E-NISN : 2614-2643
P-NISN : 2541-7037
Journal Equitable
Vol 10 No 3
2025

URGENSI PENGATURAN TERHADAP PENYALAHGUNAAN *ARTIFICIAL INTELLIGENCE* PADA TINDAK PIDANA *MALWARE* DI INDONESIA

Wilianli Melati Jaya Putri
Universitas Muhammadiyah Riau, Indonesia, wilianlimelati@gmail.com

Cheny Berlian
Universitas Muhammadiyah Riau, Indonesia, chenyberlian@umri.ac.id

Rahmi Yuniarti
Universitas Muhammadiyah Riau, Indonesia, rahmiyuniarti@umri.ac.id

Umar Dinata
Universitas Muhammadiyah Riau, Indonesia, umardinata@umri.ac.id

Abstract

The misuse of Artificial Intelligence in malware crimes is a serious challenge in the digital era, considering that Artificial Intelligence can be used to create more sophisticated and difficult to detect malware. This study examines the forms and impacts of the misuse of Artificial Intelligence in malware crimes and the urgency of regulating the misuse of Artificial Intelligence in malware crimes in Indonesia. The research method used is normative juridical with a comparative legal approach. The results of the first discussion show that the forms of misuse of Artificial Intelligence have increasingly developed, including Adaptive Malware, Smart Phishing, Artificial Intelligence Powered Ransomware, Artificial Intelligence Powered Botnets, Polymorphic Malware, Spyware Artificial Intelligence, and Artificial Intelligence Powered Worms, then discuss the legal impacts that arise and most often are related to criminal liability due to the misuse of Artificial Intelligence in malware crimes. Second, the results of the discussion show that Indonesia does not yet have specific regulations regarding the misuse of Artificial Intelligence in cybercrime. On the other hand, the European Union has established an Artificial Intelligence Act with a risk-based approach, while China regulates Artificial Intelligence through strict administrative provisions.
Keywords: *Artificial Intelligence, Malware, China, European Union.*

Abstrak

Penyalahgunaan *Artificial Intelligence* dalam tindak pidana *malware* menjadi tantangan serius dalam era digital, mengingat *Artificial Intelligence* dapat dimanfaatkan untuk menciptakan *malware* yang lebih canggih dan sulit dideteksi. Penelitian ini mengkaji mengenai bentuk dan dampak penyalahgunaan *Artificial Intelligence* pada tindak pidana *malware* serta urgensi pengaturan terhadap penyalahgunaan *Artificial Intelligence* pada tindak pidana *malware* di Indonesia. Metode penelitian yang digunakan adalah yuridis normatif dengan pendekatan perbandingan hukum. Hasil pembahasan pertama menunjukkan bahwa bentuk penyalahgunaan *Artificial Intelligence* sudah semakin berkembang yang diantaranya terdiri dari *Adaptive Malware, Smart Phising, Artificial Intelligence Powered Ransomware, Artificial Intelligence Powered Botnets, Polymorphic Malware, Spyware Artificial Intelligence,* serta *Artificial Intelligence Powered Worms,* kemudian berbicara mengenai dampak hukum yang timbul dan paling sering ialah berkaitan dengan pertanggungjawaban pidana dikarenakan penyalahgunaan *Artificial Intelligence* pada tindak pidana

malware. Kedua, hasil pembahasan menunjukkan bahwa Indonesia belum memiliki regulasi khusus terkait penyelahgunaan *Artificial Intelligence* dalam kejahatan siber. Di sisi lain, Uni Eropa telah menetapkan *Artificial Intelligence Act* dengan pendekatan berbasis resiko, sementara China mengatur *Artificial Intelligence* melalui ketentuan administratif yang ketat.
Kata kunci: *Artificial Intelligence*, *Malware,* China, Uni Eropa.

