AKADEMIK E-ISSN 2774-8863
Jurnal Mahasiswa Humanis
Vol. 5, No. 2, Mei 2025

Analisis Yuridis Perlindungan Hukum terhadap Korban Kejahatan Berbasis Teknologi Kecerdasan Buatan/*Artificial Intelligence (AI)*

Elfrida Tipe Obe[1], Aksi Sinurat[2], Rosalind Angel Fanggi[3]
Universitas Nusa Cendana Kupang, Indonesia
ridaobe16@gmail.com[1], sinurataksi12@gmail.com[2], rosalind_fanggi@yahoo.com[3]

Submitted: 24th March 2025 | **Edited**: 28th April 2025 | **Issued**: 01st May 2025

Cited on: Obe, E. T., Sinurat, A., & Fanggi, R. A. (2025). Analisis Yuridis Perlindungan Hukum terhadap Korban Kejahatan Berbasis Teknologi Kecerdasan Buatan/Artificial Intelligence (AI). *AKADEMIK: Jurnal Mahasiswa Humanis, 5*(2), 1144-1156.

ABSTRACT

Artificial Intelligence (AI) based crimes are a modern form of criminal offense that exploits AI technology to harm individuals or groups. This study aims to analyze existing legal frameworks and the challenges in implementing legal protection for victims of AIbased crimes. The research focuses on two main questions: (1) How is the legal framework structured for victims of AI related crimes? and (2) What are the implementation challenges and possible solutions for ensuring legal protection? The research uses a normative legal method through literature review and secondary data analysis. The findings reveal that while several laws can be applied to prosecute offenders, the protection of victims remains insufficient and lacks explicit regulation. Key challenges include regulatory gaps, difficulties in tracing and proving AI-related offenses, limited human and technological resources in law enforcement, and issues of privacy and data security. To address these challenges, it is necessary to formulate AI-specific regulations, establish accessible and responsive reporting mechanisms, raise public awareness, and create specialized law enforcement bodies. The study recommends legal reform that prioritizes the protection of victims' rights in the face of emerging digital threats.

Keywords: Artificial Intelligence, Victims, Legal Protection

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan besar dalam berbagai aspek kehidupan manusia. Salah satu teknologi yang berkembang pesat saat ini adalah kecerdasan buatan (Artificial Intelligence/AI), yang memungkinkan mesin meniru proses berpikir dan pengambilan keputusan manusia. Teknologi ini banyak digunakan dalam bidang ekonomi, pendidikan, keamanan, hingga layanan digital, namun di sisi lain juga membuka peluang penyalahgunaan dalam bentuk kejahatan siber (Pratiwi, 2024).

Kejahatan berbasis AI merupakan bentuk tindak pidana yang menggunakan algoritma dan kecanggihan teknologi untuk merugikan pihak lain, baik secara finansial

maupun psikologis. Salah satu contoh nyatanya adalah kasus kebocoran data Tokopedia pada tahun 2020, yang melibatkan jutaan data pengguna dan kemungkinan pemanfaatan teknologi AI oleh pelaku untuk meretas sistem keamanan (Alkindyweb, 2022). Selain peretasan, bentuk kejahatan lain yang memanfaatkan AI adalah deepfake, yakni manipulasi suara atau gambar yang dapat merusak reputasi seseorang dan menyebarkan informasi palsu (Hafsyari, 2023).

Tipe pelaku kejahatan berbasis AI bervariasi, dari pelaku profesional dengan keahlian teknis tinggi hingga pengguna awam yang memanfaatkan alat AI secara ilegal. Korban dari kejahatan ini juga beragam, mulai dari tokoh publik hingga masyarakat biasa, yang bisa mengalami kerugian ekonomi, trauma psikologis, dan pencemaran nama baik. Namun, perangkat hukum di Indonesia, seperti Undang-Undang Informasi dan Transaksi Elektronik (ITE), belum secara khusus mengatur penggunaan AI dalam konteks tindak pidana, sehingga menyulitkan proses penegakan hukum (Mahardika & Priancha, 2021).

Kesenjangan antara kemajuan teknologi dengan regulasi hukum menyebabkan lemahnya perlindungan terhadap korban kejahatan berbasis AI. Pembuktian yang sulit, keterbatasan aparat penegak hukum dalam memahami teknologi, serta rendahnya literasi digital masyarakat menjadi hambatan serius. Oleh karena itu, diperlukan kajian mendalam mengenai regulasi dan implementasi perlindungan hukum yang lebih adaptif terhadap perkembangan teknologi AI guna menjamin keadilan dan kepastian hukum (Iswanto, 2024; Jamaaluddin & Sulistyowati, 2021).

