelitian yang dilakukan oleh Sari (2022). perkembangan teknologi digital menimbulkan ancaman baru terhadap keamanan data dan privasi masyarakat, sehingga diperlukan regulasi yang lebih jelas untuk melindungi masyarakat dari penyalahgunaan teknologi informasi.

Selain itu, perkembangan teknologi digital juga menimbulkan permasalahan dalam pertanggungjawaban hukum. Dalam hukum pidana, pertanggungjawaban diberikan kepada seseorang yang melakukan perbuatan melawan hukum dengan kesalahan. Namun, dalam kejahatan yang menggunakan Artificial Intelligence, sulit menentukan siapa yang harus bertanggung jawab karena sistem dapat bekerja secara otomatis. Nugraha (2021) menyatakan bahwa cybercrime memiliki karakteristik khusus, yaitu menggunakan teknologi tinggi, bersifat lintas negara, dan melibatkan banyak pihak, sehingga

membutuhkan konsep hukum yang lebih adaptif dibandingkan kejahatan konvensional.

Penelitian mengenai kejahatan siber telah banyak dilakukan sebelumnya, namun sebagian besar masih membahas cybercrime secara umum dan belum secara khusus mengkaji penyalahgunaan Artificial Intelligence dalam perspektif hukum pidana di Indonesia. Widodo (2019) meneliti kebijakan hukum pidana dalam penanggulangan cybercrime dan menyimpulkan bahwa regulasi yang ada belum sepenuhnya mampu mengantisipasi perkembangan teknologi informasi. Sari (2022) meneliti perlindungan hukum terhadap data pribadi dan menyatakan bahwa perkembangan teknologi membutuhkan pengaturan hukum yang lebih spesifik. Nugraha (2021) meneliti penegakan hukum terhadap cybercrime dan menyatakan bahwa hukum yang ada masih memiliki keterbatasan dalam menghadapi kejahatan berbasis teknologi tinggi. Berdasarkan penelitian-penelitian tersebut, dapat diketahui bahwa kajian mengenai cybercrime sudah banyak dilakukan, tetapi penelitian yang secara khusus membahas penyalahgunaan Artificial Intelligence dalam kejahatan siber di Indonesia masih terbatas. Oleh karena itu, penelitian ini memiliki kebaruan (novelty) karena mengkaji penyalahgunaan Artificial Intelligence dalam kejahatan siber serta pertanggungjawaban hukumnya dalam sistem hukum Indonesia.

Berdasarkan latar belakang tersebut, maka permasalahan dalam penelitian ini adalah bagaimana pengaturan hukum terhadap penyalahgunaan Artificial Intelligence dalam kejahatan siber di Indonesia, bagaimana pertanggungjawaban hukum terhadap pelaku yang menggunakan Artificial Intelligence dalam melakukan kejahatan siber, serta bagaimana upaya hukum yang dapat dilakukan untuk mencegah penyalahgunaan Artificial Intelligence dalam kejahatan siber. Penelitian ini bertujuan untuk menganalisis pengaturan hukum mengenai penyalahgunaan Artificial Intelligence dalam kejahatan siber, mengkaji pertanggungjawaban hukum terhadap pelaku, serta merumuskan upaya hukum yang dapat dilakukan untuk mencegah penyalahgunaan teknologi Artificial Intelligence agar dapat memberikan kepastian hukum dan perlindungan bagi masyarakat.

Penelitian ini menggunakan metode yuridis normatif dengan pendekatan perundang-undangan dan pendekatan konseptual. Pendekatan perundang-undangan dilakukan dengan menganalisis peraturan yang berkaitan dengan kejahatan siber dan teknologi informasi, sedangkan pendekatan konseptual digunakan untuk mengkaji teori hukum yang berkaitan dengan pertanggungjawaban pidana dan perkembangan teknologi digital. Data diperoleh melalui studi kepustakaan terhadap peraturan perundang-undangan, buku, dan artikel jurnal yang relevan.

Artikel ini disusun dalam beberapa bagian. Bagian pertama merupakan pendahuluan yang berisi latar belakang, kajian penelitian sebelumnya, rumusan masalah, tujuan penelitian, metode penelitian, dan sistematika penulisan. Bagian kedua membahas perkembangan Artificial

Intelligence dan kaitannya dengan kejahatan siber. Bagian ketiga membahas pengaturan hukum kejahatan siber di Indonesia. Bagian keempat membahas pertanggungjawaban hukum dalam penyalahgunaan Artificial Intelligence. Bagian kelima membahas upaya hukum dalam pencegahan penyalahgunaan Artificial Intelligence. Bagian terakhir merupakan kesimpulan dari penelitian.