A. Pendahuluan

Perkembangan teknologi digital membawa dampak besar dalam kehidupan manusia, termasuk dalam bidang keamanan siber, salah satu inovasi yang berperan penting adalah *Artificial Intelligence*, yang kini tidak hanya memberikan manfaat, tetapi juga memunculkan risiko baru ketika dimanfaatkan dalam tindak pidana. Penyalahgunaan *Artificial Intelligence* dalam bentuk tindak pidana *malware* menghadirkan ancaman serisu karena mampu beradaptasi, menyemarkan diri, dan melewati sistem deteksi konvensional. Hal ini menjadikan kejahatan siber semkin kompleks dan sulit ditangani.

Data Badan Siber dan Sandi Negara (BSSN) mencatat sebanyak 370 juta serangan siber di Indonesia sepanjang 2022, meningkat 38,72% dari tahun sebelumnya.[1] *Malware* telah menjadi ancaman dominan, dengan Provinsi Riau yang tercatat sebagai wilayah paling banyak menerima serangan pada tahun 2023 yaitu yaitu berjumlah 54.313.225 kali serangan.[2] Kemudian terjadi juga serangan *Brain Chiper Ransomware* (Varian dari *Lockbit* 3.0) terhadap Pusat Data Nasional Sementara 2 (PDNS 2) pada Juni 2024. Serangan yang dilakukan adalah berupa menonaktifkan keamanan *Windows Defender* pada server PDNS 2, yang akhirnya memudahkan peretas untuk menyebarkan

[1] Badan Siber dan Sandi Negara (BSSN), *Laporan Tahunan 2022: Statistik Serangan Siber di Indonesia* (Jakarta: BSSN, 2023).

[2] Honeynet Project BSSN, "Statistik Serangan Siber Indonesia 2023," diakses 10 Juni 2023, https://honeynet.bssn.go.id.

ransomware.[3] Hal ini semakin mempertegas kerentanan infrastruktur digital nasional. Di tingkat global, penyalahgunaan *Artificial Intelligence* juga menimbulkan kerugian besar, seperti kasus yang terjadi di China pada tahun 2023 ketika seorang pengusaha bernama Mr. Guo ditipu menggunakan teknologi *deepfake* hingga mengalami kerugian sekitar 8,9 triliun rupiah.[4] Kedua kasus ini memperlihatkan betapa seriusnya ancaman penyalahgunaan *Artificial Intelligence* dalam kejahatan siber.

Regulasi di Indonesia seperti UU ITE dan UU PDP, memang telah menjadi dasar hukum dalam penanganan kejahatan siber. Namun, aturan tersebut masih bersifat umum dan belum secara khusus mengatur penyalahgunaan *Artificial Intelligence,* sehingga menimbulkan kekosongan hukum dalam aspek pencegahan maupun penegakan hukum. Sebaliknya, beberapa yuridiksi lain telah bergerak maju. Seperti Uni Eropa melalui *Artificial Intelligence Act* menekankan pendekatan berbasis risiko,[5] serta China yang menerapkan ketentuan administratif yang ketat seperti yakni *Provisions on the Management of Recommendation Algorithms in Internet Information Services*[6] dan *Provisions on the Administration of Deep Synthesis Internet Information Services*.[7]

[3] Agus Maulana, "Kasus Ransomware Di Indonesia: Ancaman, Contoh Kasus, Dan Cara Melindungi Bisnis Anda," Rizki Tujuhbelas Kelola, 2024, https://r17.co.id/insight/article/kasus-ransomware-di-indonesia-ancaman-contoh-kasus-dan-cara-melindungi-bisnis-anda.

[4] Ibnu Naufal, "Rp8,9 Triliun Raib! Scammer Gunakan AI Dan Deepfake Dalam Penipuan Besar-Besaran," inilah.com, 2023, https://www.inilah.com/rp89-triliun-raib-scammer-gunakan-ai-dan-deepfake-dalam-penipuan-besar-besaran.

[5] European Commission, *Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)*, 2021.

[6] Cyberspace Administration of China, *Provisions on the Management of Recommendation Algorithms in Internet Information Services*, 2021.

