

Jurnal Media Hukum

Vol. 13 Nomor 2, September 2025

Doi : 10.59414/jmh.v13i2.1030

Optimalisasi Penegakan Hukum terhadap Kejahatan Siber Berbasis AI terhadap Perempuan: Kajian Hukum Pidana dan Kebijakan Digital

Apitta Fitria Rahmawati¹, Yuris Tri Naili²

^{1,2}Jurusan Ilmu Hukum, Fakultas Ilmu Sosial, Universitas Harapan Bangsa, Purwokerto

*apittafitriarahmawati@uhb.ac.id

Article

Kata kunci:

Hukum Pidana;
Kebijakan Digital;
Kejahatan Siber;
Kecerdasan Buatan;
Perempuan

Keywords:

Criminal Law; Digital Policy; Cyber Crime; Artificial Intelligence; Women

Abstrak

Kemajuan teknologi kecerdasan buatan (AI) telah menciptakan tantangan baru di area hukum pidana, terutama mengenai kejahatan siber yang menargetkan perempuan sebagai sasaran. Fenomena seperti pornografi deepfake, pemalsuan identitas digital, hingga algoritma predator menjadi bentuk kejahatan siber gender yang semakin rumit dan sulit untuk dilacak. Penelitian ini bertujuan untuk mengkaji tiga aspek penting yaitu tipe-tipe kejahatan siber yang didorong AI dengan perhatian pada perempuan sebagai korban; efektivitas perlindungan hukum pidana nasional bagi perempuan yang menjadi sasaran kejahatan siber berbasis AI; serta strategi penguatan penegakan hukum dan perumusan kebijakan digital dalam menangani fenomena ini. Metode yang digunakan yakni penelitian hukum normatif yakni melalui peraturan yang berlaku. Hasil analisis mengindikasikan kejahatan siber yang didasarkan pada AI memiliki ciri-ciri transnasional, terautomatisasi, dan tingkat bias gender yang tinggi. Sebaliknya, sistem hukum pidana di Indonesia, termasuk KUHP dan UU ITE, belum mampu mencakup aspek teknologis dan gender dari kejahatan tersebut secara efektif. Karena itu, diperlukan reformulasi hukum pidana yang peka terhadap kemajuan teknologi dan sudut pandang keadilan gender, serta penguatan kebijakan digital yang terkoordinasi antara negara, platform digital, dan masyarakat sipil. Studi ini menyarankan peneguhan lembaga siber nasional, reformasi norma hukum pidana yang berorientasi pada AI, serta penyatuan perlindungan perempuan dalam kebijakan teknologi dan keamanan digital.

Abstract

The progress of artificial intelligence (AI) technology has introduced new difficulties in criminal law, especially concerning cybercrimes that affect women as victims. Occurrences like deepfake pornography, digital identity theft, and predatory algorithms have emerged as types of gender-based violence online that are growing more intricate and challenging to track. This study seeks to explore three key elements: the kinds of cybercrimes motivated by AI, particularly concerning women as victims; the adequacy of national criminal laws in protecting women affected by AI-driven cybercrimes; and approaches to enhance law enforcement and develop

digital policies to tackle this issue. The approach utilized is normative legal research, focusing on legislative texts and conceptual frameworks. The results of the analysis show that cybercrimes utilizing AI possess transnational traits, are automated, and demonstrate significant gender bias. In contrast, Indonesia's criminal justice system, comprising the Criminal Code and the ITE Law, has not been able to adequately address the technological and gender dimensions of these offenses. Hence, a rethinking of criminal law that considers technological progress and the viewpoint of gender justice is essential, along with the enhancement of collaborative digital strategies among the state, digital platforms, and civil society. This research suggests enhancing national cyber agencies, updating criminal law standards focused on AI, and incorporating women's safety into technology and digital security strategies.

PENDAHULUAN

Revolusi digital telah mengubah secara signifikan cara interaksi sosial, ekonomi, dan hukum. Salah satu pencapaian signifikan di zaman ini adalah hadirnya dan pengintegrasian Kecerdasan Buatan (AI) dalam berbagai bidang kehidupan manusia. Kecerdasan buatan dimanfaatkan untuk menganalisis data, mengidentifikasi pola perilaku, meramalkan kebutuhan pengguna, serta menghasilkan konten digital secara otomatis. Akan tetapi, seiring dengan meluasnya penggunaan teknologi ini, juga muncul potensi untuk penyalahgunaan, terutama dalam bidang kejahatan siber (cybercrime).

Pusat Data dan Teknologi Informasi Komunikasi Badan Siber dan Sandi Negara (Pusdatik BSSN) menyatakan bahwa munculnya kecerdasan buatan (AI) di zaman digital saat ini merupakan sebuah realitas yang tidak dapat dihindari. AI dapat berfungsi sebagai mitra strategis untuk meningkatkan efektivitas kerja dan pengambilan keputusan, tetapi juga berpotensi menjadi ancaman jika tidak dikelola dengan bijaksana ¹.

