KECERDASAN BUATAN (*ARTIFICIAL INTELLIGENCE*) DALAM PERSPEKTIF PENEGAKAN HUKUM DI INDONESIA [1]

Oleh :
Fenly Aprylo Pesak [2]
Firdja Baftim [3]
Dientje Rumimpunu [4]

ABSTRAK

Penelitian ini bertujuan untuk mengetahui dan memahami pengaturan kecerdasan buatan dalam perspektif penegakan hukum di Indonesia dan untuk mengetahui dan memahami penegakan hukum terhadap kecerdasan buatan dalam perspektif penegakan hukum di Indonesia. Penelitian ini menggunakan metode penelitian yuridis normatif, dapat ditarik kesimpulan yaitu : 1. Pengaturan hukum terhadap Kecerdasan Buatan di Indonesia masih bersifat sektoral, parsial, dan belum membentuk rezim hukum yang komprehensif. Ketiadaan undang-undang spesifik yang secara langsung mengatur AI memaksa penegak hukum untuk bertumpu pada instrumen yang ada seperti UU ITE, UU PDP, dan Surat Edaran Menteri terkait, yang secara fundamental belum dirancang untuk mengantisipasi karakteristik unik AI yang otonom dan *self-learning*. 2. Praktik penegakan hukum terhadap penyalahgunaan AI di Indonesia masih bersifat reaktif dan sangat bergantung pada interpretasi ekstensif aparat penegak hukum, seperti yang dicontohkan oleh Putusan Pengadilan Negeri Bojonegoro Nomor 125/Pid.Sus/2019/PN Bjn. Kasus ini menunjukkan bahwa UU ITE, khususnya Pasal 29 dan 35, dapat diregangkan untuk menjerat kejahatan manipulasi gambar (cikal bakal *deepfake*), namun keberhasilan ini lebih merupakan hasil *judicial activism* ketimbang dari kepastian norma.

Kata Kunci : *artificial intelligence, penegakan hukum, Indonesia*

PENDAHULUAN

A. Latar Belakang

Perkembangan pesat teknologi kecerdasan buatan (*Artificial Intelligence / AI*) membawa perubahan mendasar pada berbagai bidang kehidupan mulai dari layanan kesehatan, industri, pemerintahan, hingga sistem peradilan. AI memungkinkan otomatisasi keputusan, pengolahan data besar (*big* data), prediksi perilaku, dan pembuatan konten sintetik (mis. *deepfake*) yang memiliki dampak langsung terhadap hak-hak dasar individu dan kepentingan publik.[5] Di satu sisi, inovasi teknologi tersebut membuka peluang efisiensi dan peningkatan kualitas layanan; di sisi lain, muncul tantangan serius dalam kaitan perlindungan hukum, tanggung jawab pidana/perdata, dan kepastian hak sipil—terutama ketika instrumen hukum positif belum mengatur aspek teknis maupun konsekuensi baru dari penggunaan AI.[6]

Catatan yuridis di Indonesia menunjukkan bahwa belum terdapat definisi AI yang eksplisit dalam undang-undang pokok; oleh karenanya regulator domestik cenderung merujuk AI ke dalam kerangka hukum eksisting seperti konsep *agen elektronik* atau penyelenggaraan sistem elektronik.[7] Misalnya, Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) menaruh banyak peraturan yang relevan terhadap perbuatan berbasis sistem elektronik (mis. pengiriman informasi ancaman, pemalsuan atau manipulasi informasi), tetapi UU ITE tidak mengatur spesifik aspek algoritma, audit, penjelasan keputusan otomatis (*explainability*), atau pembagian tanggung jawab bagi aktor-aktor yang terlibat dalam siklus hidup AI.[8] Ketiadaan pengaturan substantif ini menjadikan timbulnya celah hukum (*legal lacuna*) ketika persoalan AI berwujud konkret di masyarakat.[9]

Kekosongan regulasi (*regulatory gap*) terhadap fenomena baru seperti AI adalah persoalan multidimensional: bersifat substantif (tidak ada norma yang khusus mengatur), struktural (kesenjangan kapasitas legislatif dan aparat penegak), dan prosedural (keterlambatan

---

[1] Artikel Skripsi
[2] Mahasiswa Fakultas Hukum Unsrat, NIM 19071101678
[3] Fakultas Hukum Unsrat, Magister Ilmu Hukum
[4] Fakultas Hukum Unsrat, Magister Ilmu Hukum

[5] Organisation for Economic Co-operation and Development (OECD) & Eurostat, *Artificial Intelligence in Society: Opportunities and Challenges*, OECD Publishing, Paris, 2021, hlm. 5–7.
[6] Ryan Calo, 'Robots and the Lessons of Cyberlaw', *California Law Review*, Vol. 103, 2015, hlm. 513–516.
[7] Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Pasal 1
[8] UU No. 11/2008 tentang ITE; Undang-Undang Nomor 19 Tahun 2016 (Perubahan atas UU ITE); lihat pembahasan yuridis mengenai keterbatasan UU ITE terhadap fenomena AI dalam: Potensi Pelanggaran Hak Konstitusional dalam Penggunaan Kecerdasan Buatan, *Hukumonline*, 15 Mei 2025, hlm. 2–3.
[9] John Bell & Marie-Claire Cordonier Segger (eds.), *Regulatory Law and Governance for the Anthropocene*, Routledge, London, 2020, hlm. 23–25 (membahas *regulatory gap* dalam konteks teknologi baru).

FAKULTAS HUKUM UNSRAT 2026

mekanisme evaluasi regulasi).[10] Pendekatan tradisional hukum positif yang menunggu legislasi spesifik selama ini seringkali tidak mampu mengejar laju inovasi teknologi sehingga menimbulkan ketidakpastian hukum bagi korban maupun pelaku usaha.[11] Di samping itu, penggunaan norma analogis (mis. menerapkan pasal pengancaman atau pornografi pada kasus konten *deepfake*) menimbulkan masalah pembuktian, ketepatan tipologi delik, dan adil-guna (*proportionality*) dalam penjatuhan sanksi.[12]

Respon regulator Indonesia sejauh ini bersifat parsial: Peraturan Pemerintah tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE) memberi kerangka bagi penyelenggara sistem elektronik, Undang-Undang Pelindungan Data Pribadi (UU PDP) mengatur tentang data yang sering menjadi bahan baku AI, dan Kementerian Komunikasi dan Informatika (Kominfo) telah mengeluarkan Surat Edaran Nomor 9 Tahun 2023 tentang Etika Kecerdasan Artifisial sebagai pedoman etis (*soft law*).[13] Meskipun demikian, aturan-aturan tersebut belum menciptakan rangka normatif yang komprehensif misalnya standar audit algoritma, kewajiban keterbukaan model (model *disclosure*), atau aturan liability khusus bagi sistem otonom sehingga masalah tanggung jawab, adjudikasi, dan perlindungan korban belum teratasi secara memadai.[14]

Studi ini akan menempatkan permasalahan pada titik temu antara inovasi teknologi (yang menuntut keluwesan dan ruang eksperimen) dan kebutuhan kepastian hukum (yang menuntut norma jelas, akuntabilitas, dan perlindungan hak). Pendekatan kajian akan berangkat dari analisis doktrin hukum (teori kekosongan regulasi), telaah peraturan positif Indonesia (UU ITE, UU PDP, PP PSTE, SE Kominfo), dan studi kasus yuridis sebagai contoh empiris bagaimana peradilan menangani masalah-masalah AI secara praktis. Kajian seperti ini diharapkan mampu merumuskan alternatif kebijakan misalnya pengaturan berbasis risiko, kewajiban transparansi algoritmik, mekanisme audit independen, dan model tanggung jawab berbagi (*shared liability*) yang feasible secara hukum dan efektif secara sosial.[15]

Contoh Kasus nyata yang terjadi yakni Putusan Pengadilan Negeri Bojonegoro Nomor 125/Pid.Sus/2019/PN Bjn (Perkara pembuatan foto rekayasa bermuatan pornografi yang digunakan untuk pengancaman*)*. Kasus ini sering dikutip dalam literatur sebagai contoh penyalahgunaan rekayasa gambar/video (kini sering terkait dengan istilah *deepfake*) yang menimbulkan kerugian dan ancaman bagi korban.[16]