LANDASAN TEORI

Pengertian Perlindungan Hukum

Perlindungan hukum merupakan suatu upaya yang diberikan oleh negara melalui instrumen hukum untuk menjamin dan melindungi hak-hak warga negara dari segala bentuk pelanggaran, ancaman, dan ketidakadilan. Perlindungan ini mencakup aspek preventif dan represif yang bertujuan menciptakan rasa aman serta menjamin kepastian hukum bagi individu maupun kelompok. Supanto dan Aryani (2018) menjelaskan bahwa perlindungan hukum melibatkan tindakan yang sistematis dari negara untuk memastikan warga negara memperoleh keadilan dan tidak mengalami diskriminasi dalam penegakan hukum. Sementara itu, Sari dan Wardani (2019) menekankan bahwa perlindungan hukum

erat kaitannya dengan pemulihan hak, partisipasi korban dalam proses hukum, serta akses terhadap keadilan yang efektif dan tidak diskriminatif.

Secara normatif, pengertian perlindungan hukum juga ditegaskan dalam Pasal 1 angka 6 Undang-Undang Nomor 31 Tahun 2014 tentang Perlindungan Saksi dan Korban, yang menyebutkan bahwa perlindungan adalah segala bentuk upaya pemenuhan hak dan bantuan untuk menjamin rasa aman kepada saksi dan/atau korban, yang pelaksanaannya menjadi tanggung jawab Lembaga Perlindungan Saksi dan Korban (LPSK) atau institusi terkait lainnya. Ketentuan tersebut menunjukkan bahwa perlindungan hukum tidak hanya bersifat konseptual, tetapi juga memiliki legitimasi yuridis yang kuat. Oleh karena itu, perlindungan hukum harus dilihat sebagai instrumen penting dalam menjamin keadilan, melindungi hak asasi manusia, dan menegakkan supremasi hukum dalam suatu negara hukum yang demokratis (Prabowo, 2020; Lestari, 2017).

Pengertian dan Jenis-jenis Korban

Korban tindak pidana tidak terbatas pada individu perorangan, melainkan juga dapat mencakup kelompok masyarakat, badan hukum, bahkan dalam kasus tertentu, lingkungan hidup seperti ekosistem. Secara umum, korban adalah pihak yang mengalami penderitaan fisik, mental, atau kerugian ekonomi akibat tindakan yang bertentangan dengan hukum dan hak asasi manusia. Dalam sistem hukum Indonesia, korban dibedakan menjadi dua jenis, yaitu korban langsung dan korban tidak langsung. Korban langsung merasakan dampak langsung dari tindak pidana, seperti luka fisik, trauma, atau kerugian materi. Sementara itu, korban tidak langsung merasakan dampak secara tidak langsung, misalnya keluarga korban atau pihak yang bergantung pada korban langsung.

Undang-Undang Nomor 31 Tahun 2014 memberikan landasan hukum yang kuat atas hak-hak korban dalam proses hukum. Pasal 5 UU tersebut menetapkan berbagai hak, termasuk perlindungan terhadap ancaman fisik dan psikologis, hak untuk berpartisipasi dalam menentukan bentuk perlindungan, serta hak untuk memperoleh informasi terkait perkembangan perkara. Selain itu, korban juga berhak atas bantuan hukum, penerjemah, pemulihan identitas, penggantian biaya hidup, serta pendampingan selama proses hukum berlangsung. Hak-hak tersebut menunjukkan bahwa negara memiliki tanggung jawab aktif dalam memastikan perlindungan menyeluruh terhadap korban sebagai bagian dari prinsip keadilan dan pemenuhan hak asasi manusia.