Internet Organised Crime Threat Assessment menjelaskan bahwa penerapan yang lebih umum dari alat dan layanan AI oleh penjahat dunia maya menciptakan risiko baru, yang meliputi penyalahgunaan alat dan layanan yang sah serta versi berbahaya yang dibuat secara sembarangan oleh pelanggar. Jumlah yang semakin bertambah tanpa adanya penyaringan terhadap prompt yang muncul baru-baru ini diprediksi akan meningkat dua kali lipat dan kemungkinan besar akan muncul lebih banyak iklan yang dihasilkan oleh AI yang menarik korban potensial ke dalam penipuan daring ². Salah satu jenis

¹ Badan Siber Dan Sandi Negara, "Cyber Security Awareness Webinar BSSN 2025 Serie #1: Kenalan Sama AI, Teman Atau Ancaman?," (bssn.go.id, 2025)

² Europol, *Internet Organised Crime Threat Assessment (IOCTA)*, Publications Office of the European Union, Luxemburgo, 2023)

yang semakin meresahkan adalah kejahatan siber berbasis AI yang menargetkan perempuan secara khusus³.

Perempuan menjadi kelompok yang paling terpengaruh oleh dampak negatif teknologi digital, terutama karena AI dapat digunakan untuk menghasilkan *deepfake* pornografi, cloning suara untuk pemerasan emosional (*sextortion*), serta penyebaran informasi salah atau konten pribadi tanpa izin. Tipe kejahatan ini tidak hanya merusak martabat dan integritas individu korban, tetapi juga memperkuat sistem kekerasan berbasis gender di dunia maya.

Data KBGtP pada CATAHU 2024 mencapai 330.097 kasus, naik sebesar 14,17% dibanding tahun 2023. Data KBGtP terkait keputusan pengadilan mencakup 291.213 kasus, semakin tinggi dibandingkan dengan data pelaporan yang berjumlah 38.788 kasus dan penuntutan sebanyak 96 kasus. Data vonis pengadilan yang terbanyak, sebab data dari BADILAG berupa putusan. Berdasarkan kategorinya, KBGtP pada lingkup personal lebih tinggi (309.516 kasus) dibandingkan dengan lingkup publik (12.004 kasus) dan lingkup negara (209 kasus). Sejumlah 8.368 kasus yang berasal dari Kemen-PPPA⁴.

Di samping itu, UU No. 12 Tahun 2022 tentang Tindak Pidana Kekerasan Seksual (UU TPKS) telah mengatur kekerasan seksual yang menggunakan media elektronik, tetapi belum mempertimbangkan kompleksitas metode yang dilakukan dengan bantuan AI. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) masih tidak ada cakupan terkait aspek manipulasi data oleh algoritma yang didasarkan pada kecerdasan buatan, khususnya dalam hal rekayasa wajah dan suara perempuan yang menjadi korban. Ketidadaan regulasi khusus untuk menghadapi kejahatan siber yang berbasis AI mengakibatkan terjadinya "*regulatory lag*" yaitu keterlambatan norma hukum dalam menanggapi perkembangan teknologi. Ini berpotensi menimbulkan impunitas bagi pelaku dan melakukan kriminalisasi balik terhadap korban, terutama jika perempuan yang mengadukan justru dikenakan pasal kesusilaan yang bisa ditafsirkan beragam dalam UU ITE.

Laporan diatas, menunjukkan penegakan hukum yang kurang maksimal. Penegakan hukum terkait *cybercrime* di Indonesia sangat disebabkan beberapa factor yang ada, yaitu peraturan perundang-undangan, sikap aparaturnya penegak hukum, tindakan masyarakat, fasilitas, dan budaya⁵. Oleh karena itu, diperlukan Fenomena kejahatan siber yang menggunakan AI terhadap perempuan menghadirkan tantangan hukum yang rumit. Di satu sisi, teknologi AI dapat

³ M Jaggar et al., "PERSPEKTIF GENDER DAN FILSAFAT POLITIK ALISON," 2021.

⁴ Komnas Perempuan, 2025.

⁵ Ni Putu Noni Suharyanti, "Progresivitas Dalam Penegakan Hukum Penyalahgunaan Narkotika," *Jurnal Kartika Partika*, 2017.

berfungsi secara mandiri dan sulit dipantau, sehingga menyulitkan proses bukti di pengadilan. Sebaliknya, peraturan hukum yang ada sekarang belum sepenuhnya mengatur secara rinci jenis-jenis kejahatan itu.

Aspek penting lainnya adalah minimnya kesiapan kebijakan digital untuk melindungi kelompok rentan, terutama perempuan, dari ancaman AI yang berbahaya. Pemerintah telah mendorong digitalisasi di berbagai bidang, tetapi kebijakan perlindungan hukum yang responsif dan adaptif terhadap teknologi baru masih belum mencukupi. Kebijakan digital Indonesia belum sepenuhnya menerapkan pendekatan gender dan analisis risiko berbasis AI, sehingga menghasilkan kekurangan dalam perlindungan hukum di lapangan. Dalam konteks ini, optimalisasi penegakan hukum disamping terdapat pelanggar, juga ada pencegahan, pelatihan, kerja sama lintas sektor, serta perbaikan hukum pidana yang sesuai dengan perkembangan ini. Demikian, penelitian ini memiliki tujuan mengenali tipe-tipe kejahatan siber berbasis AI yang menasar perempuan, menganalisis hambatan yang dialami oleh aparat penegak hukum dalam menghadapi permasalahan yang ada, mengevaluasi efektivitas regulasi hukum pidana dan kebijakan digital yang ada, serta merumuskan rekomendasi strategis guna mengoptimalkan penegakan hukum yang responsif terhadap kejahatan siber berbasis AI.