Amar putusan dalam perkara ini yakni Pengadilan Negeri menjatuhkan pidana kepada Terdakwa berupa pidana penjara selama 1 (satu) tahun 4 (empat) bulan. Putusan menyatakan bahwa perbuatan Terdakwa memenuhi unsur Pasal 29 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (sebagaimana telah diubah) terkait pengiriman informasi elektronik yang berisi ancaman/kekerasan atau menakut-nakuti secara pribadi; dan hakim juga menyinggung perbuatan manipulasi informasi sebagaimana Pasal 35 UU ITE (penciptaan/ manipulasi informasi elektronik agar tampak otentik) serta relevansi dengan UU Pornografi dan UU Hak Cipta ketika dipertimbangkan dampaknya pada korban.[17]

Pertimbangan hakim (dalam ringkasan) Majelis hakim menilai bahwa elemen objektif dan subjektif tindak pidana pengiriman informasi berisi ancaman terpenuhi: ada pengiriman foto hasil suntingan, ada ancaman penyebaran, dan adanya tujuan menakut-nakuti korban sehingga mendapat konsekuensi psikologis dan pemaksaan tindakan (video call). Hakim memutus berdasarkan norma UU ITE karena itu merupakan instrumen yang paling relevan untuk menjerat penggunaan media elektronik dalam konteks ancaman; hakim juga mempertimbangkan aspek kepentingan perlindungan kesusilaan dan potensi pelanggaran hak cipta/privasi korban. Putusan ini kemudian menjadi rujukan praktek untuk perkara-perkara manipulasi gambar/ancaman berbasis teknologi digital.[18]

Implikasi hukum dari kasus ini yakni putusan ini menggambarkan praktik pengisian celah hukum (*gap-filling*) oleh peradilan menggunakan ketentuan eksisting (UU ITE, UU Pornografi, UU

[10] OECD, *Regulatory Policy and Governance*, OECD Publishing, Paris, 2012, hlm. 47–49.
[11] H.L.A. Hart, *The Concept of Law*, 3rd ed., Clarendon Press, Oxford, 2012, hlm. 130–133
[12] Sudikno Mertokusumo, *Penemuan Hukum*, Liberty, Yogyakarta, 2012, hlm. 78–80
[13] *Surat Edaran Menteri Komunikasi dan Informatika Nomor 9 Tahun 2023 tentang Etika Kecerdasan Artifisial*, 19 Desember 2023; serta Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP).
[14] Marinews Mahkamah Agung, *Artificial Intelligence: Peluang dan Tantangan Pemanfaatannya*, artikel 23 Juli 2025, hlm. 3–4
[15] Julia Black, *Risk and Regulation: Journal of Law and Society*, Vol. 27, No. 2, 2000, hlm. 325–327
[16] Putusan Pengadilan Negeri Bojonegoro Nomor 125/Pid.Sus/2019/PN Bjn
[17] Ibid., hlm. 131–137
[18] Ibid., hlm. 131–136

FAKULTAS HUKUM UNSRAT 2026

Hak Cipta) untuk menuntaskan perbuatan berbasis teknologi yang pada masa itu belum familiar secara terminologi (seperti *deepfake*). Walaupun memberikan solusi hukum bagi korban, putusan tersebut juga mengilustrasikan keterbatasan instrument hukum yang ada: bukti forensik digital, nomenklatur delik yang tepat, dan ketentuan sanksi yang spesifik terhadap teknologi manipulasi belum terjemahkan secara komprehensif dalam undang-undang.[19]

B. Rumusan Masalah

1. Bagaimana pengaturan kecerdasan buatan dalam perspektif penegakan hukum di Indonesia?
2. Bagaimana penegakan hukum terhadap kecerdasan buatan dalam perspektif penegakan hukum di Indonesia?

C. Metode Penelitian

Metode pendekatan yang digunakan dalam penelitian ini adalah Metode Yuridis Normatif.

PEMBAHASAN

A. Pengaturan Kecerdasan Buatan (*Artificial Intelligence*) Dalam Perspektif Penegakan Hukum Di Indonesia

Perkembangan teknologi informasi yang pesat telah membawa perubahan signifikan dalam berbagai aspek kehidupan, termasuk dalam bidang hukum. Salah satu perkembangan yang paling menonjol adalah kemunculan kecerdasan buatan (Artificial Intelligence/AI) yang mampu meniru kemampuan kognitif manusia dalam mengolah data, mengambil keputusan, dan menghasilkan konten digital. Dalam perspektif penegakan hukum di Indonesia, keberadaan AI menimbulkan tantangan baru, terutama terkait dengan bagaimana hukum mampu mengatur, mengawasi, dan menindak penyalahgunaan teknologi tersebut. Hal ini menjadi penting mengingat AI tidak hanya digunakan untuk tujuan positif, tetapi juga berpotensi disalahgunakan untuk kepentingan yang melanggar hukum.[20]

Dalam sistem hukum Indonesia, pengaturan mengenai AI belum diatur secara khusus dalam suatu undang-undang tersendiri. Namun, berbagai peraturan perundang-undangan yang ada telah digunakan untuk mengakomodasi permasalahan yang timbul akibat penggunaan teknologi digital, termasuk AI. Salah satu regulasi utama adalah Undang-Undang Nomor 11 Tahun 2008 sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016, yang mengatur mengenai penggunaan informasi dan transaksi elektronik serta sanksi terhadap penyalahgunaannya.[21]

Salah satu regulasi utama yang digunakan dalam mengatur aspek teknologi digital di Indonesia adalah Undang-Undang Nomor 11 Tahun 2008 sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik. Undang-undang ini mengatur berbagai aspek terkait penggunaan informasi elektronik, transaksi elektronik, serta sanksi terhadap penyalahgunaannya. Dalam konteks AI, UU ITE sering dijadikan dasar hukum untuk menindak perbuatan yang melibatkan teknologi digital. Meskipun demikian, substansi UU ITE tidak secara eksplisit mengatur mengenai AI, sehingga penerapannya terhadap teknologi tersebut masih bersifat terbatas. Hal ini menunjukkan adanya kesenjangan antara norma hukum yang ada dengan perkembangan teknologi yang terjadi.[22]

UU ITE pada dasarnya dirancang untuk mengatur aktivitas di ruang siber secara umum, seperti transaksi elektronik, keamanan informasi, dan perlindungan data. Namun, AI sebagai teknologi yang memiliki karakteristik khusus, seperti kemampuan belajar mandiri dan pengambilan keputusan otomatis, memerlukan pendekatan regulasi yang berbeda. Dalam hal ini, UU ITE belum mampu menjangkau aspek-aspek kompleks yang melekat pada AI. Misalnya, dalam hal pertanggungjawaban hukum atas keputusan yang dihasilkan oleh sistem AI. Tanpa adanya pengaturan khusus, maka penentuan tanggung jawab menjadi sulit dilakukan. Hal ini menunjukkan bahwa regulasi yang ada belum cukup untuk mengatur AI secara komprehensif.[23] Selain UU ITE, terdapat pula beberapa peraturan lain yang secara tidak langsung berkaitan dengan penggunaan AI, seperti Undang-Undang Perlindungan Data Pribadi dan peraturan terkait keamanan siber. Peraturan-peraturan ini memberikan kerangka hukum yang dapat

[19] Artikel-artikel kompilatif tentang *deepfake* dan kekosongan regulasi di Indonesia; lihat juga: "Kejahatan Siber Deepfake di Era Kecerdasan Buatan", Marinews Mahkamah Agung, 7 Mei 2025, hlm. 1–3; dan Tinjauan Hukum Pidana Terhadap Penyebaran Deepfake, *J-Innovative* 2025, hlm. 2–5.

[20] Budi Suhariyanto, *Tindak Pidana Teknologi Informasi*, Jakarta: RajaGrafindo, 2013, hlm. 45.

[21] UU No. 11 Tahun 2008 jo. UU No. 19 Tahun 2016 tentang ITE.

[22] Undang-Undang Nomor 11 Tahun 2008 jo. Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik.

[23] Edmon Makarim, *Hukum Telematika di Indonesia*, Jakarta: RajaGrafindo Persada, 2005, hlm. 163.