PEMBAHASAN

1. Perkembangan Artificial Intelligence dan Kaitannya dengan Kejahatan Siber

Perkembangan teknologi digital telah membawa perubahan mendasar dalam berbagai aspek kehidupan, termasuk dalam bidang hukum dan keamanan. Artificial Intelligence (AI) sebagai salah satu bentuk kemajuan teknologi memungkinkan sistem komputer melakukan analisis data, pembelajaran, dan pengambilan keputusan secara otomatis. Kemampuan tersebut memberikan manfaat besar dalam bidang industri, komunikasi, dan keamanan, tetapi pada saat yang sama juga membuka peluang terjadinya kejahatan siber yang semakin kompleks. Kejahatan siber tidak lagi dilakukan secara konvensional, melainkan memanfaatkan teknologi yang mampu bekerja secara cepat, anonim, dan lintas negara (Rahmawati, 2017).

Perkembangan Artificial Intelligence menyebabkan pola kejahatan berubah dari yang bersifat manual menjadi otomatis. Pelaku dapat menggunakan sistem berbasis kecerdasan buatan untuk melakukan peretasan, pencurian data, atau manipulasi informasi dalam jumlah besar tanpa harus melakukan tindakan secara langsung. Kondisi ini menimbulkan kesulitan dalam penegakan hukum karena proses kejahatan tidak selalu melibatkan interaksi langsung antara pelaku dan korban. Hapsari dan Pambayun (2023) menyatakan bahwa cybercrime di era digital tidak hanya menimbulkan kerugian ekonomi, tetapi juga dapat mengancam stabilitas sosial dan keamanan negara apabila tidak diimbangi dengan sistem hukum yang memadai.

Dalam perspektif hukum, perkembangan teknologi yang sangat cepat sering kali tidak diikuti oleh perkembangan regulasi. Hal ini menyebabkan adanya kesenjangan antara kemajuan teknologi dan kemampuan hukum dalam mengaturnya. Artificial Intelligence yang mampu bekerja secara mandiri menimbulkan pertanyaan mengenai batas tanggung jawab hukum, terutama ketika suatu sistem melakukan tindakan yang merugikan tanpa perintah langsung dari manusia. Oleh karena itu, diperlukan kajian hukum yang lebih mendalam agar perkembangan teknologi tidak menimbulkan kekosongan norma yang dapat dimanfaatkan oleh pelaku kejahatan.

2. Pengaturan Hukum Kejahatan Siber di Indonesia

Pengaturan hukum mengenai kejahatan siber di Indonesia pada dasarnya telah diatur melalui Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016. Undang-undang

ini mengatur berbagai bentuk perbuatan yang dilarang dalam sistem elektronik, seperti akses ilegal, manipulasi data, penyebaran informasi palsu, dan penipuan melalui media elektronik. Namun, ketentuan tersebut disusun pada saat perkembangan teknologi belum sepesat sekarang, sehingga belum secara spesifik mengatur penggunaan Artificial Intelligence sebagai sarana dalam melakukan tindak pidana Ninggeding, 2023).

Dalam praktiknya, penggunaan Artificial Intelligence dalam kejahatan siber menimbulkan persoalan baru karena sistem dapat bekerja secara otomatis dan tidak selalu berada dalam kendali langsung pelaku. Hal ini menyebabkan kesulitan dalam menentukan unsur kesengajaan dan kesalahan dalam hukum pidana. Nugraha (2021) menyatakan bahwa karakteristik cybercrime yang bersifat lintas negara, anonim, dan menggunakan teknologi tinggi membutuhkan pendekatan hukum yang berbeda dengan kejahatan konvensional.

Selain itu, keberadaan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi menunjukkan bahwa negara mulai menyadari pentingnya perlindungan terhadap data digital. Namun, pengaturan tersebut masih bersifat umum dan belum secara khusus mengatur penggunaan Artificial Intelligence yang memanfaatkan big data dalam skala besar. Apabila tidak diatur secara jelas, penggunaan teknologi tersebut berpotensi melanggar hak privasi masyarakat. Oleh karena itu, diperlukan pembaruan hukum yang lebih spesifik agar regulasi yang ada mampu mengikuti perkembangan teknologi yang semakin cepat.

3. Bentuk Penyalahgunaan Artificial Intelligence dalam Kejahatan Siber

Artificial Intelligence dapat digunakan dalam berbagai bentuk kejahatan siber, antara lain peretasan sistem, pencurian data pribadi, manipulasi informasi, serta penipuan digital yang dilakukan secara otomatis. Kejahatan ini semakin sulit ditangani karena pelaku dapat menggunakan program yang mampu bekerja secara terus-menerus tanpa pengawasan langsung. Aini (2024) menjelaskan bahwa salah satu kendala dalam penegakan hukum cybercrime adalah sifat anonim pelaku dan mudahnya bukti digital dihapus atau diubah.