METODE

Peneliti menggunakan penelitian hukum normatif yang memiliki tujuan untuk dikaji dengan peraturan yang ada, serta prinsip-prinsip yang memiliki keterkaitan dengan kejahatan siber berbasis kecerdasan buatan terhadap Perempuan. Pendekatan yang diterapkan mencakup pendekatan hukum dan konseptual. Bahan hukum yang ditinjau meliputi undang-undang dan peraturan terkait seperti UU ITE, KUHP, UU TPKS, UU PDP dan lainnya.

PEMBAHASAN

Tipologi Kejahatan Siber Berbasis Kecerdasan Buatan (AI) dengan Fokus pada Korban Perempuan

Kejahatan siber merupakan suatu bentuk kejahatan yang baru muncul dan selalu mengalami kemajuan baik dalam hal cara bertindak atau variasi kejahatannya⁶. Kecerdasan Buatan atau AI sedang tren di semua bidang yang mampu dimanfaatkan. Berlangsungnya Kecerdasan Buatan yakni

⁶ Maskun, "Buku Kejahatan Siber (Cyber Crime): Suatu Pengantar" (Jakarta: Kencana, 2022),.

pembelajaran, penalaran, dan koreksi diri manusia yang menganalisis sebelum mengambil Keputusan⁷.

Menurut Data dari SAFEnet, pada tahun 2025 kekerasan tetap berlangsung dan menargetkan kelompok yang rentan. SAFEnet menerima total 422 aduan yang meningkat dibandingkan dengan tahun 2023 (118 aduan) dan tahun 2024 (371 aduan) pada kuartal yang sama. Pada tahun 2024, jumlah aduan KBGO mengalami peningkatan yang lebih tinggi mencapai 214,4 persen. Sedangkan kenaikan laporan KBGO pada 2025 mencapai 13,7 persen. Dalam tiga bulan awal 2025, tampak bahwa perempuan lebih sering melaporkan pengalaman KBGO mereka kepada SAFEnet. Sebanyak 271 (64,22 persen) komplain berasal dari pelapor perempuan, sedangkan pelapor laki-laki mengajukan 142 (33,65 persen) aduan. Gender yang mengidentifikasi sebagai nonbiner, mencatatkan 3 pengaduan terkait KBGO. Pelapor KBGO terdiri dari 402 aduan oleh korban langsung, 7 aduan oleh teman, 7 aduan oleh keluarga, dan 6 aduan lainnya⁸. Berdasarkan hasil temuan tersebut, terdapat beberapa tipologi kejahatan siber berbasis AI dengan korban perempuan sebagai target utama:

1. Deepfake Pornografi Non-Konsensual

Teknologi deepfake telah menciptakan masalah serius di zaman digital, khususnya bagi wanita. Dalam beberapa tahun terakhir, meningkatnya kasus pornografi deepfake menyoroti sisi kelam dari kemajuan teknologi. Banyak wanita menjadi target penyebaran video seksual yang tidak benar tanpa izin mereka⁹. Belum ada norma eksplisit dalam peraturan perundang-undangan seperti UU ITE ataupun KUHP yang mengatur terkait dengan pembuatan atau penyebaran konten deepfake secara spesifik.

2. Romance Scam Berbasis Chatbot AI

AI chatbot tidak hanya dapat secara teknis melaksanakan perintah dari penggunanya, tetapi juga mampu memberikan solusi untuk memenuhi kebutuhan manusia dalam berkomunikasi. Beragam platform menggabungkan alat-alat ini untuk memperbaiki pengalaman pengguna. Dengan kemajuan teknologi berbasis AI, semakin banyak orang yang berinteraksi dan bergantung pada teknologi ini untuk kebutuhan praktis

⁷ M Sobron and Lubis, "Implementasi Artificial Intelligence Pada System Manufaktur Terpadu," *Seminar Nasional Teknik (SEMNASTEK) UISU* 4, no. 1 (2021): 1–7.

⁸ Anton Muhajir, "Laporan Pemantauan Hak-Hak Digital Di Indonesia," *Southeast Asia Freedom of Expression Network (SAFEnet)*, 2024, 1–34.

⁹ Indah Rohmawati, Amir Junaidi, and Ariy Khaerudin, "Urgensi Regulasi Penyalahgunaan Deepfake Sebagai Perlindungan Hukum Korban Kekerasan Berbasis Gender Online (KBGO)" 4 (2024): 3239–54.

seperti mencari informasi, memesan tiket, menyelesaikan masalah layanan pelanggan, serta menjawab pertanyaan pribadi untuk mendapatkan rekomendasi atau sekadar untuk berkomunikasi¹⁰.