LEX CRIMEN UNSRAT 2026

digunakan untuk mengatur aspek tertentu dari AI, seperti pengelolaan data dan keamanan sistem. Namun, pengaturan tersebut masih bersifat parsial dan belum mencakup keseluruhan aspek AI. Akibatnya, terdapat celah hukum yang dapat dimanfaatkan untuk melakukan penyalahgunaan teknologi. Hal ini menunjukkan bahwa diperlukan pendekatan yang lebih holistik dalam mengatur AI.[24]

Dalam perspektif penegakan hukum, penggunaan regulasi yang tidak spesifik terhadap AI menimbulkan berbagai kendala. Aparat penegak hukum seringkali mengalami kesulitan dalam mengkualifikasikan suatu perbuatan yang melibatkan AI sebagai tindak pidana atau pelanggaran hukum lainnya. Hal ini disebabkan oleh tidak adanya definisi dan batasan yang jelas mengenai AI dalam peraturan perundang-undangan. Selain itu, karakteristik AI yang kompleks juga menyulitkan dalam proses pembuktian di pengadilan. Tanpa adanya pedoman yang jelas, maka penegakan hukum menjadi tidak efektif dan berpotensi menimbulkan ketidakadilan.[25]

Permasalahan lain yang muncul adalah terkait dengan pertanggungjawaban hukum atas penggunaan AI. Dalam sistem hukum Indonesia, pertanggungjawaban hukum umumnya didasarkan pada prinsip kesalahan (fault liability). Namun, dalam konteks AI, sulit untuk menentukan adanya unsur kesalahan, terutama jika AI bertindak secara otonom. Hal ini menimbulkan pertanyaan mengenai siapa yang harus bertanggung jawab atas kerugian yang ditimbulkan oleh AI. Apakah tanggung jawab berada pada pengembang, pengguna, atau pihak lain yang terkait. Tanpa adanya pengaturan yang jelas, maka penentuan tanggung jawab menjadi kabur dan berpotensi menimbulkan sengketa.[26] Selain itu, penggunaan AI juga menimbulkan tantangan dalam aspek perlindungan hukum bagi masyarakat. Teknologi AI dapat digunakan untuk berbagai tujuan, termasuk yang bersifat merugikan, seperti penyebaran informasi palsu (*fake news*), manipulasi data, dan pelanggaran privasi. Dalam kondisi ini, masyarakat menjadi pihak yang rentan terhadap dampak negatif AI. Negara memiliki kewajiban untuk melindungi masyarakat dari risiko tersebut melalui regulasi yang memadai. Namun, tanpa adanya pengaturan khusus mengenai AI, perlindungan hukum yang diberikan menjadi tidak optimal. Hal ini menunjukkan bahwa pengaturan AI sangat penting untuk menjamin hak-hak masyarakat.[27]

Untuk mengatasi berbagai permasalahan tersebut, diperlukan langkah konkret dari pemerintah dalam menyusun regulasi khusus mengenai AI. Regulasi ini harus mencakup berbagai aspek, seperti definisi AI, ruang lingkup penggunaan, standar keamanan, serta mekanisme pertanggungjawaban hukum. Selain itu, regulasi juga harus bersifat adaptif terhadap perkembangan teknologi yang sangat dinamis. Dalam proses pembentukannya, diperlukan keterlibatan berbagai pihak, termasuk akademisi, praktisi hukum, dan pelaku industri. Dengan demikian, regulasi yang dihasilkan dapat bersifat komprehensif dan mampu menjawab kebutuhan hukum yang ada.[28]

Dalam perspektif penegakan hukum, UU ITE menjadi instrumen utama dalam menjerat pelaku kejahatan berbasis teknologi, termasuk yang melibatkan AI. Pasal 29 UU ITE, misalnya, mengatur tentang larangan mengirimkan informasi elektronik yang berisi ancaman atau menakut-nakuti secara pribadi. Selain itu, Pasal 35 UU ITE mengatur tentang larangan melakukan manipulasi informasi elektronik agar tampak seolah-olah autentik. Kedua pasal ini menjadi relevan dalam menangani kasus-kasus penyalahgunaan teknologi seperti manipulasi gambar atau video berbasis AI.[29]

Salah satu contoh nyata penerapan ketentuan tersebut dapat dilihat dalam Putusan Pengadilan Negeri Bojonegoro Nomor 125/Pid.Sus/2019/PN Bjn. Dalam perkara ini, terdakwa terbukti melakukan manipulasi foto korban dengan cara mengedit wajah korban ke dalam gambar yang mengandung unsur pornografi, kemudian menggunakan hasil manipulasi tersebut untuk mengancam korban. Perbuatan ini menunjukkan bagaimana teknologi digital, yang dalam perkembangan saat ini dapat dikaitkan dengan konsep deepfake, digunakan sebagai alat untuk melakukan kejahatan.

Kronologi kasus tersebut menunjukkan bahwa pelaku mengunduh foto korban dari media sosial, kemudian menggunakan aplikasi pengedit gambar untuk membuat konten manipulatif yang menyerupai korban. Hasil manipulasi tersebut kemudian dikirimkan kepada korban disertai

[24] Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.
[25] Sudikno Mertokusumo, *Mengenal Hukum*, Yogyakarta: Liberty, 2007, hlm. 140.
[26] Moeljatno, *Asas-Asas Hukum Pidana*, Jakarta: Rineka Cipta, 2008, hlm. 81.
[27] Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia.
[28] Satjipto Rahardjo, *Ilmu Hukum*, hlm. 92.
[29] Ibid.

FAKULTAS HUKUM UNSRAT 2026

ancaman penyebaran jika korban tidak mengikuti keinginan pelaku. Tindakan ini menimbulkan tekanan psikologis yang signifikan bagi korban dan menunjukkan adanya unsur pemaksaan yang dilakukan melalui media elektronik.[30]

Majelis hakim dalam perkara tersebut menilai bahwa unsur-unsur tindak pidana sebagaimana diatur dalam Pasal 29 UU ITE telah terpenuhi. Terdapat pengiriman informasi elektronik berupa gambar hasil manipulasi, adanya ancaman penyebaran, serta tujuan untuk menakut-nakuti korban. Selain itu, hakim juga mempertimbangkan adanya manipulasi informasi sebagaimana dimaksud dalam Pasal 35 UU ITE, meskipun pasal tersebut tidak dijadikan dasar utama dalam pemidanaan.[31]

Dalam perspektif hukum pidana, kasus ini menunjukkan bahwa hukum positif Indonesia masih menggunakan pendekatan konvensional dalam menjerat kejahatan berbasis teknologi. Artinya, perbuatan yang dilakukan dengan teknologi canggih seperti AI tetap dikualifikasikan ke dalam delik-delik yang sudah ada, tanpa adanya klasifikasi khusus terhadap teknologi tersebut. Hal ini menunjukkan adanya pendekatan technology-neutral, di mana hukum tidak secara spesifik menyebut teknologi tertentu, tetapi mengatur perbuatannya.[32] Namun demikian, pendekatan tersebut memiliki keterbatasan, terutama dalam menghadapi perkembangan teknologi AI yang semakin kompleks. Misalnya, dalam kasus deepfake, sulit untuk membedakan antara konten asli dan hasil manipulasi tanpa menggunakan teknologi forensik digital yang canggih. Hal ini menimbulkan tantangan dalam pembuktian di pengadilan, yang pada akhirnya dapat mempengaruhi efektivitas penegakan hukum.[33]