Kecerdasan Buatan atau *Artificial Intelligence (AI)*

Kecerdasan buatan (*Artificial Intelligence/AI*) dapat didefinisikan dalam beberapa cara yang saling melengkapi. Pertama, AI dapat dipahami sebagai otomasi aktivitas yang berhubungan dengan pemikiran manusia, seperti pembuatan keputusan, penyelesaian masalah, dan pembelajaran, yang dilakukan oleh sistem komputer yang mampu berpikir seperti manusia. Kedua, AI juga dianggap sebagai seni dalam menciptakan mesin yang mampu menjalankan fungsinya, yang dalam situasi tertentu, membutuhkan kecerdasan manusia untuk menyelesaikan tugas tersebut, sehingga sistem ini bertindak seperti manusia. Ketiga, AI bisa diartikan sebagai studi tentang komputasi yang berupaya memahami penalaran dan tindakan, yakni sistem yang berpikir secara rasional. Keempat, AI juga merupakan cabang ilmu komputer yang mempelajari otomasi perilaku kecerdasan atau berusaha menandingi perilaku kecerdasan manusia dalam proses komputasi, yakni sistem yang bertindak secara rasional (Jamaaluddin & Sulistyowati, 2021). Dengan menggabungkan keempat definisi ini, dapat disimpulkan bahwa kecerdasan buatan adalah bagian dari ilmu komputer yang bertujuan menciptakan mesin atau sistem yang memiliki kecerdasan mirip dengan manusia.

METODE PENELITIAN

Penelitian ini menggunakan jenis penelitian hukum normatif, yaitu penelitian yang bertumpu pada studi kepustakaan dan analisis terhadap norma-norma hukum positif yang berlaku. Fokus utamanya adalah menganalisis perlindungan hukum terhadap korban kejahatan berbasis teknologi kecerdasan buatan (Artificial Intelligence/AI). Pendekatan yang digunakan adalah pendekatan deskriptif kualitatif. Pendekatan ini relevan untuk mengkaji substansi hukum terkait penggunaan AI dalam tindak pidana, serta untuk menilai sejauh mana perangkat hukum yang ada mampu memberikan perlindungan secara efektif kepada korban (Salim & Nurbani, 2020).

Sumber data yang digunakan dalam penelitian ini adalah data sekunder yang terdiri dari bahan hukum primer dan sekunder. Bahan hukum primer meliputi peraturan perundang-undangan seperti Undang-Undang Dasar 1945, Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Undang-Undang Perlindungan Saksi dan Korban, Undang-Undang Perlindungan Data Pribadi, serta Undang-Undang Pornografi. Sementara itu, bahan hukum sekunder mencakup literatur akademik, jurnal hukum,

artikel ilmiah, serta dokumen relevan lainnya yang mendukung analisis hukum terhadap kejahatan berbasis AI. Teknik pengumpulan data dilakukan melalui studi dokumen dan literatur, sedangkan teknik analisis dilakukan secara kualitatif normatif dengan pendekatan perspektif, yaitu dengan menilai sejauh mana norma hukum yang ada sesuai atau tidak sesuai dengan kebutuhan perlindungan hukum bagi korban kejahatan AI (Marzuki, 2017; Fitriani, 2021).

HASIL PENELITIAN

Pengaturan Hukum Terhadap Korban Kejahatan Berbasis Teknologi Kecerdasan Buatan/ *Artificial intelligence* (AI)

Perkembangan teknologi kecerdasan buatan (Artificial Intelligence/AI) menghadirkan tantangan baru dalam dunia hukum, terutama terkait perlindungan terhadap korban. Dalam konteks hukum Indonesia, AI dikategorikan sebagai agen elektronik sebagaimana diatur dalam UU No. 1 Tahun 2024 tentang Perubahan Kedua atas UU ITE. AI memiliki kemampuan otomatisasi dan pengambilan keputusan tanpa intervensi langsung manusia, sehingga penggunaannya dapat menimbulkan risiko pelanggaran hak, seperti penyalahgunaan data pribadi, penyebaran konten manipulatif (deepfake), dan pelanggaran privasi (Mahardika & Priancha, 2021). Meskipun UU ITE telah mengatur larangan terhadap konten bermuatan kesusilaan dan manipulasi informasi elektronik, ketentuan ini belum secara komprehensif menyentuh perlindungan hukum bagi korban kejahatan yang menggunakan teknologi AI sebagai sarana.

Regulasi yang tersedia, seperti Pasal 26, 27, 35, dan 45 UU ITE, memang memberikan dasar hukum untuk menindak pelaku kejahatan digital, termasuk penyalahgunaan teknologi AI. Namun, perlindungan terhadap korban masih bergantung pada ketentuan umum, bukan ketentuan khusus yang dirancang untuk menjawab kompleksitas kejahatan berbasis AI. Sementara itu, hak-hak korban lebih banyak dijelaskan dalam UU No. 13 Tahun 2006 tentang Perlindungan Saksi dan Korban. Meski undang-undang tersebut memberikan hak atas perlindungan fisik, psikologis, dan informasi selama proses hukum, namun kejahatan yang dilakukan dengan AI—seperti manipulasi data pribadi dan penyebaran konten deepfake—belum masuk dalam kategori tindak pidana yang secara eksplisit diakomodasi oleh undang-undang tersebut (Lestari, 2017; Supanto & Aryani, 2018).