Prespektif hukum terkait dengan chatbot masih belum menggambarkan kejelasan apakah manipulasi emosional melalui chatbot dapat untuk dikategorikan sebagai penipuan atau kejahatan berbasis relasi atau tidak. Secara psikologis juga korban dalam konteks ini akan mengalami ketertarikan emosional palsu, kebingungan identitas relasional, dan perasaan kehilangan saat menyadari kebohongan digital. Perempuan sering menjadi sasaran karena dianggap lebih mudah membangun kedekatan emosional, sehingga relasi yang dimediasi AI rentan dimanfaatkan untuk eksploitatif.

3. Penyebaran Disinformasi yang Mengarah ke Kekerasan Gender Online

Disinformasi sering kali menyulut kekerasan politik, kebencian, dan penolakan terhadap perempuan muda yang ingin berkarier di bidang politik. Disinformasi terkait gender sering dimanfaatkan oleh pihak-pihak yang mendukung negara untuk merongrong pemimpin perempuan oposisi dan juga hak-hak Perempuan¹¹.

Tidak semua bentuk disinformasi dapat dikategorikan sebagai ujaran kebencian atau pencemaran nama baik dalam hukum Indonesia. Disinformasi sering digunakan untuk membungkam suara perempuan dan menghalangi perempuan berkiprah di ruang publik sebuah bentuk kekerasan berbasis gender digital.

4. Pengintaian Digital (Digital Stalking) dengan AI

Pengintaian digital gender merujuk pada pengawasan atau pemantauan yang dilakukan terhadap orang-orang berdasarkan gender mereka di internet. Ini bisa mencakup pengawasan aktivitas daring, pengumpulan data pribadi, atau penyebaran informasi yang tidak benar yang menargetkan orang sesuai dengan jenis kelamin mereka. Pengintaian digital berbasis AI belum terdapat pengaturan khusus tentang *digital surveillance* berbasis hubungan intim atau stalking dalam ranah cyberlaw Indonesia. Secara psikologis juga korban sering mengalami *hyper-vigilance*, paranoia, dan perasaan terkurung dalam hubungan yang tidak aman. Ditinjau dari studi gender tentunya pengintaian digital berbasis AI ini banyak terjadi dalam konteks *intimate partner violence*; perempuan dipantau secara digital oleh mantan pasangan sebagai bentuk kontrol kekuasaan.

¹⁰ Graciella Yoseppin et al., "Fenomena Chatbot AI Sebagai Teman Curhat : Implikasi Pada Hubungan Antarpribadi Di Era Digital" 7 (2025): 45–53.

¹¹ Adiyanto, "Perempuan Di Seluruh Dunia Berjuang Melawan Disinformasi Gender," Media Indonesia, 2023, <https://mediaindonesia.com/weekend/568785/perempuan-di-seluruh-dunia-berjuang-melawan-disinformasi-gender>.

5. Voice Cloning untuk Penipuan Emosional dan Pemerasan

Kemampuan AI ini jelas memberikan berbagai keuntungan untuk sektor kreatif dan bisnis, seperti menghasilkan suara untuk asisten virtual atau animasi. Namun, di sisi lain, pemanfaatan *AI Voice Cloning* yang tidak terkontrol justru menimbulkan persoalan serius terkait kepercayaan konsumen, etika, dan hukum¹².

Dari penjelasan di atas, jelas bahwa tipologi kejahatan siber yang menggunakan AI terhadap perempuan bersifat kompleks: mengintegrasikan elemen manipulasi teknologi, tekanan emosional, dan eksploitasi sosial. Penegak hukum menghadapi dilema karena tidak adanya norma yang jelas dalam KUHP maupun UU ITE yang secara langsung mengidentifikasi kejahatan yang melibatkan AI sebagai elemen delik. Ini menjadi kendala dalam penentuan pasal yang sesuai serta pembuktian di tahap penyidikan.

Selain itu, perempuan yang menjadi korban menghadapi rintangan struktural dan kultural, seperti rasa malu, stigma sosial, dan ketidaktahuan tentang hak-hak hukum mereka. Oleh karena itu, selain penegakan hukum yang responsif, diperlukan pendekatan pendidikan, perlindungan bagi korban, dan pembaruan norma hukum yang lebih preskriptif terhadap AI sebagai alat kejahatan.

Perlindungan Hukum Pidana Nasional terhadap Perempuan sebagai Korban Kejahatan Siber Berbasis Kecerdasan Buatan (AI)

Perlindungan hukum bagi perempuan yang menjadi korban kejahatan masih sangat minim, meski Pasal 28 G UUD 1945 telah menetapkan kewajiban Negara untuk memberikan perlindungan hukum yang mencakup tidak hanya hak asasi manusia tetapi juga hak konstitusional yang harus direalisasikan menjadi hak-hak hukum dalam peraturan perundang-undangan¹³.