Dalam konteks hukum pembuktian, penggunaan AI juga menimbulkan persoalan terkait keabsahan alat bukti elektronik. Undang-Undang Nomor 8 Tahun 1981 belum secara eksplisit mengatur mengenai bukti digital yang dihasilkan oleh sistem AI. Meskipun UU ITE telah mengakui informasi elektronik sebagai alat bukti yang sah, namun standar pembuktiannya masih memerlukan pengembangan lebih lanjut, khususnya dalam menghadapi teknologi manipulatif seperti deepfake.[34] Selain UU ITE, pengaturan terkait AI juga dapat dikaitkan dengan Undang-Undang Nomor 44 Tahun 2008 yang melarang pembuatan dan penyebaran konten pornografi. Dalam kasus Bojonegoro, meskipun fokus utama adalah ancaman, namun konten yang digunakan memiliki unsur pornografi yang dapat menambah beratnya perbuatan pelaku. Hal ini menunjukkan adanya irisan antara berbagai rezim hukum dalam menangani kejahatan berbasis teknologi.[35] Lebih lanjut, aspek perlindungan hak cipta juga relevan dalam konteks ini, sebagaimana diatur dalam Undang-Undang Nomor 28 Tahun 2014. Penggunaan foto tanpa izin serta manipulasi terhadap karya orang lain dapat dikategorikan sebagai pelanggaran hak cipta. Dalam kasus ini, foto korban yang diambil dari media sosial digunakan tanpa persetujuan, yang berpotensi melanggar hak ekonomi dan moral pemilik karya.[36]

Dalam perspektif hak asasi manusia, penyalahgunaan AI seperti dalam kasus tersebut juga melanggar hak atas privasi dan martabat manusia. Undang-Undang Nomor 39 Tahun 1999 menjamin perlindungan terhadap kehormatan dan martabat setiap individu. Penyebaran konten manipulatif yang merugikan reputasi seseorang jelas bertentangan dengan prinsip tersebut.[37]

Beberapa negara telah mulai mengembangkan regulasi khusus terkait AI, seperti Uni Eropa dengan AI Act. Indonesia dapat mengambil pelajaran dari perkembangan tersebut untuk merumuskan kebijakan yang sesuai dengan kondisi nasional. Hal ini penting agar Indonesia tidak tertinggal dalam menghadapi tantangan hukum di era digital.[38]

Dalam jangka panjang, pengaturan AI juga harus mempertimbangkan aspek etika dan tanggung jawab sosial. Penggunaan teknologi harus diarahkan untuk memberikan manfaat bagi masyarakat, bukan sebaliknya. Oleh karena itu, diperlukan pendekatan multidisipliner yang melibatkan hukum, teknologi, dan etika dalam merumuskan kebijakan terkait AI.[39]

Dengan demikian, dapat disimpulkan bahwa pengaturan AI dalam perspektif penegakan hukum di Indonesia masih bersifat parsial dan belum komprehensif. Kasus Putusan PN Bojonegoro menjadi contoh nyata bagaimana hukum berusaha mengisi kekosongan regulasi dengan menggunakan ketentuan yang ada. Meskipun demikian, pendekatan tersebut memiliki

[30] Putusan PN Bojonegoro No. 125/Pid.Sus/2019/PN Bjn.
[31] Ibid.
[32] Andi Hamzah, *Asas-Asas Hukum Pidana*, Jakarta: Rineka Cipta, 2010, hlm. 112.
[33] Edmon Makarim, *Pengantar Hukum Telematika*, Jakarta: Rajawali Pers, 2015, hlm. 134.
[34] KUHAP (UU No. 8 Tahun 1981).
[35] UU No. 44 Tahun 2008 tentang Pornografi.
[36] UU No. 28 Tahun 2014 tentang Hak Cipta.
[37] UU No. 39 Tahun 1999 tentang HAM.
[38] European Commission, *Artificial Intelligence Act*, 2021.
[39] Lawrence M. Friedman, *The Legal System*, hlm. 16.

FAKULTAS HUKUM UNSRAT 2026

keterbatasan yang perlu diatasi melalui pembentukan regulasi yang lebih spesifik. Akhirnya, penegakan hukum terhadap penyalahgunaan AI memerlukan sinergi antara regulasi yang memadai, aparat penegak hukum yang kompeten, serta kesadaran masyarakat yang tinggi. Tanpa adanya ketiga elemen tersebut, upaya untuk menciptakan keadilan dan kepastian hukum dalam era digital akan sulit tercapai. Oleh karena itu, penguatan sistem hukum dalam menghadapi perkembangan AI menjadi suatu keniscayaan.

B. Penegakan Hukum Terhadap Kecerdasan Buatan Dalam Perspektif Penegakan Hukum Di Indonesia.

Perkembangan Kecerdasan Buatan (AI) telah menghadirkan lompatan kuantum dalam peradaban digital, namun secara simultan menciptakan anomali hukum yang belum terpecahkan secara tuntas oleh kerangka regulasi konvensional. Dalam konteks penegakan hukum di Indonesia, permasalahan mendasar bukan hanya terletak pada kecepatan legislasi yang tertinggal dari inovasi teknologi, tetapi juga pada pergeseran paradigma pertanggungjawaban pidana. Ketika sebuah algoritma *deepfake* mampu menghasilkan konten manipulatif yang sulit dibedakan dari realitas, aparat penegak hukum dihadapkan pada dilema epistemologis: membuktikan otentisitas suatu bukti elektronik di tengah kapasitas AI untuk merekonstruksi realitas secara sintetis.[40] Kondisi ini memaksa sistem peradilan pidana untuk melakukan reinterpretasi terhadap asas legalitas, mengingat karakteristik AI yang otonom dan self-learning kerap mengaburkan rantai kausalitas antara perbuatan pelaku, alat yang digunakan, dan akibat yang ditimbulkan. Lebih jauh lagi, penegakan hukum terhadap penyalahgunaan AI di Indonesia masih bersifat reaktif dan fragmentaris, belum membentuk suatu konstruksi yuridis yang holistik dalam memandang AI bukan sekadar sebagai alat kejahatan (*instrumentum sceleris*), melainkan sebagai entitas yang mentransformasi modus operandi kejahatan secara fundamental.[41]

Ketiadaan rezim hukum spesifik yang mengatur AI secara komprehensif memaksa aparat penegak hukum untuk merujuk pada instrumen-instrumen hukum positif yang telah ada, seperti Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagaimana telah diubah, sebagai 'jaring pengaman' utama.[42] Pendekatan ini, meskipun pragmatis dan diperlukan untuk mengisi kekosongan hukum (*rechtsvacuum*), mengandung kelemahan inheren karena UU ITE dirancang pada era di mana teknologi manipulasi media belum secanggih generasi AI terkini. Pasal-pasal seperti Pasal 27 hingga Pasal 35 UU ITE, yang mengatur tentang konten ilegal dan manipulasi informasi, memiliki spektrum interpretasi yang sangat luas dan berpotensi menimbulkan ketidakpastian hukum apabila diterapkan secara analogi pada kasus-kasus berbasis generative AI.[43] Problematika ini menjadi semakin pelik ketika kita menganalisis tipologi kejahatan seperti *deepfake*, yang secara substansial tidak hanya melanggar kesusilaan, tetapi juga mengkonstruksi realitas palsu yang dapat menghancurkan integritas informasi publik dan martabat individu secara permanen. Oleh karena itu, penegakan hukum di Indonesia saat ini berada dalam fase transisi yang menuntut adanya judicial activism dari para hakim untuk melakukan terobosan hukum tanpa melanggar prinsip nullum crimen sine lege.

Salah satu preseden penting yang dapat dijadikan sebagai batu uji dalam menganalisis pendekatan penegakan hukum Indonesia terhadap penyalahgunaan teknologi manipulatif adalah Putusan Pengadilan Negeri Bojonegoro Nomor 125/Pid.Sus/2019/PN Bjn. Kasus ini, meskipun secara temporal terjadi sebelum istilah deepfake populer di Indonesia, merepresentasikan pola dasar kejahatan AI yang menggunakan rekayasa gambar untuk menciptakan realitas palsu yang bersifat destruktif.[44] Dalam perkara ini, terdakwa Eko Purwanto tidak hanya sekadar menyebarkan konten pornografi, melainkan melakukan proses manipulasi visual dengan mengunduh foto-foto pribadi korban dari media sosial, lalu mentransplantasikan wajah para korban ke dalam gambar-gambar bugil yang diunduh dari sumber lain menggunakan aplikasi pengedit gambar, seperti friends blender atau perangkat lunak sejenis. Proses ini secara esensial identik dengan cara kerja face-swapping yang menjadi basis

[40] Mireille Hildebrandt, *Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology* (Cheltenham: Edward Elgar Publishing, 2015), hlm. 147.

[41] Lawrence Lessig, *Code: Version 2.0* (New York: Basic Books, 2006), hlm. 123.