Dalam aspek pidana, tindak kejahatan seperti penipuan (Pasal 378 KUHP), pencemaran nama baik (Pasal 310 KUHP), dan pemerasan (Pasal 368 KUHP) sering terjadi melalui teknologi AI. AI digunakan untuk memalsukan identitas, menciptakan konten menyesatkan, atau menyebarluaskan informasi palsu yang merugikan pihak lain secara material maupun immaterial. Meskipun hukum pidana tetap menempatkan manusia sebagai subjek hukum utama, keberadaan AI sebagai alat kejahatan memperumit proses pembuktian dan pelacakan pelaku. Oleh karena itu, sistem hukum nasional perlu memperbarui perangkat normatifnya agar mampu merespons dinamika kejahatan digital secara efektif dan adil (Prabowo, 2020; Iswanto, 2024).

Selain itu, hadirnya UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi menjadi langkah progresif dalam menjamin hak konstitusional atas privasi individu. Undang-undang ini mengatur sanksi bagi pelaku penyalahgunaan data pribadi dan menyediakan mekanisme penyelesaian sengketa secara hukum. Namun, untuk menjamin perlindungan menyeluruh, kebijakan perlindungan korban kejahatan AI harus dikembangkan secara holistik, meliputi pemulihan citra diri, bantuan psikologis, dan kemudahan akses terhadap proses hukum. Karena itu, pembuat kebijakan di Indonesia perlu segera melakukan harmonisasi regulasi, memperluas cakupan UU Perlindungan Saksi dan Korban, serta mengembangkan peraturan turunan UU ITE dan UU PDP agar lebih responsif terhadap ancaman kejahatan berbasis kecerdasan buatan (Fitriani, 2021; Sari & Wardani, 2019).

Kendala dalam Implementasi Perlindungan Hukum Terhadap Korban Kejahatan Berbasis Teknologi Kecerdasan Buatan/*Artificial intelligence* (AI) dan Upaya yang dapat Dilakukan untuk Mengatasinya

Perkembangan masyarakat yang semakin dinamis tidak sebanding dengan pergerakan hukum yang cenderung statis (Aulia, 2018). Dalam praktiknya, implementasi Undang-Undang yang bertujuan untuk memerangi kejahatan berbasis teknologi kecerdasan buatan (AI) di media sosial masih belum memadai. Lembaga penegak hukum menghadapi berbagai tantangan, dan Undang-Undang yang ada dinilai kurang efektif untuk mengatasi kejahatan yang melibatkan teknologi AI. Meskipun Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) mencakup beberapa regulasi terkait AI, belum ada Undang-Undang yang secara khusus mengatur masalah ini. Oleh karena itu, penanganan tindakan kriminal yang menggunakan teknologi AI, seperti deepfake,

hacking, dan phishing yang disebarluaskan melalui internet, hanya dapat dilakukan dengan mengandalkan regulasi yang berkaitan dengan informasi elektronik. Kesenjangan regulasi dalam menghadapi kejahatan berbasis teknologi kecerdasan buatan (AI) menjadi tantangan serius di era digital saat ini. Regulasi yang ada belum sepenuhnya mengakomodasi kompleksitas dan dinamika kejahatan yang memanfaatkan AI, menciptakan celah hukum yang dapat dimanfaatkan oleh pelaku kejahatan. AI, dengan kemampuannya untuk belajar dan beradaptasi dengan cepat, seringkali jauh lebih maju daripada sistem hukum yang cenderung tertinggal dan tidak mampu mengikuti perkembangan teknologi yang begitu pesat. Hal ini menyebabkan banyak tindakan kriminal berbasis AI, seperti deepfake, manipulasi data, dan serangan siber otomatis, tidak memiliki payung hukum yang jelas untuk penanganannya. Akibatnya, penegak hukum kesulitan dalam mengidentifikasi, membuktikan, dan menjerat pelaku kejahatan tersebut. Selain itu, kurangnya definisi yang jelas mengenai tanggung jawab hukum dalam penggunaan AI, terutama ketika melibatkan pihak ketiga atau sistem otonom, memperumit situasi. Oleh karena itu, pembaruan regulasi yang lebih komprehensif dan adaptif sangat dibutuhkan agar hukum dapat mengimbangi perkembangan teknologi dan melindungi masyarakat dari potensi penyalahgunaan AI.

