PAMPAS: *Journal of Criminal Law*
Volume 6 Nomor 2, Tahun 2025
(ISSN 2721-8325)

Perlindungan Hukum Bagi Korban Penyalahgunaan *Artificial Intelligence* (Ai) Terhadap Serangan *Malware* dalam Perspektif Peraturan Perundang Undangan

Afifah Ayu Nurjanah[1], Herry Liyus[2]
Fakultas Hukum Universitas Jambi[1]
Fakultas Hukum Universitas Jambi[2]
Author's Email Correspondent: Afifahayu822@gmail.com

ABSTRAK
Tujuan dari penelitian ini dilakukan untuk mengetahui pengaturan mengenai perlindungan hukum bagi korban penyalahgunaan *Artificial Intelligence* (AI) terhadap serangan *Malware* dalam perspektif Peraturan Perundang-Undangan yang berlaku saat ini, serta untuk mengetahui mengenai kebijakan hukum terhadap pengaturan bagi korban penyalahgunaan *Artificial Intelligence* (AI) di masa mendatang. Dengan rumusan masalah yakni: 1) bagaimana bentuk perlindungan hukum bagi korban penyalahgunaan *Artificial Intelligence* (AI) terhadap serangan Malware berdasarkan Peraturan Perundang-Undanga; 2) bagaimana kebijakan hukum terhadap pengaturan bagi korban penyalahgunaan *Artificial Intelligence* (AI) di masa mendatang. Jenis penelitian ini adalah yuridis normative. Hasil penelitian menunjukkan bahwa Perlindungan hukum bagi korban penyalahgunaan AI khususnya pada kasus serangan *Malware* masih belum efektif di Indonesia. Meskipun terdapat regulasi yang ada, seperti Pasal 28 D Ayat (1) Undang-Undang Dasar 1945 yang menjamin hak atas perlindungan hukum. Akan tetapi, penerapannya belum jelas dan komperhensif. Selanjutnya, implementasi Undang-Undang Informasi dan Transaksi Elektronik menggolongkan AI sebagai Agen Elektronik, sehingga AI belum disebutkan secara gramatikal pada aturan tersebut. Kebijakan hukum pidana terhadap perlindungan bagi korban penyalahgunaan AI terhadap serangan *Malware* di Indonesia belum bersifat konkrit dan tegas dalam melakukan suatu perbaikan atau pembuatan peraturan khusus mengenai AI yang didalamnya mengatur tentang ketentuan mengenai batasan-batasan secara jelas dan mengikat dalam pengolahan system kerja kecerdasan buatan ini. Kebijakan mengenai AI harus diatur secara tegas mengenai sanksi pidana pada serangan *Malware* yang memanfaatkan kecerdasan buatan, dan memberikan penjelasan dalam aturan terkait perlindungan terhadap korban penyalahgunaan AI berupa serangan *Malware* untuk mencegah dan menanggulangi tindak pidana tersebut, serta memberikan hak-hak yang harus didapatkan korban dari penyalahgunaan AI.

Kata Kunci: perlindungan; hukum; korban; penyalahgunaan; *AI*

ARTICLE HISTORY
Submission: 2025-05-07
Accepted: 2025-07-03
Publish: 2025-07-03

KEYWORDS: *legal protection; victims; misuse; AI*

ABSTRACT
The aim of this research is 1) The purpose of this study was to determine the regulation regarding legal protection for victims of Artificial Intelligence (AI) abuse against Malvare attacks from the perspective of current applicable laws and regulations, as well as to determine the legal policy regarding the regulation for victims of Artificial Intelligence (AI) abuse in the future. With the formulation of the problem, namely: 1) what is the form of legal protection for victims of Artificial Intelligence (AI) abuse against Malvare attacks based on laws and regulations; 2) what is the legal policy regarding the regulation for victims of Artificial Intelligence (AI) abuse in the future. This type of research is normative juridical. The results of the study indicate that legal protection for victims of AI abuse, especially in cases of Malware attacks, is still ineffective in Indonesia. Although there are existing regulations, such as Article 28 D Paragraph (1) of the 1945 Constitution which guarantees the right to legal protection. However, its implementation is not yet clear and comprehensive. Furthermore, the implementation of the Electronic Information and Transactions Law classifies AI as an Electronic Agent, so that AI has not been grammatically mentioned in the regulation. The criminal law policy on protection for victims of AI abuse against Malware attacks in Indonesia is not yet concrete and firm in making improvements or making special regulations regarding AI which regulate provisions regarding clear and binding limitations in the processing of this artificial intelligence work system. The policy regarding AI must be strictly regulated regarding criminal sanctions for Malware attacks that utilize artificial intelligence, and provide an explanation in the rules related to protection for victims of AI abuse in the form of Malvare attacks to prevent and overcome these crimes, as well as provide the rights that victims must obtain from AI abuse.

A. PENDAHULUAN

Perlindungan hukum merupakan segala bentuk upaya pemerintah untuk memberikan jaminan adanya kepastian hukum dan perlindungan kepada warga negaranya agar hak-hak yang dimiliki oleh seseorang tidak dilanggar oleh orang lain, dan bagi yang melanggar akan diberikan sanksi sesuai dengan peraturan yang berlaku. Perlindungan Hukum menurut Satjito Rahardjo adalah:

Adanya upaya yang melindungi kepentingan masyarakat dengan cara mengalokasikan suatu Hak Asasi Manusia (HAM) yang telah dirugikan oleh orang lain dan perlindungan tersebut diberikan kepada masyarakat agar dapat menikmati seluruh hak-hak mereka yang telah diberikan oleh hukum. Hukum difungsikan untuk menciptakan perlindungan yang besifat fleksibel, adaptif, serta prediktif dan antisipatif.[1] Perlindungan hukum perlu dikonstruksikan dalam Norma hukum harus mampu merumuskan secara lebih konkret norma dan nilai yang berlaku dalam Masyarakat.[2]

[1] Rahardjo, Satjipto, *Ilmu Hukum*, PT. Citra Aditya Bakti, Bandung, 2000, hlm.55.

[2]Hafrida et al., "Students' Perception of the Criminalization of Cohabitation (Kumpul Kebo) in Indonesia: From Quantitative to Normative Analysis," *Jambe Law Journal* 7, no. 1 (July 22, 2024): 127–47, https://doi.org/DOI: https://doi.org/10.22437/home.v7i1.340.