[7] Cyberspace Administration of China, *Provisions on the Administration of Deep Synthesis Internet Information Services*, 2022.

Berdasarkan kondisi tersebut, penelitian ini bertujuan untuk menganalisis bentuk penyalahgunaan *Artificial Intelligence* dalam tindak pidana *malware*, serta mengkaji mengenai urgensi pengaturan di Indonesia melalui pendekatan perbandingan hukum. Penelitin ini diharapkan dapat memberikan kontribusi bagi pembentukan regulasi nasional yang lebih komprehensif, sehingga mampu memberikan perlindungan hukum yang efektif terhadap ancaman penyalahgunaan *Artificial Intelligence* di era digital.

B. Rumusan Masalah

1. Bagaimana bentuk serta dampak penyalahgunaan *Artificial Intelligence* pada Tindak Pidana *Malware*?
2. Bagaimana urgensi pengaturan terhadap penyalahgunaan *Artificial Intelligence* pada Tindak Pidana *Malware* di Indonesia?

C. Tujuan Penelitian

1. Untuk menganalisis mengenai bentuk serta dampak penyalahgunaan *Artificial Intelligence* pada Tindak Pidana *Malware*;
2. Untuk menganalisis mengenai urgensi penyalahgunaan *Artificial Intelligence* pada Tindak Pidana *Malware* di Indonesia.

D. Metode Penelitian

Penelitian ini menggunakan metode yuridis normatif dengan menekankan kajian literatur terhadap peraturan perundang-undangan, doktrin, dan literatur hukum terkait.[8] Pendekatan yang digunakan ialah Pendekatan Undang-Undang (*Statute Approach*) dan Pendekatan Komparatif (*Comparative*

[8] Prof. Dr. Suteki and Galang Taufani, *Metodologi Penelitian Hukum : Filsafat, Teori Dan Praktik*, 1st ed. (Jakarta: Rajawali Pers, 2022), hlm 147.

Approach), yaitu dengan menganalisis regulasi mengenai *Artificial Intelligence* di Uni Eropa dan China sebagai pembanding untuk menilai kekosongan hukum di Indonesia.[9]

Sumber data penelitian terdiri dari bahan hukum primer, meliputi peraturan perundang-undangan nasional seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) serta Undang-Undang Perlindungan Data Pribadi (UU PDP), maupun regulasi internasional seperti *EU Artificial Intelligence Act* dan ketentuan administratif *Artificial Intelligence* di China. Selain itu digunakan bahan hukum sekunder berupa buku, jurnal, artikel ilmiah, dan laporan resmi lembaga, serta bahan hukum tersier seperti kamus hukum dan ensiklopedia.

Data yang diperoleh dianalisis secara kualitatif, yaitu dengan mendeskripsikan dan menafsirkan ketentuan hukum yang ada, kemudian menarik kesimpulan mengenai urgensi pembentukan regulasi khusus terkait penyalahgunaan *Artificial Intelligence* dalam tindak pidana *malware* di Indonesia.[10]

E. Hasil Penelitian dan Pembahasan

Penyalahgunaan teknologi *Artificial Intelligence* dalam tindak pidana siber, khususnya *malware,* telah menimbulkan tantangan baru bagi sistem hukum di Indonesia. Berbeda dengan *malware* konvensional, *malware* berbasis *Artificial Intelligence* memiliki kemampuan untuk belajar, beradaptasi, dan mengubah polanya sehingga lebih sulit dideteksi oleh sistem keamanan.[11] Bentuk penyalah-

[9] Dr. Muhaimin, *Metode Penelitian Hukum*, 1st ed. (Mataram: Mataram University Press, 2020), hlm 56.

[10] Bambang Waluyo, *Penelitian Hukum dalam Praktek* (Jakarta: Sinar Grafika, 2002), hlm 72.