[42] Sinta Dewi Rosadi, *Cyber Law: Aspek Hukum Privasi dan Data Pribadi* (Bandung: PT Refika Aditama, 2015), hlm. 98.

[43] Maskun dan Wiwik Meilarati, *Aspek Hukum Penipuan Digital* (Makassar: CV. Social Politic Genius, 2019), hlm. 67.

[44] Putusan Pengadilan Negeri Bojonegoro Nomor 125/Pid.Sus/2019/PN Bjn, hlm. 4-5.

FAKULTAS HUKUM UNSRAT 2026

teknologi deepfake berbasis AI generatif modern, di mana elemen biometrik korban diambil alih secara sepihak untuk menciptakan representasi palsu. Tindakan terdakwa yang mengirimkan hasil suntingan tersebut kepada korban disertai ancaman penyebarluasan ke media sosial menunjukkan adanya eskalasi dari sekadar pelanggaran privasi menjadi pemaksaan dan teror psikologis yang terstruktur.[45]

Analisis mendalam terhadap kronologi perkara ini menunjukkan bahwa aparat penegak hukum dan majelis hakim sedang berhadapan dengan manifestasi awal dari kejahatan siber yang bersifat *hybrid*, di mana batas antara dunia fisik dan representasi digital menjadi kabur. Para korban tidak hanya dirugikan secara moral karena foto bermuatan pornografi, tetapi juga kehilangan kendali atas identitas digital mereka; wajah mereka diobjektifikasi dan digunakan sebagai alat pemerasan. Dalam kerangka penegakan hukum, tantangan utamanya adalah bagaimana membuktikan bahwa kumpulan piksel yang direkayasa itu telah menimbulkan akibat hukum yang nyata, yaitu rasa takut dan paksaan terhadap korban.[46] Majelis hakim dalam perkara ini menerapkan konstruksi yuridis Pasal 29 UU ITE, yang mengkriminalisasi pengiriman informasi elektronik berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi. Pemilihan pasal ini sangat krusial karena menunjukkan bahwa fokus pemidanaan tidak semata-mata pada konten porno yang dihasilkan, melainkan pada motif dan dampak ancaman yang ditimbulkan oleh penyalahgunaan hasil rekayasa gambar tersebut. Ini merupakan langkah progresif di mana hakim mengidentifikasi bahwa substansi kejahatan terletak pada "ancaman" yang dimediasi oleh teknologi.

Penerapan Pasal 29 UU ITE dalam perkara a quo menimbulkan diskursus menarik mengenai titik berat penegakan hukum di era AI, apakah pada output konten ilegal atau pada intent serta impact dari penggunaan teknologi. Dengan menjerat pelaku menggunakan pasal ancaman, pengadilan secara implisit mengakui bahwa kemampuan manipulasi gambar telah menciptakan "senjata digital" baru yang daya paksanya setara dengan ancaman konvensional.[47] Terdakwa memanfaatkan ketidakmampuan korban untuk menyangkal otentisitas gambar rekayasa tersebut; dalam alam pikir korban, jika gambar itu tersebar, sosial akan menghakimi berdasarkan apa yang terlihat, bukan berdasarkan fakta manipulasi. Di sinilah kekhususan kejahatan berbasis AI generatif: ia menyerang tidak hanya individu, tetapi juga meracuni epistemologi sosial, yaitu kepercayaan publik terhadap kebenaran visual.[48] Hakim Bojonegoro dengan cerdas melihat bahwa perbuatan terdakwa memenuhi elemen objektif (pengiriman foto suntingan) dan subjektif (niat menakut-nakuti dan memaksa korban melakukan video call). Putusan ini membuktikan bahwa instrumen hukum yang ada, meskipun belum menyebut kata AI, secara substansi mampu menangkap esensi kejahatan jika aparat penegak hukum melakukan interpretasi teleologis yang berorientasi pada perlindungan korban.

Selain Pasal 29 UU ITE, pertimbangan hakim yang menyinggung relevansi Pasal 35 UU ITE membuka pintu bagi diskursus tentang standar otentisitas informasi elektronik. Pasal 35 mengatur larangan memanipulasi informasi elektronik agar tampak seolah-olah otentik. Dalam konteks AI deepfake, masalah otentisitas ini menjadi inti permasalahan.[49] *Algoritma Generative Adversarial Networks* (GANs), yang merupakan mesin dari deepfake, bekerja dengan cara membuat suatu konten palsu yang justru terlihat sangat "alami". Perbuatan terdakwa dalam kasus Bojonegoro, yang menggabungkan wajah korban ke tubuh orang lain, adalah upaya untuk menciptakan kesan "otentik" palsu yang dapat merusak reputasi. Apabila dikaitkan dengan Undang-Undang Perlindungan Data Pribadi (UU PDP), pengambilan data biometrik wajah dari Facebook tanpa izin dan pemanfaatannya untuk manipulasi juga merupakan pelanggaran serius terhadap prinsip pemrosesan data.[50] Namun, karena UU PDP belum berlaku efektif pada saat putusan dijatuhkan, pendekatan UU ITE menjadi

[45] Eddy O.S. Hiariej, *Prinsip-Prinsip Hukum Pidana* (Yogyakarta: Cahaya Atma Pustaka, 2016), hlm. 132.

[46] Bobby Duffy, *The Perils of Perception: Why We're Wrong About Nearly Everything* (London: Atlantic Books, 2018), hlm. 210.

[47] Danielle K. Citron, *Hate Crimes in Cyberspace* (Cambridge: Harvard University Press, 2014), hlm. 73.

[48] Robert Chesney dan Danielle Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security", *California Law Review*, Vol. 107, No. 6, 2019, hlm. 1785.

[49] Eoghan Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*, 3rd ed. (Waltham: Academic Press, 2011), hlm. 459.

[50] Dwi Ratna Arianti, "Perlindungan Hukum Terhadap Data Pribadi di Era Ekonomi Digital", *Jurnal Legislasi Indonesia*, Vol. 16, No. 2, 2019, hlm. 178.

LEX CRIMEN UNSRAT 2026

satu-satunya remedium yang memungkinkan. Hal ini menunjukkan bahwa meskipun terjadi ketertinggalan legislasi (legal lag), hakim sebagai corong keadilan dapat menjembatani celah tersebut melalui interpretasi yang ekstensif namun tetap dalam batas penalaran hukum yang sah.

Dalam konteks penegakan hukum yang lebih luas, kasus Bojonegoro mengajarkan kita tentang bahaya automation bias dalam sistem peradilan. Jika ke depan terdapat perkara di mana sebuah video deepfake yang sangat sempurna diajukan sebagai alat bukti, akankah aparat penegak hukum memiliki kapasitas forensik digital yang mumpuni untuk membedakannya? Putusan Nomor 125/Pid.Sus/2019/PN Bjn ini beruntung karena manipulasi yang dilakukan masih tergolong sederhana dan pengakuan terdakwa memperkuat pembuktian.[51] Namun, dengan kemajuan AI, bukan tidak mungkin ke depan akan muncul situasi di mana seorang saksi atau korban justru dikriminalisasi balik dengan tuduhan fitnah karena pelaku berhasil membuat rekayasa yang meyakinkan seolah-olah korbanlah pelaku. Hal ini menuntut peningkatan kapasitas sumber daya manusia penegak hukum, baik polisi, jaksa, maupun hakim, dalam memahami seluk-beluk teknologi deep learning dan forensik digital. Tanpa pemahaman tersebut, pengadilan berpotensi menjadi panggung untuk melegitimasi kebohongan struktural yang dihasilkan oleh algoritma.[52]

Dari perspektif perlindungan korban, penegakan hukum dalam kasus ini sebenarnya telah menerapkan prinsip *victim-centric approach* meskipun secara sederhana. Hakim mengakui penderitaan psikologis korban akibat ancaman penyebaran foto. Namun, dalam ekosistem AI modern, diperlukan mekanisme ganti rugi dan pemulihan yang lebih progresif. Bagaimana sistem hukum memulihkan nama baik seseorang yang wajahnya telah "dicuri" untuk konten pornografi, jika konten tersebut telah menyebar secara viral melalui platform pesan terenkripsi?[53] UU ITE dan KUHP belum memberikan kerangka restitusi yang jelas untuk pemulihan identitas digital. Negara, dalam hal ini, perlu memikul tanggung jawab untuk memaksa pelaku dan platform digital turut serta dalam proses digital wiping atau setidaknya delisting konten. Putusan ini hanya menyentuh pada pemidanaan pelaku, tetapi belum menyentuh dimensi pemulihan kedaulatan data korban. Peristiwa pemaksaan video call juga menunjukkan adanya potensi eksploitasi seksual lanjutan yang belum tentu tertampung dalam dakwaan, sebuah dark figure of crime yang kerap luput dari jaring penegakan hukum.