Berdasarkan pendapat tersebut dapat diartikan bahwa perlindungan hukum bertujuan untuk melindungi harkat dan martabat seseorang, serta pengakuan terhadap hak-hak yang dimiliki oleh subyek hukum berdasarkan peraturan atau kaidah yang berlaku. Pada dasarnya perlindungan hukum diberikan kepada seluruh subyek hukum, termasuk korban tindak kejahatan.

Perlindungan hukum terhadap korban kejahatan adalah bentuk dari perlindungan hukum kepada seseorang yang menjadi korban kejahatan dengan tujuan untuk melindungi hak-hak korban.[3] Perlindungan hukum terhadap korban kejahatan ini merupakan amanat dari Pasal 28D ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 (UUD 1945) bahwa "setiap orang berhak atas pengakuan, jaminan, perlindungan, dan kepastian hukum yang adil serta perlakuan yang sama dihadapan hukum". Menurut Susanto perlindungan hukum terhadap korban kejahatan memiliki beberapa fungsi, yaitu:

Melindungi korban dari ancaman dan tindakan berbahaya yang dapat membahayakan jiwa, fisik, kesehatan, serta nilai-nilai dan hak asasinya. *M*enjaga dan melindungi keadilan bagi seluruh masyarakat. *A*lat untuk menentukan arah, tujuan dan pelaksanaan pembangunan secara adil.[4]

Selain diatur dalam UUD 1945, perlindungan hukum terhadap korban kejahatan juga diatur dalam Undang-Undang Nomor 31 Tahun 2014 tentang Perubahan Atas Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban memberikan pengertian perlindungan adalah segala upaya pemenuhan hak dan pemberian bantuan untuk memberikan rasa aman kepada saksi dan/atau korban yang wajib dilaksanakan oleh Lembaga terkait sesuai dengan ketentuan.

Perlindungan hukum bagi korban tindak pidana tidak hanya diberikan kepada korban kejahatan yang diatur didalam Kitab Undang-Undang Hukum Pidana (KUHP) saja, melainkan korban tindak kejahatan di luar KUHP seperti kejahatan pada Teknologi Informasi berbasis digital. Saat ini era globalisasi informasi membawa dampak yang sangat besar bagi kehidupan manusia, Perkembangan teknologi informasi justru cenderung membawa dampak negative dalam perkembangan modus kejahatan, dengan adanya kemajuan teknologi, maka berkembang pula cara-cara untuk melakukan kejahatan. Modus kejahatan yang terjadi di era digital ini sering kali dilakukan melalui computer dan jaringan komputer sebagai alat bantu dalam melakukan aksinya [5]seperti *cyber stalking, cyber bullying*, peretasan, penyalahgunaan *Artificial Intelligence* (AI) dan masih banyak lagi kejahatan yang lain yang dapat merugikan bagi penggunanya (korban) baik secara materiil maupun nonmateriil.

Salah satu bentuk tindak kejahatan digital yang dapat merugikan adalah tindak kejahatan *Artificial Intelligence* (AI). *Artificial Intellegence* (AI) atau yang biasa dikenal dengan sebutan Kecerdasan Buatan merupakan suatu teknologi yang terdapat pada

---

[3] Bawole, Herlyanty, "Perlindungan Hukum Terhadap Korban Kejahatan", *Jurnal LEGALITAS* Volume 2 Nomor 2, 2017, hlm. 26-27, http://ejurnal.untag-smd.ac.id/index.php/LG/article/download/3382/3293.

[4] Yulia, Rena dan Aliyth Prakarsa, "Perlindungan Hukum Terhadap Korban Kejahatan Praktik Kedokteran Ilegal", *Jurnal.komisiyudisial.go.id E-ISSN:2579-4868; P-ISSN: 1978-6506* Vol. 13 No. 1, 2020, https://jurnal.komisiyudisial.go.id/index.php/jy/article/download/341/pdf/2602, hlm. 57-58.

[5] Diansah, Hendri, Usman, dan Yulia Monita, Kebijakan Hukum Pidana Terhadap Tindak Pidana *Carding*, *PAMPAS: Journal Of Criminal*. Volume: 3, Nomor: 1, 2022, hlm. 16, https://online-journal.unja.ac.id/Pampas/article/download/17704/13283

system komputer yang mampu melakukan pengembangan sistem dan mesin yang biasanya dilakukan oleh kecerdasan manusia. [6] *Artificial Intelligence* (AI) adalah bidang multidisiplin yang bertujuan untuk mengotomatisasikan aktivitas yang membutuhkan kecerdasan manusia, dimana kecerdasan buatan dan manusia dapat berkerjasama dalam membuat suatu keputusan yang tidak terlalu dipengaruhi oleh nilai-nilai pribadi.

Penyalahgunaan pada *Artificial Intelligence* (AI) memiliki berbagai jenis, antara lain : *carding* (mencuri nomor kartu kredit milik orang lain), *defacing* (mengalihkan wesite asli ke website yang lain), *hacking* dan *cracking* (memasuki computer atau sistem elektronik milik orang lain tanpa izin), *phising* (penipuan pada website yang memiliki nama hampir menyerupai website yang asli), *malware* (program atau software jahat yang menyusup ke dalam computer atau system pada computer), *spamming* (mengirimkan berita secara berulang-ulang), dan masih banyak lagi bentuk kejahatan yang dapat diakses melalui kecanggihan *Artificial Intelligemce* (AI) tersebut.

Terkait dengan jenis-jenis penyalahgunaan AI diatas, salah satu bentuk penyalahgunaan AI terbesar di Indonesia adalah serangan *malware*. *Malware* atau *Malicous Software* merupakan suatu program yang dirancang dengan tujuan untuk merusak dengan cara menyusup ke dalam system computer atau perangkat lunak pada komputer. *Malware* merupakan bentuk kejahatan dari perkembangan teknologi seperti kemajuan kecerdasar buatan atau *Artificial Intelligence* (AI) yang menjadikan ancaman yang berbahaya dalam dunia *cyber*.[7]

Kondisi Indonesia terhadap serangan *malware* sangatlah memprihatinkan, hal ini dibuktikan berdasarkan data keamanan siber *Microsoft* 2023, Indonesia berada di posisi ke-2 negara yang paling banyak terkena malware pada perangkat computer, dimana trafik anomaly sebanyak 47.231.390 terindikasi malware.[8] Menurut pusat keamanan siber perusahaan di Washington, Amareika Serikat, serangan siber yang paling banyak menyerang Indonesia adalah jenis *Malware*. Serangan *Malware* ini masih menjadi tranding issue di dunia siber karena *malware* dibuat secara khusus agar tersembunyi dan sulit untuk terdeteksi sehingga tetap dapat berada didalam sebuat system computer untuk periode waktu tertentu tanpa sepengetahuan pemilik system tersebut, sehingga keamanan system pada computer tidak dapat mendeteksi bahwa sistemnya telah terserang atau terinfeksi *malware*.