Undang-Undang Nomor 23 Tahun 2004 mengenai Penghapusan Kekerasan dalam Rumah Tangga (UU PKDRT), Undang-Undang Nomor 12 Tahun 2022 tentang Tindak Pidana Kekerasan Seksual (UU TPKS), dan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Namun, kejahatan siber memanfaatkan teknologi kecerdasan buatan (AI), perlindungan hukum yang ada masih terbatas dan belum sepenuhnya mencakup karakteristik serangan digital berbasis AI terhadap wanita.

¹² Asep Koswara, Magister Manajemen, and Fakultas Ekonomi, "EKSPLOITASI AI VOICE CLONING DALAM PEMASARAN DIGITAL : ANALISIS" 4, no. 2 (2024): 77-83.

¹³ Silvia Novitasari, Yayan Sopyan, and Mara Sutan Rambe, "Pembaharuan Perlindungan Hukum Terhadap Perempuan Korban Kekerasan Seksual Dalam Undang-Undang Nomor Renewal of Legal Protection for Women Victims of Sexual Violence in Law Number 12 of 2022" 3, no. 1 (2024).

Ditinjau secara normatif, Pasal 27 ayat (1) UU ITE menyatakan bahwa setiap orang dilarang untuk mendistribusikan, mentransmisikan, dan/atau membuat dapat diaksesnya informasi elektronik yang memiliki muatan melanggar kesusilaan. Untuk memastikan adanya jaminan tersebut serta merespons perkembangan berbagai kejahatan *cybercrime* yang terjadi melalui media elektronik, pemerintah mengesahkan Undang-Undang Nomor 19 Tahun 2016 sebagai perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yang dikenal dengan UU ITE. Dalam peraturan ini terdapat pasal yang mengatur tentang pengiriman dokumen elektronik yang mengandung unsur melanggar kesusilaan yaitu Pasal 27 ayat (1)¹⁴. Namun, UU ITE belum secara eksplisit mengatur penggunaan kecerdasan buatan sebagai alat kejahatan. Akibatnya, sering kali aparat hukum harus bergantung pada penafsiran analogi atau kontekstual untuk menentukan unsur-unsur kejahatan.

Sebagian besar Perempuan korban kejahatan siber AI enggan melapor karena rasa malu dan tekanan sosial. Banyak korban mengalami rasa malu, bersalah, dan ketakutan akan penilaian negatif dari masyarakat sekitar, yang mengakibatkan trauma yang memengaruhi aktivitas sehari-hari, seperti kesulitan tidur, mimpi buruk, dan ketidaknyamanan saat menggunakan media sosial¹⁵. Salah satu yang menjadi faktor penghambat yakni korban kebanyakan malu, terlebih jika wajahnya disalahgunakan dalam konten seksual bahkan banyak yang lebih memilih baik dari sisi hukum mereka yang seharusnya dilindungi dan bisa diproses. Keadaan ini menunjukkan bahwa perlindungan hukum pidana tidak terkait dengan perangkat hukum saja, melainkan aksesibilitas, kesadaran hukum, dan kepedulian gender dalam proses penegakan hukum. Hukum pidana yang efektif tidak hanya sebatas mengatur, tetapi juga harus mampu memastikan pemulihan bagi korban dan menghindari reviktimisasi.

Dikaitkan dengan pengaturan hukum pidana yang bersifat materiil, KUHP baik versi lama maupun KUHP Baru Tahun 2023 belum mengatur secara rinci terkait dengan penggunaan AI dalam tindak pidana. Walaupun elemen dasar kejahatan siber bisa disesuaikan dengan beberapa pasal dalam KUHP, cara (modus) pelaksanaannya yang baru membuat kejahatan siber tergolong sebagai kejahatan khusus menurut hukum pidana di Indonesia. Dengan kata lain, dibutuhkan perangkat hukum yang lebih sigap untuk melawan

¹⁴ Hari Suharto, "Kebijakan Formulasi Hukum Pidana Pasal 27 Ayat (1) Undang- Undang Informasi Dan Transaksi Elektronik," 2020, 633–52.

¹⁵ Dita Aviliani, U I N Raden, and Intan Lampung, "Dinamika Psikologis Perempuan Korban Cyber Sexual Harassment" 13, no. 1 (2025): 44–65.

kejahatan ini¹⁶. Meskipun ada pasal-pasal umum tentang penghinaan, pencemaran nama baik, dan kejahatan terhadap kesusilaan, tidak ada yang secara jelas menyebut atau mengatur tentang kejahatan digital yang berbasis AI. Akibatnya, banyak kasus kejahatan siber yang melibatkan AI tidak dapat ditangani secara hukum dikarenakan tidak sesuai dengan kejahatan yang diatur.

Sementara itu, aspek hukum pidana formal, proses pembuktian pada kasus-kasus yang melibatkan AI sangat kompleks. Konten digital yang dihasilkan oleh AI, seperti suara atau gambar, sering kali sulit dibedakan dari konten asli secara forensik. Hal ini mengharuskan peningkatan kemampuan institusi penegak hukum, termasuk pelatihan khusus di bidang forensik AI. Tanpa hal itu, hukum pidana nasional akan terus tertinggal dari cara-cara pelaksanaan kejahatan yang semakin modern. Dari uraian tersebut, penulis menyimpulkan bahwa perlindungan hukum pidana nasional terhadap Perempuan sebagai korban kejahatan siber berbasis AI di Indonesia masih bersifat terbatas secara normative, lemah baik secara struktural maupun kultural.