Hukuman seharusnya memiliki peran penting dalam menghentikan tindak pidana penyalahgunaan teknologi kecerdasan buatan (AI). Namun, kekurangan undang-undang yang jelas mengenai AI dapat menyebabkan ketidakpastian hukum. Ketidakjelasan tentang cara mencegah dan menanggulangi kejahatan berbasis AI menciptakan ruang bagi ketidakpastian tersebut. Adagium *het recht hinkt achter de faiten aan* yang berarti hukum berjalan lambat dan tertinggal dari kemajuan manusia, menggambarkan dengan jelas kekurangan dalam sistem hukum ini. Meskipun demikian, hukum pada dasarnya berkembang seiring dengan perubahan masyarakat. Sebagaimana yang diungkapkan oleh (Rahardjo, 1991) dalam teori hukum progresifnya, hukum dibuat untuk melayani manusia, bukan untuk membatasi manusia. Oleh karena itu, hukum harus berfungsi untuk melindungi kepentingan manusia dengan menyesuaikan diri dengan perkembangan teknologi dan kebutuhan masyarakat, memastikan bahwa hukum tetap relevan dan efektif dalam menghadapi tantangan baru yang muncul, seperti penyalahgunaan AI.

Kesulitan dalam melacak dan membuktikan kejahatan berbasis kecerdasan buatan (AI) menjadi salah satu tantangan terbesar yang dihadapi oleh penegak hukum di seluruh

dunia. Hal ini terutama disebabkan oleh sifat AI yang sangat canggih, dinamis, dan dapat berevolusi dengan cepat, yang menyebabkan jejak digital yang ditinggalkan sering kali sulit diidentifikasi atau bahkan sengaja dihilangkan oleh pelaku. Kejahatan berbasis AI juga sering melibatkan pihak-pihak lintas negara, yang memperumit investigasi karena perbedaan yurisdiksi hukum, kebijakan privasi, serta kurangnya kerja sama internasional yang optimal. Sebagai contoh, serangan siber yang menggunakan AI bisa diluncurkan dari satu negara, menargetkan korban di negara lain, dan melibatkan server yang berlokasi di negara ketiga. Kondisi ini menambah hambatan dalam mengumpulkan bukti, melacak pelaku, dan menuntut mereka secara hukum, sehingga menuntut pembaruan dan peningkatan koordinasi hukum global untuk menangani kejahatan berbasis teknologi ini secara efektif.

Teknologi AI, seperti deepfake atau algoritma peretasan canggih, dapat menyamarkan identitas pelaku dan memanipulasi data dengan cara yang sulit dideteksi oleh alat forensik konvensional. Kejahatan berbasis AI sering melibatkan perangkat digital dan algoritma yang sangat kompleks, di mana bukti-bukti yang dihasilkan, seperti log, kode program, dan lainnya, memerlukan keahlian teknis khusus untuk dipahami. Ketika penyidik atau pengacara tidak memiliki latar belakang yang memadai dalam teknologi, hal ini dapat memengaruhi kualitas kasus yang dibawa ke pengadilan. Akibatnya, hakim mungkin kesulitan untuk memberikan keputusan yang adil berdasarkan bukti yang ada. Sebagai contoh, seorang hacker yang menggunakan AI untuk menipu bisa meninggalkan jejak digital, namun jika penyidik tidak mengetahui cara mengakses dan menganalisis data tersebut, pelaku dapat lolos dari hukuman. Situasi ini menuntut peningkatan pemahaman dan keterampilan teknis bagi penegak hukum agar dapat menangani kejahatan berbasis AI secara efektif.

Keterbatasan sumber daya manusia dan teknologi di lembaga penegak hukum menjadi salah satu hambatan utama dalam menangani kejahatan berbasis AI. Kejahatan ini memerlukan pemahaman mendalam tentang teknologi yang kompleks dan terus berkembang, sementara banyak lembaga penegak hukum yang belum memiliki tenaga ahli yang cukup terlatih di bidang kecerdasan buatan, analisis data, atau keamanan siber. Hal ini menyebabkan proses investigasi seringkali menemui kendala teknis, seperti kesulitan dalam mengidentifikasi metode serangan, melacak jejak digital, atau menganalisis algoritma yang digunakan oleh pelaku. Selain itu, keterbatasan anggaran

dan infrastruktur teknologi juga menjadi hambatan serius, dengan banyak lembaga penegak hukum yang masih menggunakan peralatan dan sistem yang ketinggalan zaman. Akibatnya, mereka kesulitan untuk mengimbangi kecanggihan alat dan teknik yang digunakan oleh pelaku kejahatan AI. Tanpa investasi yang memadai dalam pelatihan sumber daya manusia dan pengadaan teknologi mutakhir, lembaga penegak hukum akan terus menghadapi kesulitan dalam mengungkap, mencegah, dan menindak kejahatan berbasis AI secara efektif. Oleh karena itu, diperlukan kolaborasi antara pemerintah, sektor swasta, dan akademisi untuk meningkatkan kapasitas dan kompetensi lembaga penegak hukum dalam menghadapi tantangan ini.