Indonesia mengalami kasus kejahatan serangan *malware* berjenis *Ransomware WannaCry* yang terjadi di Rumah Sakit Harapan Kita dan Rumah Sakit Dharmais di Jakarta. Komputer milik kedua Rumah Sakit tersebut dikunci atau terenskripsi seluruh data korban sehingga pihak Rumah sakit tidak dapat mengakses kembali seluruh data tersebut. Hal ini menyebabkan system pelayanan ke dua Rumah Sakit tersebut terhenti, karena untuk dapat membuka kembali akses data tersebut, korban diminta untuk membayar tebusan terlebih dahulu dalam bentuk bitcoin (mata uang virtual) dengan jumlah sebesar US$300 atau sekitar Rp. 4.000.000, rupiah. Pelaku kejahatan *malware*

[6] Eriana, Emi Sita dan Afrizal Zein, *Artificial Intelligence (AI)*, CV. Media Aksara, Bojongsari, 2023, hlm. 1

[7] Rachmadie, Donovan Typhano dan Supanto, "Regulasi Penyimpangan Artificial Intelligence Pada Tindak Pidana Malware Berdasarkan Undang-Undang Republik Indonesia Nomor 19 Tahun 2016", *Recidive* Volume 9 No. 2, 2020, https://jurnal.uns.ac.id/recidive/article/download/47400/29634, hlm. 130-131.

[8] Kartopati, Roebiono, *Lanskap Keamanan Siber Indonesia*, Direktorat Operasi Keamanan Siber, Jakarta, 2023, hlm. 15

berjenis *Ransomware Wannacry* ini juga memberikan ancaman kepada kedua Rumah Sakit tersebut, yakni apabila korban tidak melakukan atau membayar tebusan yang diminta maka seluruh data mereka akan lenyap terhapus.

Pada Bulan Januari Tahun 2022, serangan *Malware* kembali terjadi di Indonesia yaitu pada Bank Indonesia (BI) yang menyebabkan terjadinya kebocoran data. Serangan *Malware* yang terjadi di Bank Indonesia (BI) berjenis *Ransomware Conti* yang menyerang lebih dari 200 perangkat computer dan 52.767 dokumen yang memiliki kapasita sebesar 74.84 GB.[9]

Memasuki era kecerdasan buatan atau yang lebih dikenal dengan sebutan *Artificial Intelligence* (AI) menjadikan AI sebagai tenaga baru untuk menyebarkan serangan *malware* yang tidak mudah untuk dilacak dalam muatan data yang berbahaya. Teknik AI dapat menyembunyikan kondisi yang diperlukan untuk membuka muatan berbahaya, sehingga hampir tidak mungkin pemilik menyadari bahwa system perangkat pada komputernya telah terserang oleh *malware*. Artinya kejahatan penyalahgunaan AI terhadap serangan *malware* memberikan dampak buruk bagi korban, sehingga korban dalam tindak kejahatan ini juga harus mendapat perlindungan hukum.

Pada dasarnya, perlindungan hukum bagi korban kejahatan penyalahgunaan AI terhadap serangan *malware* dapat mengacu pada Pasal 4, Pasal 26, dan Pasal 27 Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik atau yang selanjutnya ditulis dengan UU ITE. Permasalahannya adalah dalam UU ITE belum mengatur secara optimal tentang penegakan hukum atas tindak pidana *cyber* khususnya kejahatan penyalahgunaan AI terhadap serangan malware.

Permasalahan lainnya adalah Peraturan Perundang-Undangan di Indonesia belum membahas dan mengatur secara detail mengenai eksistensi dari AI. Berdasarkan Pasal 1 Ayat (9) Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta atau yang disingat sebagai UUHC mengkategorikan AI segbagai suatu program computer yang dapat menerima arahan atau perintah yang dinyatakan melalui suatu bahasa, kode, skema dan berbagai bentuk lainnya guna menjadikan sebuah perangkat elektronik yang mampu melakukan fungsi khusus dan hasil yang lebih spesifik. Kemudian Pasal 1 Undang-Undang Nomor 19 Tahun 2016 Informasi dan Transaksi Elektronik atau UU ITE hanya menjelaskan bahwa AI adalah Agen Elektronik, yakni suatu system digital yang didesain untuk dapat mengelola sebuah tindakan kepada informasi elektronik tertentu secara otomatis yang dikelola oleh individu yang bersangkutan. Sebagaimana berdasarkan UU ITE, Pasal 1 Angka 3 Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik juga mengkategorikan AI sebagai Agen Elektronik.

Berdasarkan ketiga aturan diatas maka dapat disimpulkan bahwa hingga saat ini kebijakan dan aturan hukum yang berlaku di negara Indonesia belum membahas dan mengatur secara khusus mengenai eksistensi dari AI, baik dari segi Undang-Undang Hak Cipta dan Undang-Undang Informasi dan Transaksi Elektronik yang masih menggolongkan AI sebagai objek teknologi umum, serta peraturan Pemerintah terkait Penyelenggaraan Sistem dan Transaksi Elektronik sebagai Agen Elektronik. Kurangnya pembahasan mengunai penggunaan AI dalam regulasi negara Indonesia menimbulkan

[9] Hardiansyah Zulfikar, *Kasus Serangan Ransomeware di Indonesia, BI Pernah Jadi sasaran,* https://tekno.kompas.com/read/2023/05/16/14300037/kasus-serangan-ransomware-di-indonesia-bi-pernah-jadi-sasaran diakses 21 Agustus 2024

kekhawatiran pada masyarakat tentang meningkatnya potensi pelanggaran hukum dan tindak kejahatan yang disebabkan oleh AI.

B. METODE PENELITIAN

Jenis penelitian adalah yuridis normatif. Tipe penelitian yuridis normatif yaitu penelitian yang difokuskan untuk mengkaji penerapan kaidah-kaidah atau norma-norma dalam hukum positif. Yuridis normatif yaitu pendekatan yang menggunakan konsepsi *statute approach*.