Analisis lebih lanjut menunjukkan adanya irisan yang menarik antara rezim UU ITE, UU Hak Cipta, dan UU Pornografi yang disebut hakim dalam pertimbangannya. Unsur hak cipta sebenarnya unik karena wajah seseorang bukanlah objek hak cipta, melainkan bagian dari hak privasi dan data pribadi.[54] Namun, penyebutan ini mengindikasikan kebingungan awal dalam menempatkan perlindungan atas fitur biometrik dalam skema hukum properti intelektual. Pada era AI, fitur wajah adalah behavioral data yang bernilai ekonomi tinggi. Kasus Bojonegoro membuktikan bahwa sistem hukum kita cenderung menggunakan pendekatan multi-tafsir lintas undang-undang untuk menambal celah-celah yang ada. Strategi ini menunjukkan bahwa penegakan hukum di Indonesia masih bertumpu pada legal hybridization, yaitu memanfaatkan pasal-pasal dari berbagai sektor untuk menghadapi kejahatan yang multidimensi.[55] Pendekatan ini efektif untuk solusi jangka pendek (*stop-gap measure*), namun rapuh karena rawan menimbulkan disparitas putusan dan tidak memberikan kepastian standar penanganan perkara AI di masa depan.

Penegakan hukum terhadap AI juga tidak bisa dilepaskan dari isu kedaulatan digital dan yurisdiksi. Meskipun terdakwa dalam kasus Bojonegoro adalah individu yang jelas identitasnya dan perbuatannya dilakukan secara langsung tanpa melintasi batas negara, kejahatan deepfake kontemporer kerap melibatkan pelaku lintas negara atau penggunaan server asing.[56] Jika aplikasi friends blender yang digunakan tersebut menyimpan data di server luar negeri, muncul potensi jurisdictional conflict. Bagaimana aparat penegak hukum Indonesia mengakses bukti digital yang berada di bawah yurisdiksi asing tanpa melanggar kedaulatan negara lain? Konvensi Budapest tentang Kejahatan Siber, yang belum

[51] Josua Sitompul, *Cyberspace, Cybercrimes, Cyberlaw: Tinjauan Aspek Hukum Pidana* (Jakarta: Tatanusa, 2012), hlm. 295.

[52] Satjipto Rahardjo, *Penegakan Hukum: Suatu Tinjauan Sosiologis* (Yogyakarta: Genta Publishing, 2009), hlm. 47.

[53] Wahyudi Djafar et al., *Perlindungan Data Pribadi di Indonesia* (Jakarta: Lembaga Studi dan Advokasi Masyarakat (ELSAM), 2020), hlm. 89.

[54] Agus Sardjono, *Hak Kekayaan Intelektual dan Tantangan Implementasinya di Indonesia* (Depok: UI Press, 2019), hlm. 102.

[55] M. Arsyad Sanusi, *Hukum dan Teknologi* (Jakarta: Sinar Grafika, 2017), hlm. 158.

[56] Sigid Suseno, *Yurisdiksi Tindak Pidana Siber* (Bandung: PT Refika Aditama, 2013), hlm. 88.

diratifikasi Indonesia hingga kini, sebenarnya menyediakan kerangka kerja sama internasional untuk akses data lintas batas yang cepat.[57] Keengganan meratifikasi konvensi ini menempatkan aparat penegak hukum kita dalam posisi yang inferior ketika berhadapan dengan kejahatan AI yang bersifat transnasional. Akibatnya, pengungkapan kasus seperti Bojonegoro berikutnya, yang mungkin sudah menggunakan teknologi AI berbasis cloud computing internasional, akan menemui kebuntuan pada fase penyidikan.

Dalam kerangka pembangunan hukum nasional, putusan Bojonegoro adalah sebuah "batu loncatan" menuju kodifikasi hukum AI di Indonesia. Para hakim dalam sistem *civil law* tidak terikat pada preseden, namun putusan ini memiliki kekuatan persuasif yang kuat. Para perumus kebijakan harus mencermati bahwa perbuatan seperti yang dilakukan Eko Purwanto akan berlipat ganda dengan hadirnya AI *text-to-image* dan video generators yang semakin mudah diakses publik. Jika dulu pelaku butuh waktu berjam-jam untuk mengedit foto secara manual di *Photoshop*, kini dengan Stable Diffusion atau Midjourney, hanya dalam hitungan detik wajah seseorang dapat dimasukkan ke dalam skenario apapun yang diinginkan. Ini berarti niat jahat (*mens rea*) dapat dieksekusi dengan kecepatan yang belum pernah terjadi dalam sejarah kriminalitas. Oleh karena itu, penegakan hukum harus di-backup dengan kebijakan due diligence yang ketat terhadap penyedia layanan AI, termasuk kewajiban untuk memiliki *content safety system*.

Pertimbangan lain yang krusial adalah potensi penggunaan AI tidak hanya oleh pelaku individu, tetapi juga oleh aktor politik untuk menciptakan kampanye hitam. Jika satu individu dapat menyebabkan trauma sedemikian rupa pada korban di Bojonegoro, apa yang dapat dilakukan oleh entitas terorganisir dengan sumber daya besar untuk menciptakan deepfake politis? Penegakan hukum di Indonesia harus siap menghadapi *weaponization of AI* dalam skala masif. Di sinilah letak urgensi penguatan kapasitas siber Polri dan BSSN untuk mampu melakukan deteksi dini dan take down konten secara real-time. Menunggu sampai korban mengadu, seperti yang terjadi pada korban dalam perkara ini, bukanlah strategi yang memadai di tengah serangan yang bersifat high-speed dan high-impact. Perlu dibangun mekanisme *public-private partnership* di mana platform media sosial diwajibkan secara hukum untuk proaktif memfilter konten deepfake non-konsensual tanpa harus menunggu perintah pengadilan.

Dari perspektif filsafat pemidanaan, putusan satu tahun empat bulan memicu perdebatan tentang tujuan pemidanaan di era disrupsi digital. Teori retributif menuntut hukuman setimpal dengan derita korban; jika penderitaan psikologis korban sangat dalam, maka pidananya pun harus berat. Teori *deterrence* (penjeraan) juga menghendaki hukuman yang keras untuk menakuti calon pelaku lain di tengah tren peningkatan kejahatan siber. Namun, teori rehabilitatif melihat bahwa pelaku manipulasi deepfake mungkin juga memerlukan intervensi psikologis, karena obsesi seksual menyimpang yang memanfaatkan teknologi. Putusan Bojonegoro condong ke arah retributif ringan, yang boleh jadi karena keterbatasan tuntutan. Ke depan, jaksa perlu lebih berani menuntut maksimal dengan memperhitungkan dampak kualitatif dari penyalahgunaan AI, yaitu kehancuran integritas digital seseorang. Penegakan hukum yang progresif harus memandang peretasan identitas sebagai bentuk kekerasan digital yang serius, bukan hanya sekadar kenakalan di dunia maya.

Kaitannya dengan Hak Asasi Manusia (HAM), penyalahgunaan AI yang menimpa korban di Bojonegoro merupakan pelanggaran terhadap hak atas rasa aman dan perlindungan diri pribadi sebagaimana dijamin UUD 1945. Negara tidak boleh abai karena kewajiban negara dalam kerangka duty to protect adalah melindungi warga dari ancaman, termasuk ancaman yang bersumber dari teknologi tinggi. Jika negara hanya menyediakan UU ITE tanpa memberikan output pemidanaan yang efektif dan dukungan infrastruktur digital yang aman, maka negara telah lalai memenuhi kewajiban konstitusionalnya. Oleh karena itu, putusan ini harus menjadi pengingat bahwa penegakan hukum terhadap AI bukan semata-mata soal teknis pasal, tetapi soal keberpihakan negara melindungi harkat dan martabat manusia dari eksploitasi algoritma. Setiap keterlambatan dalam merespons kejahatan ini adalah bentuk pengingkaran terhadap hak konstitusional warga negara untuk hidup dengan aman dan bebas dari rasa takut.