Strategi Optimalisasi Penegakan Hukum dan Formulasi Kebijakan Digital dalam Menanggulangi Kejahatan Siber Berbasis AI terhadap Perempuan

Perkembangan teknologi kecerdasan buatan (AI) yang tidak sebanding dengan kesiapan regulasi dan kemampuan lembaga penegak hukum telah menciptakan celah yang semakin dieksploitasi oleh pelaku kejahatan siber, terutama yang menargetkan kelompok rentan seperti perempuan. Kejahatan siber yang dulunya konvensional kini telah berevolusi dengan penggunaan AI untuk menciptakan konten palsu (deepfake), melakukan tiruan suara, atau menjalin hubungan emosional palsu melalui chatbot. Pada nyatanya biasanya kecepatan pelaku dalam memanfaatkan celah teknologi melebihi kapasitas kita untuk memberikan respons secara hukum. Ini mengindikasikan kebutuhan mendesak akan strategi yang terintegrasi antara penegakan hukum dan kebijakan digital untuk menangani fenomena ini secara menyeluruh.

Strategi awal yang harus dilakukan adalah merumuskan kembali norma hukum pidana yang secara jelas mengakui penggunaan AI sebagai alat atau objek kejahatan. UU ITE dan KUHP baru belum secara khusus mengatur mengenai jenis-jenis kejahatan yang melibatkan AI, sehingga banyak kasus mengalami kekurangan dalam aspek hukum. Regulasi yang tegas terkait kejahatan yang menggunakan AI, khususnya yang berkaitan dengan eksploitasi seksual, manipulasi digital, atau peretasan data yang didasarkan pada algoritma,

¹⁶ Mochammad Rifky Syahrian and Widhi Cahyo Nugroho, "Tinjauan Yuridis Mengenai Kekerasan Pada Perempuan Dalam Kejahatan Cybercrime" 3, no. 1 (2023): 782-96.

sangat penting. Selain itu, penting untuk memperkuat ketentuan terkait yurisdiksi internasional guna menangani kejahatan siber yang dilakukan melalui server atau platform di luar Indonesia.

UU ITE, mengalami revisi sejak disahkan pada 2008, tetap dianggap kurang memadai. Terdapat sejumlah penyebab kenapa UU ITE dinilai gagal pada konteks ini, yaitu UU ITE tidak menawarkan definisi yang tepat mengenai "deepfake" atau teknologi AI lainnya, sehingga penegakan hukum terhadap praktik-praktik tersebut menjadi sulit. UU ITE lebih menekankan pada regulasi umum terkait informasi dan transaksi elektronik, tanpa mencakup masalah khusus mengenai teknologi AI, seperti manipulasi media dan penyebaran informasi yang tidak benar¹⁷.

Berkaitan apa yang disebutkan diatas, penulis memberikan saran guna terkait dengan perluasan secara mendetail beberapa pasal dalam UU ITE karena masih kurang memadai definisi, basis sistem yang ada, bahkan transparansi serta analisis terkait dengan AI secara spesifik.

Strategi kedua yakni dengan penguatan struktur kelembagaan para aparat penegak hukum menjadi kunci utama dalam rangka pengoptimalannya. Penyidik di wilayah masih mengalami kendala dalam akses terhadap perangkat digital forensik yang berbasis AI. Oleh sebab itu, penting untuk membentuk unit khusus penanganan kejahatan AI di Polda dan Mabes Polri, dilengkapi dengan pelatihan teknis serta SOP penanganan kasus yang mengutamakan korban perempuan. Penyusunan panduan mengenai penanganan barang bukti digital serta kemampuan menganalisis jejak AI juga perlu segera dilaksanakan secara nasional. Peningkatan Kapasitas Institusi Penegak Hukum pada Forensik Digital lembaga penegak hukum di Indonesia, seperti Direktorat Tindak Pidana Siber (Dittipidsiber) Polri, untuk secara berkala mengikuti pelatihan dan sertifikasi internasional di bidang forensik digital terkait metode-metode terkini dalam analisis digital dan penyelidikan kejahatan siber¹⁸.

Ketiga, strategi perlindungan korban perlu dilengkapi dengan infrastruktur pemulihan dan pelaporan yang berbasis teknologi digital. Seringkali, wanita yang menjadi korban kejahatan siber ragu untuk melapor karena merasa malu, khawatir akan disalahkan, atau tidak mengetahui hak-haknya. Penyidik mengungkapkan bahwa "korban deepfake sering kali memilih untuk tidak berbicara meskipun sangat terganggu secara mental, karena

¹⁷ Adnasohn Aqilla Respati, "Reformulasi Undang-Undang ITE Terhadap Artificial Intelligence Dibandingkan Dengan Uni Eropa Dan China AI Act Regulation Reformulation of the ITE Law on Artificial Intelligence Compared to the European Union and China AI Act Regulation" 7, no. 3 (2024): 4–12.