C. PEMBAHASAN

1. Perlindungan Hukum Bagi Korban Penyalahgunaan Artificial Intelligence (AI) terhadap Serangan Malware Berdasarkan Peraturan Perundang-Undangan

Artificial Intelligence (AI) adalah suatu kemampuan yang dimiliki oleh computer digital atau robot yang dikendalikan oleh computer itu sendiri dengan tujuan untuk memecahkan suatu masalah yang biasanya dikaitkan dengan kemampuan pemrosesan intelektual yang lebih tinggi dari manusia.[10] Knight dan Rich berpendapat bahwa :

"Kecerdasan Buatan atau *Artificial Intelligence* (AI) merupakan suatu bagian dari computer science yang memahami tentang upaya untuk menciptakan computer sebagaimana apa yang dapat dilakukan oleh manusia bahkan lebih baik dari itu".[11]

Pembuatan *Artificial Intelligence* (AI) difokuskan untuk menciptakan suatu kecerdasan buatan yang dimiliki oleh pola piker dan perilaku manusia. Pemanfaatan kekuatan teknologi AI dapat menjadi salah satu item agenda penting yang diiringi dengan perkembangan revolusi industri 4.0 yang artinya kunci dari revolusi ini terletak pada Big Data dan AI.

Perkembangan teknologi *Artificial Intelligence* (AI) yang semakin maju justru membawa dampak penyalahgunaan oleh manusia itu sendiri. Oknum-oknum yang tidak bertanggungjawab ini menjadikan AI sebagai alat baru dalam melakukan aksi kejahatan dalam dunia cyber yaitu penyalahgunaan AI dalam pengambilan data dan pengelola data milik pengguna untuk diretas atau dibobol melalui berbagai jaringan system computer untuk kepentingan pribadinya,

Penyalahgunaan *Artificial Intelligence* (AI) mengacu pada penggunaan teknologi AI yang memiliki tujuan yang merugikan, illegal atau suatu tindakan yang tidak etis. Penyalahgunaan pada AI mempunyai berbagai jenis, diantaranya:

a. *Carding*, yaitu mencuri nomor kartu kredit milik orang lain
b. *Defacing*, yaitu mengalihkan website asli ke website yang lain;
c. *Hacking* dan *cracking*, yaitu memasuki computer atau system elektronik milik orang lain tanpa izin;
d. *Phishing*, yaitu penipuan yang dilakukan pada website yang memiliki nama yang hamper menyerupai website yang asli;
e. *Malware*, yaitu suatu program atau *software* jahat yang menyusup ke dalam computer atau system pada computer;
f. *Spamming*, yaitu proses mengirimkan berita secara berulang-ulang.

[10] Santoso, Joseph Teguh, *Kecerdasan Buatan Dan Jaringan Syaraf Buatan*, Yayasan Prima Agus Teknik, Semarang, 2021, hlm. 2.

[11] Sulistyowati, Indah, *Kecerdasan Buatan (Artificial Intelligence)*, UMSIDA PRESS, Sidoarjo, 2021, hlm. 4.

Penyalahgunaan *Artificial Intelligence* (AI) menyebabkan munculnya suatu potensi bahaya mengenai masalah yang bias dan diskriminasi dalam pengambilan keputusan yang dilakukan oleh AI. Keputusan yang diambil oleh AI sering kali mengalami kekhawatiran tentang privasi dan keamanan data, karena *Artificial Intelligence* (AI) dapat menganalisis, mengumpulkan serta menginterpretasikan data pribadi seseorang dalam skala yang belum pernah terjadi diwaktu sebelumnya.[12]

Penyalahgunaan *Artificial Intelligence* (AI) di Indonesia telah menjadi perhatian pemerintah dan berbagai pemangku kepentingan, khususnya mengenai bagaimana regulasi pengaturan tentang penggunaan *Artificial Intelligence* (AI) yang masih terbatas dan belum diatur secara khusus mengenai potensi bahayanya penyalahgunaan *Artificial Intelligence* (AI) ini terhadap hak asasi manusia.[13]

Kecerdasan Buatan atau *Artificial Intelligence* (AI) saat ini diklasifikasikan sebagai "Agen Elektronik" yang diatur dalam Pasal 1 Angka 8 Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.

Pasal 1 Angka 8 Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik mengklasifikasikan *Artificial Intelligence* (AI) sebagai Agen Elektronik karena AI memiliki kemampuan untuk mengotomatisasikan proses pengambilan informasi dan perangkat system yang mampu untuk melakukan setiap tindakan terhadap informasi elektronik secara otomatis dan terorganisasi.[14]

Aturan lebih lanjut mengenai *Artificial Intelligence* (AI) yaitu Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem Dan Transaksi Elektronik sebagai turunan dari UU ITE. Dalam Pasal 36 hingga Pasal 40 Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem Dan Transaksi Elektronik sebenarnya telah mengatur mengenai batas-batas kewajiban dan tanggungjawab penyedia Agen Elektronik, termasuk menawarkan fitur yang memungkinkan bagi pengguna untuk mengubah informasi ketika transaksi masih berlangsung.[15] Namun, regulasi ini belum membahas secara mendalam mengenai aspek-aspek seperti perlindungan hak asasi manusia, akuntabilitas dan transparansi dalam penggunaan AI.

Lembaga Negara seperti Kementerian Komunikasi dan Informatika (Kominfo) dan Otoritas Jasa Keuangan (OJK) juga telah mengeluarkan pedoman etika mengenai penggunaan AI dalam berbagai sektor. Namun, pedoman ini hanya bersifat sukarela dan tidak memiliki kekuatan hukum yang mengikat.[16]

---

[12] Masrichah, Siti, Ancaman Dan Peluang Artificial Intelligence (AI), *Jurnal Pendidikan dan Sosial Humaniora*, Vol. 3, No. 3, 2023, https://journal.amikveteran.ac.id/index.php/Khatulistiwa/article/download/1860/1467/6316, hlm. 84.

[13] Raharjo, Budi, *Teori Etika Dalam Kecerdasan Buatan (AI)*, Yayasan Prima AGus Teknik, 2023, hlm. 19.

[14] Trunapasha, Adzar Anugrah, Pan Lindawaty Suherman Sewu, dkk, Penyalahgunaan Artificial Intelligence Terhadap Tokoh Masyarakat Dalam Konten Media Sosial Berdasarkan Perundang-Undangan Di Indonesia, *VERITAS: Jurnal Program Pascasarjana Ilmu Hukum*, Vol. 9, No. 2, 2023, https://uia.e-journal.id/veritas/., hlm. 83.

[15] *Ibid*.

[16] Rizki, Mochamad Januar, Mendorong Pemerintah Segera Susun Regulasi Tata Kelola AI Yang Komperhensif, Hukum Online, https://www.hukumonline.com/berita/a/mendorong-

Berdasarkan aturan diatas telah mendeskripsikan bahwa Indonesia memerlukan kajian hukum yang mendalam mengenai potensi dari ancaman bahaya yang ditimbulkan oleh penyalahgunaan *Artificial Intelligence* (AI) terhadap hak asasi manusia. Kajian ini diperlukan untuk mengidentifikasi mengenai celah hukum dan kebutuhan regulasi yang komperehnsif dalam pengaturan mengenai penggunaan *Artificial Intelligence* (AI) secara bertanggungjawab dan melindungi hak-hak fundamental bagi warga negara.