Selain itu, penggunaan Artificial Intelligence dalam media sosial memungkinkan penyebaran informasi palsu melalui sistem bot yang dapat membuat banyak akun secara otomatis. Penyebaran informasi yang tidak benar dalam jumlah besar dapat mempengaruhi opini publik dan bahkan menimbulkan gangguan terhadap stabilitas sosial dan politik. Sitanggang et al. (2024) menyatakan bahwa perkembangan teknologi digital menuntut adanya pengawasan yang lebih ketat karena kejahatan tidak hanya merugikan individu, tetapi juga dapat berdampak pada kepentingan negara.

Bentuk lain penyalahgunaan Artificial Intelligence adalah penggunaan sistem otomatis untuk melakukan penipuan online dan pencurian identitas. Teknologi ini memungkinkan pelaku

melakukan tindakan tanpa harus berada di lokasi yang sama dengan korban, sehingga proses pembuktian menjadi lebih sulit. Kondisi ini menunjukkan bahwa perkembangan teknologi tidak hanya menimbulkan jenis kejahatan baru, tetapi juga menimbulkan kesulitan baru dalam penegakan hukum.

4. Pertanggungjawaban Hukum dalam Penyalahgunaan Artificial Intelligence

Dalam hukum pidana, pertanggungjawaban diberikan kepada seseorang yang melakukan perbuatan melawan hukum dengan kesalahan. Namun, dalam kasus kejahatan yang menggunakan Artificial Intelligence, tidak selalu mudah menentukan siapa yang harus bertanggung jawab karena sistem dapat bekerja secara otomatis. Matondang (2025) menyatakan bahwa perkembangan teknologi menuntut adanya penyesuaian dalam konsep pertanggungjawaban hukum, karena kejahatan siber sering melibatkan lebih dari satu pihak.

Dalam penyalahgunaan Artificial Intelligence, pertanggungjawaban hukum dapat dibebankan kepada beberapa pihak, yaitu pembuat program, pengguna program, pemilik sistem, atau perusahaan yang memperoleh keuntungan dari penggunaan teknologi tersebut. Apabila Artificial Intelligence hanya digunakan sebagai alat, maka pertanggungjawaban tetap berada pada manusia sebagai pelaku. Namun, apabila sistem bekerja secara mandiri tanpa pengawasan langsung, maka diperlukan konsep pertanggungjawaban baru seperti strict liability atau corporate liability.

Analisis ini menunjukkan bahwa konsep pertanggungjawaban hukum yang ada saat ini belum sepenuhnya mampu menjawab permasalahan yang timbul akibat perkembangan teknologi kecerdasan buatan. Oleh karena itu, diperlukan pengaturan hukum yang lebih jelas agar tidak terjadi kekosongan norma dalam menentukan pihak yang harus bertanggung jawab.

5. Upaya Hukum dalam Pencegahan Penyalahgunaan Artificial Intelligence

Pencegahan penyalahgunaan Artificial Intelligence dalam kejahatan siber tidak dapat dilakukan hanya dengan menggunakan regulasi yang ada, tetapi memerlukan pembaruan hukum yang lebih adaptif. Judijanto (2025) menyatakan bahwa perkembangan teknologi digital selalu lebih cepat dibandingkan perkembangan hukum, sehingga negara harus secara berkala memperbarui regulasi agar mampu mengendalikan kejahatan siber.

Selain pembaruan regulasi, penegakan hukum juga harus diperkuat dengan meningkatkan kemampuan aparat dalam bidang forensik digital. Kejahatan siber memerlukan metode pembuktian yang berbeda dengan kejahatan konvensional, sehingga aparat penegak hukum harus memiliki kemampuan teknis yang memadai. Selain itu, kerja sama internasional juga diperlukan karena kejahatan siber sering dilakukan lintas negara.

Upaya pencegahan juga harus dilakukan melalui peningkatan literasi digital masyarakat. Masyarakat perlu memahami risiko penggunaan teknologi agar tidak mudah menjadi korban

kejahatan. Pendidikan keamanan digital, pengawasan terhadap penggunaan teknologi, serta penguatan sistem keamanan siber merupakan langkah penting untuk mencegah penyalahgunaan Artificial Intelligence di masa mendatang.

Dengan adanya pembaruan regulasi, penguatan penegakan hukum, dan peningkatan kesadaran masyarakat, diharapkan penyalahgunaan Artificial Intelligence dalam kejahatan siber dapat dikendalikan sehingga tujuan hukum untuk memberikan kepastian, keadilan, dan kemanfaatan dapat tercapai.