[11] L. R. Kaplan, "Artificial Intelligence in Spyware: Evasion and Data Theft Techniques," *Cybersecurity Review* 16, no. 3 (2022): 134–145.

gunaan ini mencakup beberapa bentuk diantaranya *malware* yang dapat beradaptasi dan belajar (*Adaptive Malware*), *Phising* cerdas (*Smart Phising*), *Ransomware* yang digerakkan oleh *Artificial Intelligence* (*Artificial Intelligence Powered Ransomware*), *Botnet* dan Serangan Terkoordinasi (*Artificial Intelligence Powered Botnets*), *Polymorphic Malware* berbasis *Artificial Intelligence, Spyware* yang didukung *Artificial Intelligence,* serta *Artificial Intelligence Powered Worms*.[12] Fenomena ini menunjukkan bahwa kejahatan siber kini tidak lagi sekedar berbasis pada kode statis, melainkan melibatkan *Artificial Intelligence* atau kecerdasan buatan yang semakin dinamis.

Di Indonesia, kasus serangan siber terus meningkat seiring dengan berkembangnya teknologi. Serangan *Brain Chiper Ransomware* terhadap Pusat Data Nasional Sementara (PDNS) 2 pada Juni 2024 memperlihatkan dampak nyata kerentanan infrastruktur digital nasional. Kasus tersebut mengakibatkan lumpuhnya sejumlah layanan publik yang sangat vital bagi masyarakat. Kejadian ini mem-pertegas bahwa *malware* canggih, terlebih yang didukung oleh teknologi *Artificial Intelligence,* dapat menimbulkan kerugian serius tidak hanya bagi individu tetapi juga bagi kepentingan negara. Situasi ini memperlihatkan urgensi pengaturan yang lebih komprehensif untuk mengantisipasi kejahatan berbasis *Artificial Intelligence.*

Kerangka hukum di Indonesia masih memiliki keterbatasan UU ITE dan UU PDP memang telah menjadi dasar dalam menangani tindak pidana siber,

[12] Sameer Patil et al., "Intelligent Worms: The Next Threat of AI-Driven Malware," *Journal of Information Security* 12, no. 2 (2022): 87–99.

tetapi keduanya bersifat umum dan tidak secara spesifik menyinggung mengenai penggunaan *Artificial Intelligence.* Kekosongan hukum ini menimbulkan kesenjangan dalam aspek pencegahan, penindakan, maupun pemulihan bagi korban. Kondisi tersebut sejalan dengan pandangan Philipus M. Hadjon mengenai perlindungan hukum, bahwa hukum seharusnya memberikan rasa aman dan perlindungan terhadap hak-hak warga negara, baik preventif maupun represif.[13] Tanpa adanya regulasi yang jelas mengenai penyalahgunaan *Artificial Intelligence,* masyarakat Indonesia berada dalam posisi rentan karena tidak memperoleh perlindungan hukum yang optimal apalagi ditambah dengan pergeseran budaya masyarakat Indonesia menuju masyarakat digital.

Uni Eropa menjadi salah satu pelopor dalam membentuk regulasi komprehensif terkait kecerdasan buatan melalui *Artificial Intelligence Act.* Regulasi ini menggunakan pendekatan berbasis resiko (*risk-based approach*), di mana sistem dikategorikan kedalam risiko minimal, terbatas, tinggi, hingga terlarang. Sementara itu China lebih berfokus pada stabilitas sosial dan kedaulatan digital melalui regulasi *Provisions on the Administration of Deep Synthesis Internet Information Services* (互联网信息服务深度合成管理规定). Tetapi pendekatan normative yang mereka terapkan memiliki perbedaan cukup signifikan.

Misalnya, pengaturan mengenai larangan penggunaan *Artificial Intelligence* untuk tujuan tertentu, Uni

[13] Philipus M. Hadjon, *Perlindungan Hukum bagi Rakyat di Indonesia* (Surabaya: Bina Ilmu, 1987), hlm 25.