Perkembangan teknologi *Artificial Intelligence* (AI) atau yang biasa disebut Kecerdasan Buatan telah membuka peluang baru dalam bidang kriminologi, yaitu penyalahgunaan *Artificial Intelligence* (AI) berupa serangan *Malware*. Serangan *Malware* memanfaatkan *Artificial Intelligence* (AI) untuk menciptakan suatu serangan virus berbahaya yang menyerang system jaringan pada computer dan pencurian pada data pribadi pengguna yang melibatkan eksploitasi Kecerdasan Buatan dalam peretasan system computer.

Menurut Badan Siber dan Sandi Negara (BSSN), total 411.000 anomali traffic atau serangan malware yang terjadi pada sistem computer di setiap harinya pada tahunm 2023. Hal ini dikarenakan serangan *Malware* berjenis *Ransomeware* ini memiliki teknologi yang lebih mutakhir karena tidak telihat. Merujuk pada data Kaspersky (perusahaan keamanan siber anti-virus) kejahatan siber di Indonesia yang menggunakan serangan Malware berjenis Ransomeware kepada pengguna terdeteksi sebanyak 97.226 per Januari hingga Desember pada 2023. Keadaaan ini menyebabkan 52% system keamanan siber di Indonesia menjadi lebih sulit dalam menangani serangan malware disbanding 3 tahun terakhir.[17]

Serangan *Malware* memiliki tekhnologi yang lebih mutakhir sehingga proses pembobolan pada system computer menjadi lebih efesien karena virus *malware* tidak terlalu mencolok. Metode ini memungkinkan otomatisasi hanya dengan mengeksploitasi celah pada system komputer dan kebocoran kredensial (pasangan username dan password) yang telah ada sebelumnya.

Serangan *malware* sendiri sudah banyak terjadi di kalangan masyarakat Indonesia. Salah satu contonya adalah kasus yang terjadi pada pertengahan Mei 2023, Bank Syariah Indonesia (BSI) menjadi korban dari seranngan *Malware* berjenis *Ransomeware Lockbit* 3.0 dengan total data yang berhasil dibobol diduga mencapai 1,5 *terrabyte* (TB). Data yang telah dibobol tersebut merupakan data pelanggan yang diantaranya seperti nama, nomor ponsel, saldo rekening, Riwayat transasksi, informasi pekerjaan dan beberapa data privasi milik nasabah Bank Syariah Indonesia (BSI).[18]

Pelaku peretasan yang terjadi pada Bank Syariah Indonesia (BSI) ini telah mencuri data sebanyak 15 juta nasabah dan telah mengambil sekitar 1,5 *terrabyte* data internal Bank Syariah Indonesia (BSI) tersebut. Pelaku peretas *Lockbit* ini meminta tebusan

pemerintah-segera-susun-regulasi-tata-kelola-ai-yang-komperhensif-lt66333a6b06c16/. diakses 29 Oktober 2024.

[17] CNN Indonesia, Serangan Siber Menggila, 411 Ribu Malware Baru Muncul Tiap Hari di RI, https://www.cnnindonesia.com/teknologi/20240522130109-185-1100872/serangan-siber-menggila-411-ribu-malware-baru-muncul-tiap-hari-di-ri, diakses 29 Oktober 2024.

[18] Artikel DJKN, Ransomeware, Ancaman dan Langkah-Langkat Untuk Menghindarinya, https://www.djkn.kemenkeu.go.id/kanwil-jabar/baca-artikel/16188/Ransomware-Ancaman-dan-Langkah-Langkah-untuk-Menghindarinya.html, diakses 29 Oktober 2024

sebesar US$ 20 juta atau sekitar Rp. 296 miliar kepada Bank Syariah Indonesia (BSI) agar mereka tidak membocorkan data nasabah Bank Syariah Indonesia (BSI).[19]

Lockbit merupakan grup peretas berskala global yang menjalankan bisnis berupa *Ransomeware As A Service* (RAAS) yaitu sebagai layanan model bisnis kejahatan siber yang mana para pengembang *Ransomeware* menjual *Malware* mereka ke peretas yang lain.[20]

Selanjutnya 7 November 2024 serangan *Malware* kembali terjadi pada serangan siber yang menargetkan pengguna PC Windows melalaui iklan pada web berbahaya. Modus ini berlangsung ketika pengguna sedang melakukan browsing, kemudian tanpa sadar mengklik iklan yang menutupi seluruh layer hingga membuat konten tak terlihat.[21]

Iklan yang telah muncul terbut akan mengarahkan pengguna ke halaman *Captcha* palsu dan pesan kesalahan Chrome palsu untuk mengelabuhi pengguna agar mengunduh *Malware* berbahaya yang dikenal sebagai *stealer*. *Captcha* merupakan fitur keamanan yang digunakan pada situs web dan aplikasi untuk memverifikasi apakah pengguna adalah manusia atau program atau bot otomatis.[22]

Bagi pengguna yang telah mengklik tombol "saya bukan robot" maka skrip berbahaya akan disalin ke clipboard pengguna, kemudian pengguna diminta untuk menempelkan ke terminal, yang akhirnya akan mengunduh dan meluncurkan trojan seperti Lumma. Malware ini dirancang untuk mencuri informasi sensitive seperti asset kripto, cookie, dan data pengelola kata sandi. Para hacker juga akan mengambil tangkapan layer, memperoleh kredensial untuk layanan akses jarak jauh, dan mengontrol perangkat korban dengan mengunduh alat akses jarak jauh.

Dari beberapa contoh kasus tersebut menunjukkan bahwa perkembangan *Artificial Intelligence* (AI) membawa potensi bahaya yang signifikan bagi masyarakat khususnya terhadap serangan *Malware* yang semakin banyak terjadi di Indonesia, dimana bentuk-bentuk penyalahgunaan *Artificial Intelligence* (AI) yang paling banyak terjadi adalah dalam bentuk penyebaran data pribadi seseorang yang disebarluaskan dan dibagikan secara umum ke public untuk suatu tindakan yang tidak etis dan merugikan tanpa sepengetahuan dari pemilik.[23].