Menelisik lebih dalam, istilah "aplikasi sejenis *friends blender*" yang disebut dalam putusan menunjukkan bahwa perangkat lunak yang digunakan pelaku adalah tools yang relatif mudah diperoleh. Di era Gen-AI, akses terhadap teknologi semacam itu semakin demokratis, yang

[57] Council of Europe, *Convention on Cybercrime (Budapest Convention)*, ETS No. 185, 2001.

FAKULTAS HUKUM UNSRAT 2026

berimplikasi pada potensi lonjakan pelaku dari berbagai lapisan masyarakat. Penegakan hukum harus mengantisipasi fenomena *democratization of crime*.[58] Tidak diperlukan keahlian teknis tinggi untuk menjadi pelaku deepfake saat ini. Hal ini membutuhkan edukasi hukum masif kepada masyarakat bahwa mengedit foto orang lain menjadi konten negatif adalah kejahatan serius. Selama ini, banyak pihak menganggap remeh "iseng" mengedit foto. Putusan Bojonegoro mengirimkan pesan *deterrence* yang jelas bahwa "iseng" tersebut dapat berujung pada penjara. Sosialisasi putusan-putusan semacam ini oleh aparat penegak hukum sama pentingnya dengan pembuatan regulasi baru, karena berfungsi sebagai *social defence* untuk mencegah kriminalisasi massal warga yang tidak paham hukum.

Selanjutnya, dari sudut pandang integritas bukti, kekhawatiran terbesar di masa depan adalah ketika pelaku menggunakan AI untuk menghasilkan bukti palsu guna menghancurkan alibi. Misalnya, terdakwa dapat mengklaim bahwa rekaman CCTV yang menunjukkan dirinya di TKP adalah hasil deepfake yang dijebakkan oleh musuhnya. Ini disebut sebagai liar's dividend, di mana keberadaan teknologi deepfake dimanfaatkan oleh para penjahat untuk menyangkal bukti yang sah.[59] Dalam kasus Bojonegoro, bukti masih berpihak pada kebenaran karena pelaku tidak dapat menyangkal bukti digital yang ada. Namun, bagaimana jika di persidangan berikutnya seorang terdakwa yang lebih cerdas teknologi berargumen bahwa log pengiriman dan gambar adalah rekayasa AI yang ditanamkan oleh hacker? Sistem peradilan kita harus siap dengan standard operating procedure (SOP) forensik yang ketat, termasuk analisis metadata dan rantai kustodi barang bukti digital yang tidak terputus, untuk mematahkan argumen liar's dividend tersebut. Tanpa itu, penegakan hukum bisa lumpuh oleh keraguan yang diciptakan oleh kecanggihan AI itu sendiri.

Kesimpulannya, penegakan hukum terhadap Kecerdasan Buatan dalam perspektif Indonesia yang tercermin dari penanganan kasus Bojonegoro menunjukkan bahwa sistem kita mampu merespons, namun respons itu masih bersifat tambal sulam dan sangat bergantung pada kejelian hakim semata. Putusan 125/Pid.Sus/2019/PN Bjn adalah bukti bahwa UU ITE, sebagai *living law digital*, dapat diregangkan untuk menutupi kelambanan legislasi.[60] Akan tetapi, kita tidak bisa selamanya mengandalkan kebijaksanaan individual hakim tanpa adanya kepastian hukum. Diperlukan reformasi hukum pidana materiil yang memasukkan bab khusus tentang "Tindak Pidana Berbasis Kecerdasan Buatan", yang meliputi definisi, kualifikasi, pemberatan pidana, serta tanggung jawab penyedia platform. Penegakan hukum yang ideal di masa depan adalah yang bersifat technology-neutral namun harm-specific; aturan tidak perlu menyebut aplikasi spesifik, tetapi harus jelas mengkriminalisasi "dampak" yang ditimbulkan oleh teknologi otomatis, seperti manipulasi realitas yang merugikan. Kasus Bojonegoro adalah pelajaran berharga bahwa di balik setiap piksel rekayasa, ada potensi kehancuran hidup manusia yang harus ditebus dengan kepastian hukum yang tegas dan tidak kompromis.

PENUTUP

A. Kesimpulan

1. Pengaturan hukum terhadap Kecerdasan Buatan di Indonesia masih bersifat sektoral, parsial, dan belum membentuk rezim hukum yang komprehensif. Ketiadaan undang-undang spesifik yang secara langsung mengatur AI memaksa penegak hukum untuk bertumpu pada instrumen yang ada seperti UU ITE, UU PDP, dan Surat Edaran Menteri terkait, yang secara fundamental belum dirancang untuk mengantisipasi karakteristik unik AI yang otonom dan *self-learning*. Hal ini menciptakan *regulatory gap* yang serius, mengakibatkan ketidakpastian hukum terutama dalam menentukan subjek pertanggungjawaban pidana dan standar validitas alat bukti digital hasil rekayasa AI. Dengan demikian, landasan filosofis, sosiologis, dan yuridis untuk penegakan hukum yang efektif di era AI belum tertanam kuat dalam kerangka hukum positif Indonesia, sehingga diperlukan akselerasi legislasi yang bersifat antisipatif dan *technology-neutral* untuk mengisi kekosongan hukum ini.
2. Praktik penegakan hukum terhadap penyalahgunaan AI di Indonesia masih bersifat reaktif dan sangat bergantung pada interpretasi ekstensif aparat penegak hukum, seperti yang dicontohkan oleh Putusan Pengadilan Negeri Bojonegoro Nomor

[58] Marc Goodman, *Future Crimes: Inside the Digital Underground and the Battle for Our Connected World* (New York: Anchor Books, 2015), hlm. 332.

[59] Henry Ajder et al., "The State of Deepfakes: Landscape, Threats, and Impact", *Deeptrace*, September 2019, hlm. 14.

[60] Abdul Halim Barkatullah, *Hukum Transaksi Elektronik di Indonesia* (Bandung: Nusa Media, 2019), hlm. 231.

FAKULTAS HUKUM UNSRAT 2026

125/Pid.Sus/2019/PN Bjn. Kasus ini menunjukkan bahwa UU ITE, khususnya Pasal 29 dan 35, dapat diregangkan untuk menjerat kejahatan manipulasi gambar (cikal bakal *deepfake*), namun keberhasilan ini lebih merupakan hasil *judicial activism* ketimbang dari kepastian norma. Penegakan hukum menghadapi tantangan multidimensional, mulai dari pembuktian forensik digital yang kompleks, rendahnya literasi AI di kalangan aparat, hingga potensi distorsi realitas akibat *liar's dividend* yang dapat melumpuhkan proses peradilan. Fokus pemidanaan yang masih berorientasi pada pelaku (*offender-oriented*) dan belum sepenuhnya mengintegrasikan pemulihan kerugian korban (*victim-centric*) menandakan bahwa sistem peradilan pidana kita belum sepenuhnya siap menghadapi masifnya dampak destruktif dari kejahatan berbasis AI.