Eropa melalui Pasal 5 *Artificial Intelligence Act* melarang penggunaan sistem *Artificial Intelligence* untuk manipulasi bawah sadar yang dapat membahayakan pengguna, yang berbunyi: *"...to materially distort a person's behavior in a manner that causes or is likely to cause that person or another person physical or psychological harm..."*[14]

China melalui Pasal 17 Peraturan Sintesis Mendalam, melarang produksi dan penyebaran konten berbasis *Artificial Intelligence* yang dapat mengganggu keamanan nasional, stabilitas sosial, dan kepentingan hukum warga negara, yang berbunyi:

"…深度合成服务提供者提供以下深度合成服务，可能导致公众混淆或者误认的，应当在生成或者编辑的信息内容的合理位置…"[15]

Kemudian, mengenai transparansi penggunaan *Artificial Intelligence,* Uni Eropa melalui Pasal 50 *Artificial Intelligence Act* mengatur bahwa penggunaan harus diberitahukan apabila mereka sedang berinteraksi dengan sistem *Artificial Intelligence*, yang berbunyi:

"*1) Providers shall ensure that AI systems intended to interact directly with natural persons are designed and developed in such a way that the natural persons concerned are informed that they are interacting with an AI system…*"[16]

[14] European Parliament and Council of the European Union, *Artificial Intelligence Act,* Final Text Agreed 2024, art. 5.

[15] Cyberspace Administration of China (CAC), *Provisions on the Administration of Deep Synthesis Internet Information Services*, promulgated December 11, 2022, effective January 10, 2023, art. 17.

[16] European Parliament and Council of the European Union, *Artificial Intelligence Act*, Final Text Agreed 2024, art. 50.

China melalui Pasal 10 Peraturan Sintesis Mendalam, yang menyatakan bahwa konten yang dihasilkan melalui teknologi *deep synthesis* harus diberi label atau penanda yang jelas, untuk memastikan publik tidak disesatkan oleh konten tersebut, yang berbunyi:

"*深度合成服务提供者应当加强深度合成内容管理，采取技术或者人工方式对深度合成服务使用者的输入数据和合成结果进行审核...*"[17]

Terakhir mengenai pengawasan dan penegakan hukum, Uni Eropa melalui Pasal 64 hingga 77 *Artificial Intelligence Act* membentuk otoritas pengawasan yang bersifat independen dan diberi wewenang untuk mengawasi kepatuhan terhadap peraturan ini, serta menjatuhkan sanksi administratif bagi pelanggaran, yang berbunyi:

"*The EU is creating an "AI Office" to improve its knowledge and skills in artificial intelligence (AI). This office will be supported by the member countries of the EU, who will help it carry out its duties as outlined in the regulations…*"[18]

Sementara itu, China tidak mengatur pembentukan lembaga khusus dalam peraturannya, namun melalui Pasal 19 Peraturan Sintesis Mendalam, pengawas-an dilaksanakan secara langsung oleh *Cyberspace Administration of China* (CAC) sebagai otoritas yang memiliki fungsi administratif, pengawasan konten, dan keamanan siber, yang berbunyi:

[17] Cyberspace Administration of China (CAC), *Provisions on the Administration of Deep Synthesis Internet Information Services*, promulgated December 11, 2022, effective January 10, 2023, art. 10.

[18] European Parliament and Council of the European Union, *Artificial Intelligence Act*, Final Text Agreed 2024, art. 64.

"完成备案的深度合成服务提供者和技术支持者应当在其对外提供服务的网站、应用程序等的显著位置标明其备案编号并提供公示信息链接"[19]

Jika dibandingkan dengan yuridiksi lain, langkah Indonesia terlihat tertinggal. Uni Eropa melalui *Artificial Intelligence Act* menerapkan pendekatan berbasis risiko. Sistem *Artificial Intelligence* yang dikategorikan berisiko tinggi, termasuk yang berpotensi digunakan untuk kejahatan siber, diwajibkan memnuhi standar transparansi, keamanan, dan akuntabilitas yang ketat. Pendekatan ini menekankan pada pencegahan sejak tahap perancangan teknologi. Sementara itu, China memilih jalur administratif yang lebih ketat dengan memberlakukan *Deep Synthesis Provisions* dan *Algorithmic Recommendation Management Provisions* kedua regulasi tersebut secara langsung membatasi ruang gerak teknologi *Artificial Intelligence* yang dapat menimbulkan ancaman, serta memberikan kewenangan besar kepada pemerintah dalam mengawasi penggunaannya.