Perlindungan data diri seseorang sangat penting dilakukan karena untuk mencegah terjadinya pencurian terhadap identitas pribadi, terjadinya penipuan, bahkan mencegah terjadinya kejahatan pada dunia maya yang kini telah marak terjadi. Perlindungan data pribadi juga merupakan bagian dari Hak Asasi Manusia (HAM), serta negara wajib untuk melindungi kerahasiaan data pribadi seseorang.

---

[19] Diah, Dini, & Fakta Dugaan Serangan Ransomeware Oleh Lockbit Ke BSI, https://koran.tempo.co/read/berita-utama/482085/7-fakta-dugaan-serangan-ransomware-oleh-lockbit-ke-bsi, diakses 29 Oktober 2024.

[20] IBM, Apa Itu Ransomeware-as-a-Service (RaaS)?, https://www.ibm.com/id-id/topics/ransomware-as-a-service, diakses 29 Oktober 2024.

[21] Bima, Modus Penipuan 'Saya Bukan Robot' Mengintai, Awas Rekening Bisa Terkuras!, https://gamebrott.com/modus-penipuan-saya-bukan-robot-mengintai/, diakses pada 7 November 2024.

[22] Syiroojuddin, Julian, Awas Captcha 'Saya Bukan Robot' Dijadikan Modus Baru Penipuan Online, https://jabarekspres.com/berita/2024/11/08/awas-captcha-saya-bukan-robot-dijadikan-modus-baru-penipuan-online/, diakses pada 8 November 2024.

[23] Yuniarti, Siti, Perlindungan Hukum Data Pribadi Di Indonesia, *Jurnal BECOSS*, Vol. 1. No. 1, 2020, https://journal.binus.ac.id/index.php/BECOSS/article/view/6030, hlm.148.

Permasalahannya adalah regulasi yang ada seperti Undang-Undang Informasi dan Transaksi Elektronik dan peraturan terkait belum ada yang mengatur sejara jelas dalam mengatasi serangan *Malware* terhadap data diri atau pribadi seseorang. Saat ini Perlindungan privasi dan data pribadi seseorang masih diatur dalam pasal 28G Undang-Undang Dasar Republik Indonesia Tahun 1945, yaitu :

"setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat dan harta bendayang dibawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi".

Akan tetapi, perlindungan data pribadi itu hanya sebatas diatur dalam Undang-Undang Dasar 1945. Sementara itu Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik serta Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik belum membahas secara khusus mengenai perlindungan terhadap perivasi, termasuk juga membahas perlindungan terhadap korban kejahatan penyalahgunaan AI.

Pada hal ini Pasal 4, Pasal 26, Pasal 27, dan Pasal 30 Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) hanya membahas perlindungan hukum bagi korban penyalahgunaan pemanfaatan teknologi informasi dan transaksi elektronik secara umum. Sedangkan perlindungan hukum terhadap korban penyalahgunaan *Artificial Intelligence* (AI) terhadap serangan *Malware* belum diatur secara khusus dan jelas.

Penggunaan *Artificial Intelligence* (AI) dalam Peraturan Perundang-Undangan di Indonesia yaitu Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 digolongkan hanya sebagai Agen Elektronik. Akibatnya penggunaan AI masih sulit untuk diawasi. Padahal Penggunaan *Artificial Intelligence* (AI) tanpa pengawasan merupakan hal yang sangat berbahaya, mekipun *Articial Intelligence* (AI) adalah kecerdasan buatan, namun program AI sendiri tidak memiliki moral. *Artificial Intelligence* (AI) tidak memiliki pengetahuan mengenai tindakan yang diperbuat apakah tindakan tersebut benar atau salah.

Berdasarkan kondisi tersebut, maka dampak yang terjadi saat ini ialah korban penyalahgunaan *Artificial Intelligence* (AI) yang belum mendapatkan bentuk perlindungan yang diatur secara jelas dan lebih efesien, sehingga korban mengalami kekhawatiran dan merasakan ketidakseimbangan dalam pengayoman hukum terhadap korban. Padahal perlindungan hukum menjadi salah satu upaya untuk mengembalikan kerugian yang dialami oleh korban penyalahgunaan *Artificil Intelligence* (AI).

2. Kebijakan Hukum Terhadap Pengaturan Bagi Korban Penyalahgunaan Artificial Intelligence (AI) di Masa Mendatang

Perkembangan Kecerdasan Buatan atau *Artificial Intelligence* (AI) telah memberikan dampak yang sangat besar terhadap berbagai aspek kehidupan masyarakat di Indonesia, yang mana diantaranya aspek hukum, ekonomi, social, dan lain sebagainya. Peluang yang dihasilkan oleh kemajuan *Artificial Intelligence* (AI) telah menunjukkan bahwa potensi AI telah mendorong secara signifikan dalam berbagai sektor dan meningkatkan kualitas hidup manusia.[24] Meski demikian, dibalik banyaknya manfaat *Artificial*

[24] Masrichah, S, Ancaman Dan Peluang Artificial Intelligence (AI), Khatulistiwa : *Jurnal Pendidikan dan Sosial Humaniora*, Vol. 3, No. 3, https://journal.amikveteran.ac.id/index.php/Khatulistiwa/article/download/1860/1467/6316, hlm. 84.

Intelligence (AI) terhadap masyarakat di Indonesia, penerapan AI juga menghadirkan dampak dan resiko yang akan membutuhkan regulasi khusus.

Penggunaan *Artificial Intelligence* (AI) tanpa pengawasan merupakan hal yang sangat berbahaya, mekipun *Articial Intelligence* (AI) kecerdasan buatan, namun program AI sendiri tidak memiliki moral. *Artificial Intelligence* (AI) tidak memiliki pengetahuan mengenai tindakan yang diperbuat apakah tindakan tersebut benar atau salah. AI hanya menjalankan sistem berdasarkan perintah, yang artinya semua tindakan AI tergantung pada penggunanaya.

Indonesia hingga saat ini belum ada pembahasan lebih lanjut mengenai *Artificial Intelligence* (AI) dan pengaruhnya terhadap hukum di Indonesia. Indonesia belum mempunyai aturan hukum apapun yang membahas secara khusus mengenai robot-robot pintar yang dihasilkan oleh *Artificial Intelligence* (AI). Saat ini, Indonesia mengandalkan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Dalam UU ITE ini mengatur mengenai perlindungan data pribadi dan hak privasi individu, menetapkan aturan hukum yang terkait informasi dan teknologi, serta berfungsi sebagai kerangka hukum dalam berbagai aspek digital.[25]

Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) sudah tidak memadai dalam menangani berbagai kejahatan cyber yang semakin sering muncul seiring dengan majunya perkembangan *Artificial Intelligence* (AI). Modus kejahatan yang melibatkan *Artificial Intelligence* (AI) semakin beragam dan kompleks sehingga perlunya pembaharuan hukum yang lebih relevan dan spesifik terhadap kemajuan dari *Artificial Intelligence* (AI).