¹⁸ Oky Syalendro et al., "Tindak Pidana Cyber Crime Dalam Hukum Indonesia Serta Upaya Pencegahan Dan Penanganan Kasus Tindak Pidana Cyber Crime" 4, no. 1 (2025): 335–47.

bingung harus melapor kemana”. Maka dari itu, diperlukan platform pelaporan online yang aman, bersahabat bagi perempuan, dan terhubung langsung dengan penegak hukum serta lembaga layanan bagi korban.

Perbedaan antara perkembangan teknologi dan peraturan hukum mengakibatkan kurangnya perlindungan bagi korban kejahatan yang menggunakan AI. Bukti yang rumit, kekurangan petugas penegak hukum dalam memahami teknologi, serta minimnya literasi masyarakat digital menjadi kendala yang signifikan. Oleh sebab itu, diperlukan penelitian mendalam terkait regulasi dan penerapan perlindungan hukum yang lebih responsif terhadap kemajuan teknologi AI untuk menjamin keadilan dan kepastian hukum ¹⁹.

Melalui pendekatan yang menyeluruh antara reformasi hukum pidana, penguatan sistem penegakan hukum, kebijakan digital yang responsif, serta keterlibatan masyarakat sipil, strategi ini diharapkan dapat mengatasi tantangan kejahatan siber berbasis AI yang menargetkan perempuan. Tanpa tindakan nyata tersebut, perempuan akan tetap menjadi korban berulang di ruang digital yang belum sepenuhnya terlindungi.

KESIMPULAN

Kejahatan siber yang dipicu oleh kecerdasan buatan (AI) telah menciptakan pola serangan digital baru yang rumit, terstruktur, dan menargetkan kelompok-kelompok rentan, terutama wanita. Dengan memanfaatkan teknologi visual dan audio (seperti deepfake), manipulasi emosional berbasis chatbot, serta penyebaran konten otomatis yang menjatuhkan martabat, AI berfungsi sebagai alat yang efektif bagi pelaku untuk mengeksploitasi korban tanpa adanya interaksi fisik langsung.

Dalam konteks hukum nasional, regulasi seperti UU ITE, UU TPKS, dan KUHP belum sepenuhnya responsif terhadap kemajuan teknologi AI. Ketiadaan regulasi yang jelas mengenai AI sebagai alat atau objek tindak kejahatan menciptakan kekosongan hukum yang menyulitkan penegak hukum untuk mengambil tindakan yang tepat terhadap pelanggar. Sebaliknya, keterbatasan sumber daya teknis, tidak adanya SOP yang jelas, serta belum adanya sistem pelaporan yang aman dan mendukung korban semakin menjauhkan hukum yang berlaku dari kenyataan digital di lapangan.

Peningkatan kasus kejahatan AI terhadap perempuan tidak sebanding dengan kapasitas lembaga yang cukup. Korban seringkali ragu untuk melapor akibat rasa malu, takut, atau kurangnya pengetahuan digital. Ini menunjukkan bahwa pendekatan hukum yang represif saja tidak memadai; diperlukan

¹⁹ Elfrida Tipe Obe et al., “Analisis Yuridis Perlindungan Hukum Terhadap Korban Kejahatan Berbasis Teknologi Kecerdasan Buatan / Artificial Intelligence (AI)” 5, no. 2 (2025): 1144-56.

reformulasi hukum, penguatan institusi, dan kebijakan digital yang mendukung korban. Secara keseluruhan, penanganan kejahatan siber berbasis AI yang menargetkan perempuan memerlukan respons terintegrasi yang mencakup reformasi norma hukum, meningkatkan kapabilitas dari aparat penegak hukum, serta mengembangkan infrastruktur digital yang aman, responsif, dan berperspektif gender. Tanpa tindakan-tindakan tersebut, perempuan akan tetap berada dalam posisi yang tidak aman di tengah perkembangan teknologi yang semakin disruptif.

REFERENSI

Buku

Maskun. (2022). *Buku Kejahatan Siber (Cyber Crime): Suatu Pengantar*. Jakarta: Kencana.

Jurnal

Adiyanto. "Perempuan Di Seluruh Dunia Berjuang Melawan Disinformasi Gender." Media Indonesia, 2023. <https://mediaindonesia.com/weekend/568785/perempuan-di-seluruh-dunia-berjuang-melawan-disinformasi-gender>.

Aviliani, Dita, U I N Raden, and Intan Lampung. "Dinamika Psikologis Perempuan Korban Cyber Sexual Harassment" 13, no. 1 (2025): 44–65. <https://doi.org/10.18592/jsi.v13i1.15920>.

Badan Siber Dan Sandi Negara. "Cyber Security Awareness Webinar BSSN 2025 Serie #1: Kenalan Sama AI, Teman Atau Ancaman?" bssn.go.id, 2025. <https://www.bssn.go.id/cyber-security-awareness-webinar-bssn-2025-serie-1-kenalan-sama-ai-teman-atau-ancaman/>.