Perbandingan ini memperlihatkan bahwa negara-negara besar telah menempatkan *Artificial Intelligence* sebagai isu strategis dalam bidang hukum dan keamanan. Model regulasi Uni Eropa yang berbasis risiko dapat menjadi inspirasi bagi Indonesia untuk membangun regulasi adaptif, sedangkan pendekatan administratif dari China menunjukkan pentingnya kontrol negara terhadap penyebaran teknologi berbahaya. Dalam konteks ini, gagasan Satjipto

[19] Cyberspace Administration of China (CAC), *Provisions on the Administration of Deep Synthesis Internet Information Services*, promulgated December 11, 2022, effective January 10, 2023, art. 19.

Rahardjo mengenai hukum progresif menjadi relevan. Hukum progresif menekankan bahwa hukum tidak boleh kaku dan terjebak dalam teks, tetapi harus mampu menjawab kebutuhan masyarakat dan perkembangan zaman.[20] Dengan demikian, pengaturan hukum mengenai *Artificial Intelligence* di Indonesia tidak hanya sekedar meniru model negara lain, tetapi harus dikembangkan secara inovatif untuk menyesuaikan dengan kebutuhan nasional dan dinamika kejahatan siber.

Urgensi pembentukan regulasi di Indonesia semakin jelas apabila dikaitkan dengan karakteristik kejahatan siber yang lintas batas negara. Tanpa kerangka hukum yang jelas, aparat penegak hukum akan kesulitan dalam menindak pelaku maupun melakukan kerja sama internasional. Selain itu, regulasi juga diperlukan untuk memberikan perlindungan hukum yang lebih pasti bagi masyarakat sebagai pengguna teknologi digital. Oleh karena itu, pembentukan regulasi khusus mengenai *Artificial Intelligence* dalam tindak pidana *malware* merupakan kebutuhan mendesak untuk mewujudkan perlindungan hukum yang efektif dan sejalan dengan semangat hukum progresif.

F. Penutup/Kesimpulan

Bentuk dan dampak penyalahguna-an *Artificial Intelligence* digambarkan kedalam beberapa bentuk, *Artificial Intelligence* merupakan teknologi yang mampu meniru kecerdasan manusia dan diterapkan dalam berbagai sektor. Namun *Artificial Intelligence* juga dapat disalahgunakan, salah satunya dalam pembuatan dan penyebaran *malware,*

[20] Satjipto Rahardjo, *Hukum Progresif: Hukum yang Membebaskan* (Jakarta: Kompas, 2009), hlm 45.

yang dapat menyebabkan kerugian besar bagi individu, institusi bahkan negara. Penyalahgunaan *Artificial Intelligence* dalam tindak pidana *malware* membuka celah baru dalam kejahatan siber yang lebih canggih, sistematis dan sulit dilacak. Kemudian mengenai dampak yang timbul akibat penyalahgunaan *Artificial Intelligence* ini ialah kekosongan hukum yang mengakibatkan tidak adanya pengaturan yang jelas dalam mengatur penyalahgunaan *Artificial Intelligence* sehingga menyebabkan berbagai dampak serius baik bagi individu maupun negara.