Isu privasi dan keamanan data menjadi tantangan besar dalam proses investigasi, yang juga dapat memperburuk situasi korban yang merasa dirugikan. Dalam melakukan investigasi, lembaga penegak hukum seringkali harus mengakses data pribadi korban. Masalah muncul ketika regulasi perlindungan data pribadi menghalangi akses yang diperlukan untuk mengumpulkan bukti. Hal ini membuat korban ragu untuk melapor karena khawatir data pribadi mereka akan disalahgunakan oleh pihak yang tidak bertanggung jawab. Oleh karena itu, Indonesia membutuhkan regulasi hukum yang spesifik untuk mengatur kecerdasan buatan, yaitu Undang-Undang Kecerdasan Buatan (UU AI). Undang-Undang ini harus fokus pada regulasi pengiriman dan penerimaan pesan elektronik melalui teknologi AI, memberikan pedoman yang jelas dan bijaksana dalam pemanfaatan kecerdasan buatan. Hal ini sangat penting, terutama di tengah gangguan teknologi yang terus berkembang saat ini dan yang mungkin terjadi di masa depan (Hafsyari, 2023). Mekanisme pelaporan dan penanganan yang efektif sangat penting dalam menangani kejahatan berbasis AI, mengingat kompleksitas dan dampak luas yang dapat ditimbulkan oleh tindakan tersebut. Sistem pelaporan harus dirancang agar mudah diakses oleh semua lapisan masyarakat, baik melalui platform online, aplikasi mobile, atau saluran offline seperti call center dan kantor layanan khusus. Hal ini bertujuan untuk memastikan bahwa korban kejahatan AI, seperti penipuan digital, penyebaran deepfake, atau penyalahgunaan data pribadi, dapat segera melaporkan insiden tanpa hambatan teknis atau birokratis. Selain itu, sistem pelaporan tersebut harus ramah pengguna dengan fitur-fitur seperti panduan langkah demi langkah, dukungan multibahasa, serta opsi pelaporan anonim untuk melindungi privasi korban.Setelah pelaporan diterima, mekanisme penanganan harus responsif dan terkoordinasi dengan

E-ISSN 2774-8863

baik antara berbagai pihak, seperti lembaga penegak hukum, regulator teknologi, dan penyedia layanan digital. Tim khusus yang terlatih dalam menangani kejahatan berbasis AI perlu dibentuk untuk melakukan investigasi yang cepat dan akurat, termasuk mengidentifikasi sumber kejahatan, melacak pelaku, serta mengamankan bukti digital. Proses ini harus didukung oleh teknologi canggih, seperti analisis data forensik dan alat deteksi AI, untuk memastikan keakuratan dan kecepatan penanganan kasus. Selain itu, korban harus diberikan dukungan holistik yang mencakup bantuan hukum untuk memulihkan hak-hak mereka serta dukungan psikologis untuk mengatasi trauma yang mungkin timbul. Mekanisme ini juga harus mencakup upaya pencegahan, seperti edukasi publik tentang risiko kejahatan berbasis AI dan cara melindungi diri. Dengan sistem pelaporan dan penanganan yang terintegrasi dan responsif, diharapkan korban kejahatan AI dapat merasa lebih terlindungi, sementara pelaku dapat diadili secara adil, sehingga efek jera dapat tercipta di masyarakat.