Europol. *Internet Organised Crime Threat Assessment (IOCTA). Publications Office of the European Union, Luxemburgo*, 2023. <https://doi.org/10.2813/442713>.

Jaggar, M, Jl Salemba, Raya No, Kec Senen, Kota Jakarta Pusat, and D K I Jakarta. "PERSPEKTIF GENDER DAN FILSAFAT POLITIK ALISON," 2021.

Komnas Perempuan. "CATAHU 2024: MENATA DATA, MENAJAMKAN ARAH: REFLEKSI PENDOKUMENTASIAN DAN TREN KASUS KEKERASAN TERHADAP PEREMPUAN." Komnas Perempuan, 2025. <https://komnasperempuan.go.id/catatan-tahunan-detail/catahu-2024-menata-data-menajamkan-arrah-refleksi-pendokumentasian-dan-tren-kasus-kekerasan-terhadap-perempuan>.

Koswara, Asep, Magister Manajemen, and Fakultas Ekonomi. "EKSPLOITASI AI VOICE CLONING DALAM PEMASARAN DIGITAL: ANALISIS" 4, no. 2 (2024): 77–83.

Maskun. "Buku Kejahatan Siber (Cyber Crime): Suatu Pengantar." Jakarta: Kencana, 2022.

- <https://books.google.com/books?hl=en&lr=&id=b1S6EAAAQBAJ&oi=fnd&pg=PA88&dq=kejahatan+hukum+cyber+crime+cyber+law&ots=qbRtkmJsQA&sig=LGIFu12sry9awdQKXyfwjOnnib4>.
- Muhajir, Anton. "Laporan Pemantauan Hak-Hak Digital Di Indonesia." *Southeast Asia Freedom of Expression Network (SAFE-net)*, 2024, 1–34.
- Novitasari, Silvia, Yayan Sopyan, and Mara Sutan Rambe. "Pembaharuan Perlindungan Hukum Terhadap Perempuan Korban Kekerasan Seksual Dalam Undang-Undang Nomor Renewal of Legal Protection for Women Victims of Sexual Violence in Law Number 12 of 2022" 3, no. 1 (2024).
- Obe, Elfrida Tipe, Aksi Sinurat, Rosalind Angel Fanggi, Universitas Nusa, and Cendana Kupang. "Analisis Yuridis Perlindungan Hukum Terhadap Korban Kejahatan Berbasis Teknologi Kecerdasan Buatan / Artificial Intelligence (AI)" 5, no. 2 (2025): 1144–56.
- Respati, Adnasohn Aqilla. "Reformulasi Undang-Undang ITE Terhadap Artificial Intelligence Dibandingkan Dengan Uni Eropa Dan China AI Act Regulation Reformulation of the ITE Law on Artificial Intelligence Compared to the European Union and China AI Act Regulation" 7, no. 3 (2024): 4–12.
- Rohmawati, Indah, Amir Junaidi, and Ariy Khaerudin. "Urgensi Regulasi Penyalahgunaan Deepfake Sebagai Perlindungan Hukum Korban Kekerasan Berbasis Gender Online (KBGO)" 4 (2024): 3239–54.
- Sobron, M, and Lubis. "Implementasi Artificial Intelligence Pada System Manufaktur Terpadu." *Seminar Nasional Teknik (SEMNAS-TEK) UISU* 4, no. 1 (2021): 1–7.
<https://jurnal.uisu.ac.id/index.php/semnastek/article/view/4134>.
- Suharto, Hari. "Kebijakan Formulasi Hukum Pidana Pasal 27 Ayat (1) Undang-Undang Informasi Dan Transaksi Elektronik," 2020, 633–52.
- Suharyanti, Ni Putu Noni. "Progresivitas Dalam Penegakan Hukum Penyalahgunaan Narkotika." *Jurnal Kartika Partika*, 2017.
- Syahrian, Mochammad Rifky, and Widhi Cahyo Nugroho. "Tinjauan Yuridis Mengenai Kekerasan Pada Perempuan Dalam Kejahatan Cybercrime" 3, no. 1 (2023): 782–96. <https://doi.org/10.53363/bureau.v3i1.216>.
- Syalendro, Oky, Arief Fahmi, Lubis R Yusak, and Andri Ende. "Tindak Pidana Cyber Crime Dalam Hukum Indonesia Serta Upaya Pencegahan Dan Penanganan Kasus Tindak Pidana Cyber Crime" 4, no. 1 (2025): 335–47.
- Yoseppin, Graciella, Putu Ayu, Mas Nagita, and Yuni Kasih Purba. "Fenomena Chatbot AI Sebagai Teman Curhat: Implikasi Pada Hubungan Antarpribadi Di Era Digital" 7 (2025): 45–53.

Website

- Badan Siber Dan Sandi Negara. (2025). Cyber Security Awareness Webinar BSSN 2025 Serie #1: Kenalan Sama AI, Teman atau Ancaman? Retrieved July 17, 2025, from bssn.go.id website: <https://www.bssn.go.id/cyber-security-awareness-webinar-bssn-2025-serie-1-kenalan-sama-ai-teman-atau-ancaman/>