KESIMPULAN

Pengaturan hukum terhadap penyalahgunaan Artificial Intelligence dalam kejahatan siber di Indonesia pada dasarnya telah diatur melalui Undang-Undang Informasi dan Transaksi Elektronik serta peraturan perundang-undangan lain yang berkaitan dengan teknologi informasi, namun pengaturan tersebut belum secara khusus mengatur penggunaan Artificial Intelligence sebagai sarana dalam melakukan tindak pidana. Hal ini menimbulkan kekosongan norma hukum yang berpotensi menimbulkan ketidakpastian dalam penegakan hukum, terutama dalam menentukan pertanggungjawaban apabila kejahatan dilakukan melalui sistem yang bekerja secara otomatis.

Pertanggungjawaban hukum dalam penyalahgunaan Artificial Intelligence pada prinsipnya tetap dibebankan kepada manusia sebagai pelaku, baik sebagai pembuat, pengguna, maupun pihak yang memperoleh keuntungan dari penggunaan teknologi tersebut. Namun, perkembangan teknologi kecerdasan buatan yang semakin pesat menunjukkan bahwa konsep pertanggungjawaban hukum yang ada saat ini belum sepenuhnya mampu mengakomodasi karakteristik kejahatan siber yang bersifat kompleks, lintas negara, dan berbasis sistem otomatis. Oleh karena itu, diperlukan pengaturan hukum yang lebih spesifik dan adaptif agar dapat memberikan kepastian hukum serta perlindungan bagi masyarakat.

Upaya pencegahan penyalahgunaan Artificial Intelligence dalam kejahatan siber perlu dilakukan melalui pembaruan regulasi yang lebih komprehensif, penguatan penegakan hukum di bidang siber, peningkatan kemampuan aparat dalam menangani kejahatan digital, serta peningkatan literasi digital masyarakat. Selain itu, penelitian selanjutnya diharapkan dapat mengkaji lebih mendalam mengenai model pertanggungjawaban hukum terhadap penggunaan teknologi kecerdasan buatan agar sistem hukum di Indonesia mampu mengikuti perkembangan teknologi yang semakin cepat.

DAFTAR PUSTAKA

Aini, N. (2024). Tantangan pembuktian dalam kasus kejahatan siber di Indonesia. Jurnal Judge, 4(2). https://journal.cattleyadf.org/index.php/Judge/article/view/566

Hapsari, R. D., & Pambayun, K. G. (2023). Ancaman cybercrime di Indonesia dalam perspektif hukum. Jurnal Konstituen, 5(1). https://sj.eastasouth-institute.com/index.php/shh/article/view/544

Marzuki, P. M. (2010). Penelitian hukum. Jakarta: Kencana Prenada Media Group.

Matondang, A. M. (2025). Kebijakan hukum pidana terhadap kejahatan cyber. JHLG Journal, 2(1). https://ojs.rewangrencang.com/index.php/JHLG/article/view/994

Ninggeding, N. Y. (2023). Penegakan hukum terhadap cyber crime di Indonesia. Jurnal Ilmu Hukum, 8(2). https://jurnal.uwp.ac.id/fh/index.php/jurnalilmuhukum/article/view/107

Nugraha, R. (2021). Perspektif hukum Indonesia dalam penanganan cybercrime di era digital. Jurnal Ilmiah Hukum Dirgantara, 11(2). https://journal.universitassuryadarma.ac.id/index.php/jihd/article/view/767

Rahmawati, I. (2017). Analisis manajemen risiko ancaman kejahatan siber (cybercrime). Jurnal Pertahanan & Bela Negara, 7(2). https://jurnal.idu.ac.id/index.php/JPBH/article/view/179

Sari, R. (2022). Perlindungan hukum terhadap data pribadi di era digital. De Jure: Jurnal Penelitian Hukum, 22(2). https://ejournal.balitbangham.go.id/index.php/dejure/article/view/2229

Sitanggang, A. S., Darmawan, F., & Manurung, D. (2024). Hukum siber dan penegakan hukum di Indonesia. Jurnal Penelitian Teknologi Informasi, 4(3). https://www.journal.uniba.ac.id/index.php/SH/article/view/1318

Soekanto, S., & Mamudji, S. (2006). Penelitian hukum normatif: Suatu tinjauan singkat. Jakarta: RajaGrafindo Persada.

Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

Widodo, W. (2019). Kebijakan hukum pidana dalam penanggulangan cybercrime di Indonesia. Masalah-Masalah Hukum, 48(2), 197–206. https://ejournal.undip.ac.id/index.php/mmh/article/view/20565