Edukasi dan kesadaran masyarakat memainkan peran penting dalam menghadapi tantangan kejahatan berbasis AI, mengingat banyaknya individu yang belum sepenuhnya memahami risiko dan dampak yang dapat ditimbulkan oleh penyalahgunaan teknologi ini. Untuk meningkatkan pemahaman masyarakat, diperlukan upaya sistematis dan berkelanjutan melalui berbagai bentuk kampanye publik dan program edukasi digital yang dapat menjangkau semua kalangan, mulai dari anak-anak hingga orang dewasa. Kampanye publik dapat dilakukan melalui media tradisional seperti televisi, radio, dan surat kabar, serta media digital seperti platform sosial media, situs web, dan aplikasi mobile. Materi yang disampaikan harus informatif, mudah dipahami, dan relevan dengan kehidupan sehari-hari, seperti cara mengenali penipuan digital, menghindari penyebaran deepfake, atau melindungi data pribadi dari serangan siber. Program edukasi digital perlu diintegrasikan ke dalam kurikulum pendidikan formal dan nonformal, mulai dari sekolah dasar hingga perguruan tinggi, serta pelatihan khusus untuk profesional dan pelaku usaha. Materi edukasi ini harus mencakup penjelasan tentang bagaimana teknologi AI bekerja, potensi risiko yang terkait, dan langkah-langkah praktis untuk melindungi diri, seperti penggunaan kata sandi yang kuat, verifikasi dua faktor, dan menghindari mengklik tautan mencurigakan. Institusi pendidikan dan pelatihan juga dapat berkolaborasi dengan pakar teknologi, lembaga pemerintah, dan organisasi masyarakat sipil untuk menyediakan sumber daya dan pelatihan yang komprehensif.

Kesadaran masyarakat juga dapat ditingkatkan melalui inisiatif komunitas, seperti workshop, seminar, dan diskusi publik yang melibatkan berbagai pemangku kepentingan, termasuk akademisi, praktisi teknologi, dan perwakilan pemerintah. Dengan meningkatkan literasi digital dan pemahaman tentang kejahatan AI, masyarakat akan lebih siap untuk menghadapi tantangan ini secara proaktif dan mengurangi kerentanan terhadap eksploitasi. Pada akhirnya, edukasi dan kesadaran yang baik tidak hanya melindungi individu, tetapi juga berkontribusi pada terciptanya lingkungan digital yang lebih aman dan bertanggung jawab bagi semua pihak. Pembentukan lembaga penegak hukum khusus yang fokus pada penanganan kejahatan berbasis AI merupakan langkah strategis dan mendesak dalam menghadapi kompleksitas serta dinamika kejahatan di era digital. Unit khusus ini, yang dapat berada di bawah naungan kepolisian atau lembaga terkait seperti badan siber nasional, harus dilengkapi dengan sumber daya manusia yang terlatih dan memiliki keahlian di bidang teknologi informasi, keamanan siber, serta hukum digital. Anggota unit ini perlu menjalani pelatihan intensif untuk memahami cara kerja teknologi AI, metode yang digunakan pelaku kejahatan, dan teknik investigasi digital yang mutakhir. Selain itu, unit ini harus didukung oleh infrastruktur teknologi canggih, seperti alat analisis data forensik, sistem deteksi deepfake, dan platform pemantauan aktivitas siber, untuk memastikan kecepatan dan akurasi dalam menangani kasus-kasus kejahatan AI.

Unit khusus ini juga harus memiliki kewenangan yang jelas dan mandat yang kuat untuk melakukan investigasi, penindakan, dan pencegahan kejahatan berbasis AI. Hal ini termasuk kemampuan untuk melacak dan mengidentifikasi pelaku, baik individu maupun korporasi, yang memanfaatkan AI untuk tujuan ilegal, seperti penipuan digital, penyebaran konten palsu, atau serangan siber otomatis. Selain itu, unit ini perlu bekerja sama erat dengan lembaga internasional dan organisasi lintas negara, mengingat kejahatan berbasis AI sering kali bersifat transnasional dan melibatkan jaringan global. Kolaborasi ini dapat mencakup pertukaran informasi, bantuan teknis, dan koordinasi penegakan hukum untuk memastikan bahwa pelaku tidak dapat menghindari jerat hukum hanya dengan beroperasi di luar yurisdiksi.Selain fungsi penegakan hukum, unit khusus ini juga harus berperan aktif dalam upaya pencegahan dan edukasi. Mereka dapat mengembangkan pedoman dan protokol keamanan untuk penggunaan AI yang bertanggung jawab, serta menyelenggarakan pelatihan dan workshop bagi masyarakat,

pelaku usaha, dan instansi pemerintah tentang cara mengenali dan menghindari kejahatan berbasis AI. Dengan adanya lembaga penegak hukum khusus ini, diharapkan dapat tercipta mekanisme yang lebih efektif dan terintegrasi dalam menangani kejahatan AI, sekaligus memberikan rasa aman dan perlindungan yang lebih baik bagi masyarakat di tengah pesatnya perkembangan teknologi.