Korban dari penyalahgunaan *Artificial Intelligence* (AI) ini seharusnya mendapatkan perlindungan hukum yang efektif dengan diperlukannya kerjasama pemerintah dalam memberikan regulasi yang jelas untuk meningkatkan peraturan mengenai pencegahan dan penanganan dalam pelaku Penyalahgunaan *Artificial Intelligence* (AI).

Korban penyalahgunaan *Artificial Intelligence* (AI) harus mendapatkan kebijakan mengenai serangan dari penyalahgunaan AI. Kebijakan hukum terkait dengan perlindungan hukum bagi korban penyalahgunaan *Artificial Intelligence* (AI) terhadap serangan *Malware*. Adapun bentuk-bentuk kebijakan yang dapat dilakukan diantaranya sebagai berikut:

1. Regulasi yang ketat

   Regulasi yang ketat dalam penggunaan *Artificial Intelligence* (AI) mengacu pada serangkaian aturan dan pedoman dalam penggunaan AI, yang dirancang untuk memastikan bahwa pengembangan dari penerapan *Artificial Intelligence* (AI) dilakukan secara tanggung jawab, etis, dan aman.
2. Kerangka Etika

   Kerangka etika dalam pencegahan pada penyalahgunaan *Artificial Intelligence* (AI) adalah seperangkat prinsip dan pedoman yang mengatur mengenai pengembangan, penggunaan, dan dampak pada penggunaan *Artificial Intelligence* (AI).

[25] Martinelli, Imelda, Yohana, Cora Vanessa, dan Hiumawan, Urgensi Pengaturan dan Perlindungan Rights Of Privacy Terhadap Artificial Intelligence Dalam Pandangan Hukum Sebagai Sosial Engineeering, *Jurnal Tana Mana*, Vol.4, No.2, http://ojs.staialfurqan.ac.id/jtm/article/download/415/323, hlm.158

3. Pendidikan dan kesadaran

   Pendidikan dan kesadaran dalam pencegahan penyalahgunaan *Artificial Intelligence* (AI) merupakan aspek yang sangat penting untuk memastikan apakah teknologi ini digunakan secara bertanggung jawab dan etis atau tidak. Hal ini berupaya untuk meningkatkan pemahaman masyarakat tentang apa saja manfaat dan risiko yang timbul dari penggunaan *Artificial Intelligence* (AI)

4. Perlindungan hukum yang lebih kuat

   Pemerintah harus mengembangkan regulasi yang lebih spesifik dan efesien untuk melindungi korban penyalahgunaan *Artificial Intelligence* (AI) seperti serangan Malware dan kekerasan serta ancaman berbasis elektronik, dengan sanksi yang tegas.[26] Perlindungan hukum yang lebih kuat ini salah satunya gunakan untuk melindungi data pribadi seseorang agar tidak terjadinya suatu penyalahgunaan pada data pribadi seseorang yang diakibatkan oleh penyalahgunaan pada *Artificial Intelligence* (AI).

5. Sistem sanksi pidana yang jelas

   Peraturan Pemerintah harus menetapkan system sanksi pidana yang komperhensif, termasuk denda dan hukuman penjara bagi pelaku penyalahgunaan *Artificial Intelligence* (AI) agar pelaku mendapatkan efek jera. Sistem sanksi pidana yang jelas terhadap pelaku penyalahgunaan *Artificial Intelligence* (AI) mengacu pada kerangkat hukum yang tegas dan jelas, baik jelas mengeani aturan konsekuensi hukum bagi pelaku yang telah melanggar hukum.

Berdasarkan penjelasan diatas, kebijakan hukum tersebut sangat penting dilakukan oleh negara dalam pengayoman bagi warga negara yang telah menjadi korban dari penyalahgunaan *Artificial Intelligence* (AI), sebagai bentuk dari upaya untuk memberikan batasan yang jelas mengenai regulasi penggunaan *Artificial Intelligence* (AI) di Indonesia.

Regulasi kebijakan hukum terhadap *Artificial Intelligence* (AI) mencakup mengenai beberapa bentuk, yaitu perlindungan terhadap hak-hak korban berupa perlindungan identitas dan informasi mereka, pendampingan hukum, dan informasi mengenai proses hukum. Selanjutnya, memberikan pertanggungjawaban yang sesuai dengan perbuatan pelaku, serta meminimalisir penyalahgunaan *Artificial Intelligence* (AI) yaitu mengenai pengembangan system keamanan yang kuat di Indonesia, hal ini bertujuan untuk melindungi data dan algoritma pada Artificial Intelligence (AI) dari tindakan manipulasi dan akses yang tidak sah.

D. SIMPULAN

Perlindungan hukum bagi korban penyalahgunaan *Artificial Intelligence* (AI) khususnya pada kasus serangan Malware masih belum efektif di Indonesia. Meskipun terdapat regulasi yang ada, seperti Pasal 28 D Ayat (1) Undang-Undang Dasar 1945 yang menjamin hak atas perlindungan hukum. Akan tetapi, penerapannya belum jelas dan komperhensif. Selanjutnya, implementasi Undang-Undang Informasi dan Transaksi Elektronik menggolongkan *Artificial Intelligence* (AI) sebagai Agen Elektronik, sehingga

[26] Putra, Izil Hidayat, Perlindungan Hukum Terhadap Korban Penyalahgunaan Artificial Intelligence (AI) Berupa Deepfake Pornografi Menurut Peraturan Perundang-Undangan, UNJA Journal of LegalStudies, Vol. 01, No. 02, 2023, https://online-journal.unja.ac.id/jols/article/download/33080/18366/104186, hlm. 120.

Artificial Intelligence (AI) belum disebutkan secara gramatikal pada aturan tersebut. Kebijakan hukum pidana terhadap perlindungan bagi korban penyalahgunaan *Artificial Intelligence* (AI) terhadap serangan *Malware* di Indonesia belum bersifat konkrit dan tegas dalam melakukan suatu perbaikan atau pembuatan peraturan khusus mengenai *Artificial Intelligence* (AI) yang didalamnya mengatur tentang ketentuan mengenai batasan-batasan secara jelas dan mengikat dalam pengolahan system kerja kecerdasan buatan ini. Kebijakan mengenai *Artificial Intelligence* (AI) harus diatur secara tegas mengenai sanksi pidana pada serangan *Malware* yang memanfaatkan kecerdasan buatan, dan memberikan penjelasan dalam aturan terkait perlindungan terhadap korban penyalahgunaan *Artificial Intelligence* (AI) berupa serangan *Malware* untuk mencegah dan menanggulangi tindak pidana tersebut, serta memberikan hak-hak yang harus didapatkan korban dari penyalahgunaan *Artificial Intelligence* (AI).