Urgensi pengaturan terhadap penyalahgunaan *Artificial Intelligence* dalam tindak pidana *malware* di Indonesia sangat penting dikarenakan belum adanya regulasi secara khusus. Instrumen hukum yang digunakan masih mengacu pada peraturan umum seperti UU ITE dan UU PDP. Regulasi tersebut belum secara eksplisit mengatur bentuk-bentuk kejahatan siber berbasis *Artificial Intelligence* maupun pertanggungjawaban pelaku yang menggunakan teknologi *Artificial Intelligence* sebagai alat kejahatan. Regulasi di Uni Eropa dan China memberikan pendekatan yang lebih komprehensif terhadap pengendalian teknologi *Artificial Intelligence*. Uni Eropa melalui *Artificial Intelligence Act* dan prinsip *risk-based approach*-nya telah membagi sistem *Artificial Intelligence* berdasarkan tingkat resiko, termasuk ancaman terhadap hak asasi manusia. Sementara itu, China mengatur *Artificial Intelligence* melalui peraturan administratif seperti *Provisions on the Management of Recommendation Algorithms in Internet Information Services* dan *Provisions on the Administration of Deep Synthesis Internet Information Services,* yang mengontrol

penggunaan *Artificial Intelligence* untuk mencegah penyalahgunaan, termasuk manipulasi informasi dan konten berbahaya.

Relevansi pengaturan *Artificial Intelligence* di Uni Eropa dan China terhadap hukum Indonesia menunjukkan pentingnya pembentukan regulasi nasional yang lebih spesifik terhadap teknologi *Artificial Intelligence,* termasuk dalam konteks kejahatan siber. Indonesia dapat mempelajari pendekatan regulatif dari kedua negara tersebut, baik dari segi filosofi perlindungan HAM (Uni Eropa) maupun pengawasan teknologi secara administratif (China), untuk merancang kebijakan yang adaptif terhadap perkembangan teknologi digital dan potensi penyalahgunaannya.

Daftar Pustaka

1. Buku

Hadjon, Philipus M. *Perlindungan Hukum bagi Rakyat di Indonesia*. Surabaya: Bina Ilmu, 1987.

Muhaimin, Dr. *Metode Penelitian Hukum*. 1st ed. Mataram: Mataram University Press, 2020.

Rahardjo, Satjipto. *Hukum Progresif: Hukum yang Membebaskan*. Jakarta: Kompas, 2009.

Suteki, Prof. Dr., and Galang Taufani. *Metodologi Penelitian Hukum: Filsafat, Teori dan Praktik*. 1st ed. Jakarta: Rajawali Pers, 2022.

Waluyo, Bambang. *Penelitian Hukum dalam Praktek*. Jakarta: Sinar Grafika, 2002.

2. Jurnal Ilmiah

Kaplan, L. R. "Artificial Intelligence in Spyware: Evasion and Data Theft Techniques." *Cybersecurity Review* 16, no. 3 (2022): 134–145.

Patil, Sameer, et al. “Intelligent Worms: The Next Threat of AI-Driven Malware.” *Journal of Information Security* 12, no. 2 (2022): 87–99.

3. Peraturan Perundang-Undangan

Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik.

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

Cyberspace Administration of China. *Provisions on the Management of Recommendation Algorithms in Internet Information Services*. 2021.

Cyberspace Administration of China. *Provisions on the Administration of Deep Synthesis Internet Information Services*. 2022.

European Commission. *Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)*. 2021.

4. Laporan/Dokumen Resmi

Badan Siber dan Sandi Negara (BSSN). *Laporan Tahunan 2022: Statistik Serangan Siber di Indonesia*. Jakarta: BSSN, 2023.

Honeynet Project BSSN. "Statistik Serangan Siber Indonesia 2023." Diakses 10 Juni 2023. https://honeynet.bssn.go.id.

5. Website/Artikel

Maulana, Agus. "Kasus Ransomware di Indonesia: Ancaman, Contoh Kasus, dan Cara Melindungi Bisnis Anda." Rizki Tujuhbelas Kelola, 2024. https://r17.co.id/insight/article/kasus-ransomware-di-indonesia-ancaman-contoh-kasus-dan-cara-melindungi-bisnis-anda.

Naufal, Ibnu. "Rp8,9 Triliun Raib! Scammer Gunakan AI dan Deepfake dalam Penipuan Besar-Besaran." *inilah.com*, 2023. https://www.inilah.com/rp89-triliun-raib-scammer-gunakan-ai-dan-deepfake-dalam-penipuan-besar-besaran.