KESIMPULAN

Berdasarkan analisis permasalahan yang telah dibahas, dapat disimpulkan bahwa meskipun pengaturan mengenai perlindungan hukum terhadap korban kejahatan berbasis teknologi kecerdasan buatan (AI) sudah ada, peraturan tersebut belum sepenuhnya efektif. Perlindungan hukum bagi korban AI masih kurang jelas dan tidak memadai dalam menjamin hak-hak korban. Oleh karena itu, diperlukan perubahan undang-undang yang lebih spesifik untuk mengatur penggunaan AI yang berpotensi merugikan banyak pihak. Dalam hal ini, kolaborasi antara pemerintah, masyarakat, dan pihak terkait sangat penting untuk memastikan perlindungan yang lebih kuat dan menyeluruh bagi korban.

Selain itu, kesenjangan dalam regulasi dan kesulitan dalam melacak serta membuktikan kejahatan berbasis AI menjadi tantangan besar bagi penegak hukum di seluruh dunia. Keberadaan AI yang terus berkembang pesat, bersifat dinamis, dan dapat beradaptasi dengan cepat menambah kompleksitas dalam upaya penegakan hukum. Seringkali, pelaku kejahatan menggunakan AI untuk menghilangkan jejak digital atau menyembunyikan bukti, yang membuat proses penyelidikan semakin sulit. Oleh karena itu, penguatan mekanisme pelaporan dan penanganan yang lebih efektif menjadi elemen penting untuk mengatasi kejahatan berbasis AI yang memiliki dampak luas dan kompleks.

DAFTAR PUSTAKA

Alkindyweb. (2022). 7+ Kasus Hacking Menggemparkan Indonesia & Penyebabnya. https://alkindyweb.com

Aulia, M. Z. (2018). Hukum progresif dari Satjipto Rahardjo: Riwayat, urgensi, dan relevansi. *Undang: Jurnal Hukum*, *1*(1), 159–185.

Carma, G. O. D. (2018). *Pelaksanaan Perlindungan Hukum Terhadap Korban Tindak Pidana Terorisme Di Bali* [S1, UAJY]. https://e-journal.uajy.ac.id/16725/

Fitriani, Y. (2021). Metodologi Penelitian Hukum Normatif dalam Penelitian Ilmiah. *Jurnal Hukum dan Pembangunan*, 51(1), 1–15. https://doi.org/10.21143/jhp.vol51.no1.

Hafsyari, Z. S. (2023). Perlindungan Hukum bagi Korban Deepfake Pornografi. https://pleads-fhunpad.medium.com

Iswanto, B. (2024). *Artificial Intelligence: Urgensi Pengaturan dan Tantangannya di Indonesia*. UINSI Repository.

Jamaaluddin, & Sulistyowati, I. (2021). Buku Ajar Mata Kuliah Kecerdasan Buatan (AI). UMSIDA Press.

Lestari, M. D. (2017). *Akses terhadap Keadilan bagi Korban: Tinjauan terhadap Peran LPSK*. Jurnal Ilmiah Hukum, 6(2), 87–98.

Mahardika, Z. P., & Priancha, A. (2021). *Pengaturan Hukum Artificial Intelligence Indonesia Saat Ini*. Hukumonline.com.

Marzuki, P. M. (2017). *Penelitian Hukum: Edisi Revisi*. Kencana.

Prabowo, R. E. (2020). *Prinsip Perlindungan Hukum dalam Negara Hukum Indonesia*. Jurnal Hukum Pro Justitia, 38(1), 23–34.

Pratiwi, H. (2024). Buku Ajar Kecerdasan Buatan: Disertai Praktik Baik Pemanfaatannya. Asadel Liamsindo Teknologi.

Salim, H. S., & Nurbani, N. (2020). *Penerapan Teori Hukum pada Penelitian Tesis dan Disertasi*. RajaGrafindo Persada.

Sari, D. P., & Wardani, R. P. (2019). *Perlindungan Hukum terhadap Korban Tindak Pidana: Perspektif HAM dan Peraturan Perundang-Undangan*. Jurnal Hukum dan HAM, 10(2), 145–156.

Supanto, & Aryani, N. W. (2018). *Hukum dan Perlindungan Korban dalam Sistem Peradilan Pidana*. Pustaka Pelajar.

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

Undang-Undang Republik Indonesia Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban.

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

Undang-Undang Republik Indonesia Nomor 31 Tahun 2014 tentang Perlindungan Saksi dan Korban.