DAFTAR PUSTAKA

Adzar Anugrah Trunapasha, Pan Lindawaty Suherman Sewu, dkk, Penyalahgunaan Artificial Intelligence Terhadap Tokoh Masyarakat Dalam Konten Media Sosial Berdasarkan Perundang-Undangan Di Indonesia, *VERITAS: Jurnal Program Pascasarjana Ilmu Hukum*, Vol. 9, No. 2, 2023, https://uia.e-journal.id/veritas/.

Artikel DJKN, Ransomeware, Ancaman dan Langkah-Langkat Untuk Menghindarinya, https://www.djkn.kemenkeu.go.id/kanwil-jabar/baca-artikel/16188/Ransomware-Ancaman-dan-Langkah-Langkah-untuk-Menghindarinya.html

Bima, Modus Penipuan 'Saya Bukan Robot' Mengintai, Awas Rekening Bisa Terkuras, https://gamebrott.com/modus-penipuan-saya-bukan-robot-mengintai/

Budi Raharjo, *Teori Etika Dalam Kecerdasan Buatan (AI)*, Yayasan Prima AGus Teknik, 2023

CNN Indonesia, Serangan Siber Menggila, 411 Ribu Malware Baru Muncul Tiap Hari di RI, https://www.cnnindonesia.com/teknologi/20240522130109-185-1100872/serangan-siber-menggila-411-ribu-malware-baru-muncul-tiap-hari-di-ri

Diah, Dini, & Fakta Dugaan Serangan Ransomeware Oleh Lockbit Ke BSI, https://koran.tempo.co/read/berita-utama/482085/7-fakta-dugaan-serangan-ransomware-oleh-lockbit-ke-bsi

Donovan Typhano Rachmadie dan Supanto, "Regulasi Penyimpangan Artificial Intelligence Pada Tindak Pidana Malware Berdasarkan Undang-Undang Republik Indonesia Nomor 19 Tahun 2016", *Recidive* Volume 9 No. 2, 2020, https://jurnal.uns.ac.id/recidive/article/download/47400/29634

Emi Sita Eriana dan Afrizal Zein, *Artificial Intelligence (AI)*, CV. Media Aksara, Bojongsari, 2023

Hafrida et al., "Students' Perception of the Criminalization of Cohabitation (Kumpul Kebo) in Indonesia: From Quantitative to Normative Analysis," *Jambe Law Journal* 7, no. 1 (July 22, 2024): 127–47, https://doi.org/DOI: https://doi.org/10.22437/home.v7i1.340.

Hardiansyah Zulfikar, *Kasus Serangan Ransomeware di Indonesia, BI Pernah Jadi sasaran,* https://tekno.kompas.com/read/2023/05/16/14300037/kasus-serangan-ransomware-di-indonesia-bi-pernah-jadi-sasaran

Hendri Diansah, Usman, dan Yulia Monita, Kebijakan Hukum Pidana Terhadap Tindak Pidana *Carding*, *PAMPAS: Journal Of Criminal*. Volume: 3, Nomor: 1, 2022, https://online-journal.unja.ac.id/Pampas/article/download/17704/13283

Herlyanty Bawole, "Perlindungan Hukum Terhadap Korban Kejahatan", *Jurnal LEGALITAS* Volume 2 Nomor 2, Desember 2017, http://ejurnal.untag-smd.ac.id/index.php/LG/article/download/3382/3293

IBM, Apa Itu Ransomeware-as-a-Service (RaaS)?, https://www.ibm.com/id-id/topics/ransomware-as-a-service

Imelda Martinelli, Yohana, Cora Vanessa, dan Hiumawan, Urgensi Pengaturan dan Perlindungan Rights Of Privacy Terhadap Artificial Intelligence Dalam Pandangan Hukum Sebagai Sosial Engineeering, *Jurnal Tana Mana*, Vol.4, No.2, http://ojs.staialfurqan.ac.id/jtm/article/download/415/323

Indah Sulistyowati, *Kecerdasan Buatan (Artificial Intelligence)*, UMSIDA PRESS, Sidoarjo, 2021

Izil Hidayat Putra, Perlindungan Hukum Terhadap Korban Penyalahgunaan Artificial Intelligence (AI) Berupa Deepfake Pornografi Menurut Peraturan Perundang-Undangan, UNJA Journal of LegalStudies, Vol. 01, No. 02, 2023, https://online-journal.unja.ac.id/jols/article/download/33080/18366/104186

Joseph Teguh Santoso, *Kecerdasan Buatan Dan Jaringan Syaraf Buatan*, Yayasan Prima Agus Teknik, Semarang, 2021

Mochamad Januar Rizki, Mendorong Pemerintah Segera Susun Regulasi Tata Kelola AI Yang Komperhensif, Hukum Online, https://www.hukumonline.com/berita/a/mendorong-pemerintah-segera-susun-regulasi-tata-kelola-ai-yang-komperhensif-lt66333a6b06c16/.

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

Rena Yulia dan Aliyth Prakarsa, "Perlindungan Hukum Terhadap Korban Kejahatan Praktik Kedokteran Ilegal", *Jurnal.komisiyudisial.go.id E-ISSN:2579-4868; P-ISSN: 1978-6506* Vol. 13 No. 1, 2020, https://jurnal.komisiyudisial.go.id/index.php/jy/article/download/341/pdf/2602

Roebiono Kartopati, *Lanskap Keamanan Siber Indonesia*, Direktorat Operasi Keamanan Siber, Jakarta, 2023

Satjipto Rahardjo, *Ilmu Hukum*, PT. Citra Aditya Bakti, Bandung, 2000

Siti Masrichah, Ancaman Dan Peluang Artificial Intelligence (AI), *Jurnal Pendidikan dan Sosial Humaniora*, Vol. 3, No. 3, 2023, https://journal.amikveteran.ac.id/index.php/Khatulistiwa/article/download/1860/1467/6316

Siti Yuniarti, Perlindungan Hukum Data Pribadi Di Indonesia, *Jurnal BECOSS*, Vol. 1. No. 1, 2020, https://journal.binus.ac.id/index.php/BECOSS/article/view/6030

Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.