B. Saran

1. Pemerintah bersama Dewan Perwakilan Rakyat perlu segera mengambil inisiatif untuk membentuk kerangka regulasi nasional yang komprehensif dan spesifik mengenai Kecerdasan Buatan. Regulasi ini idealnya tidak hanya berbentuk satu undang-undang sektoral, melainkan sebuah rezim hukum yang mengintegrasikan aspek pidana, perdata, dan administratif. Selain itu, regulasi harus menganut pendekatan *risk-based approach* seperti model *EU AI Act*, yang mengklasifikasikan risiko AI untuk menentukan tingkat kewajiban pengembang dan pengguna, serta secara tegas mengatur larangan praktik AI berbahaya seperti *social scoring* oleh pihak swasta dan *deepfake* non-konsensual. Tanpa adanya kepastian hukum yang jelas, penegakan hukum akan terus berjalan di tempat, terombang-ambing oleh tafsir yang berpotensi melanggar asas legalitas.
2. Peningkatan kapasitas kelembagaan dan sumber daya manusia aparat penegak hukum harus menjadi prioritas utama. Program pelatihan yang berkelanjutan dan masif mengenai forensik digital, analisis metadata, dan pemahaman teknis *Generative AI* perlu diwajibkan bagi penyidik Polri, jaksa, dan hakim. Selain itu, Mahkamah Agung disarankan untuk segera menerbitkan pedoman teknis (PERMA atau SEMA) tentang penanganan perkara yang melibatkan alat bukti elektronik hasil AI, termasuk standar pengujian otentisitas bukti untuk menangkal fenomena *liar's dividend*. Kerja sama internasional melalui ratifikasi Konvensi Budapest juga menjadi langkah esensial untuk mempermudah akses data lintas batas dalam penyidikan kejahatan AI. Terakhir, paradigma penegakan hukum harus diubah menjadi lebih progresif dan berorientasi pada korban, termasuk menyediakan mekanisme *digital wiping* dan restitusi yang terstandarisasi untuk memulihkan hak-hak korban kejahatan berbasis AI.

DAFTAR PUSTAKA

BUKU

Bell, John & Marie-Claire Cordonier Segger (eds.). *Regulatory Law and Governance for the Anthropocene*. London: Routledge, 2020.

Berger, Peter L. dan Thomas Luckmann. *The Social Construction of Reality: A Treatise in the Sociology of Knowledge*. New York: Anchor Books, 1966.

Drahos, Peter & John Braithwaite. *Information Feudalism: Who Owns the Knowledge Economy?*. London: Earthscan, 2002.

Duffy, Bobby. *The Perils of Perception: Why We're Wrong About Nearly Everything*. London: Atlantic Books, 2018.

Friedman, Lawrence M. *The Legal System: A Social Science Perspective*. New York: Russell Sage Foundation, 1975.

Foucault, Michel. *Power/Knowledge: Selected Interviews and Other Writings 1972–1977*. New York: Pantheon Books, 1980.

Goodman, Marc. *Future Crimes: Inside the Digital Underground and the Battle for Our Connected World*. New York: Anchor Books, 2015.

Hamzah, Andi. *Asas-Asas Hukum Pidana*. Jakarta: Rineka Cipta, 2010.

Hart, H.L.A. *The Concept of Law*, edisi ke-3. Oxford: Clarendon Press, 2012.

Hiariej, Eddy O.S. *Prinsip-Prinsip Hukum Pidana*. Yogyakarta: Cahaya Atma Pustaka, 2016.

Hildebrandt, Mireille. *Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology*. Cheltenham: Edward Elgar Publishing, 2015.

Husserl, Edmund. *Ideas Pertaining to a Pure Phenomenology and to a Phenomenological Philosophy*. Dordrecht: Kluwer Academic Publishers, 1983.

Lessig, Lawrence. *Code: Version 2.0*. New York: Basic Books, 2006.

FAKULTAS HUKUM UNSRAT 2026

Makarim, Edmon. *Hukum Telematika di Indonesia*. Jakarta: RajaGrafindo Persada, 2005.
Marzuki, Peter Mahmud. *Penelitian Hukum*, Cetakan ke-4. Jakarta: Kencana Prenata Media Group, 2008.
Mertokusumo, Sudikno. *Mengenal Hukum: Suatu Pengantar*, Edisi Revisi. Yogyakarta: Cahaya Atma Pustaka, 2010.
Mertokusumo, Sudikno. *Penemuan Hukum*. Yogyakarta: Liberty, 2012.
Moeljatno. *Asas-Asas Hukum Pidana*. Jakarta: Rineka Cipta, 2008.
Muladi dan Barda Nawawi Arief. *Teori-Teori dan Kebijakan Pidana*. Bandung: Alumni, 2010.
Rahardjo, Satjipto. *Hukum Progresif*. Jakarta: Kompas, 2009.
Rahardjo, Satjipto. *Ilmu Hukum*. Bandung: Citra Aditya Bakti, 2014.
Rahardjo, Satjipto. *Masalah Penegakan Hukum: Suatu Tinjauan Sosiologis*. Bandung: Sinar Baru, 1983.
Rahardjo, Satjipto. *Penegakan Hukum: Suatu Tinjauan Sosiologis*. Yogyakarta: Genta Publishing, 2009.
Ramli, Ahmad. *Cyber Law dan HAKI dalam Sistem Hukum Indonesia*. Bandung: Refika Aditama, 2010.
Rosadi, Sinta Dewi. *Cyber Law: Aspek Hukum Privasi dan Data Pribadi*. Bandung: PT Refika Aditama, 2015.
Sanusi, M. Arsyad. *Hukum dan Teknologi*. Jakarta: Sinar Grafika, 2017.
Sitompul, Josua. *Cyberspace, Cybercrimes, Cyberlaw: Tinjauan Aspek Hukum Pidana*. Jakarta: Tatanusa, 2012.
Soekanto, Soerjono dan Sri Mamudji. *Penelitian Hukum Normatif Suatu Tinjauan Singkat*, Cetakan ke-14. Jakarta: PT RajaGrafindo Persada, 2012.
Soekanto, Soerjono. *Faktor-Faktor yang Mempengaruhi Penegakan Hukum*, Cetakan ke-15. Jakarta: PT RajaGrafindo Persada, 2014.
Soekanto, Soerjono. *Pengantar Penelitian Hukum*. Jakarta: UI Press, 1989.
Soemitro, Ronny Hanitijo. *Metodologi Penelitian Hukum Dan Jurimetri*. Jakarta: Ghalia Indonesia, 1990.
Subagyo, P. Joko. *Metode Penelitian Dalam Teori & Praktik*. Jakarta: Rineka Cipta, 2011.
Suhariyanto, Budi. *Tindak Pidana Teknologi Informasi*. Jakarta: RajaGrafindo, 2013.
Suseno, Sigid. *Yurisdiksi Tindak Pidana Siber*. Bandung: PT Refika Aditama, 2013.
Widodo. *Hukum Pidana di Bidang Teknologi Informasi*. Yogyakarta: Aswaja, 2013.

PERATURAN PERUNDANG-UNDANGAN

Undang - Undang Dasar Negara Republik Indonesia Tahun 1945.
Kitab Undang-Undang Hukum Pidana (KUHP).
Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana (KUHAP).
Undang-Undang Nomor 1 Tahun 2004 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.
Undang-Undang Nomor 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-undangan.
Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia.
Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.
Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.
Surat Edaran Menteri Komunikasi dan Informatika Nomor 9 Tahun 2023 tentang Etika Kecerdasan Artifisial.
Putusan Pengadilan Negeri Bojonegoro Nomor 125/Pid.Sus/2019/PN Bjn.
Universal Declaration of Human Rights, 1948.

JURNAL / LAPORAN

Ajder, Henry, et al. "The State of Deepfakes: Landscape, Threats, and Impact." *Deeptrace*, September 2019.
Arianti, Dwi Ratna. "Perlindungan Hukum Terhadap Data Pribadi di Era Ekonomi Digital." *Jurnal Legislasi Indonesia*, Vol. 16, No. 2, 2019.
Black, Julia. "Risk and Regulation." *Journal of Law and Society*, Vol. 27, No. 2, 2000.
Calo, Ryan. "Robots and the Lessons of Cyberlaw." *California Law Review*, Vol. 103, 2015.
Chesney, Robert, dan Danielle Citron. "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security." *California Law Review*, Vol. 107, No. 6, 2019.
Coglianese, Cary, dan David Lehr. "Regulating by Robot: Administrative Decision Making in the Machine-Learning Era." *Georgetown Law Journal*, Vol. 105, 2017.
Henry, Nicola, Asher Flynn, dan Anastasia Powell. "Technology-Facilitated Sexual Violence: A Literature Review of Empirical

FAKULTAS HUKUM UNSRAT 2026

Research." *Trauma, Violence, & Abuse*, Vol. 19, No. 2, 2018.

Mahanani, Anies, dan Sulistyanta. "Tinjauan Yuridis Tindak Pidana Pengancaman dengan Foto Rekayasa Bermuatan Pornografi (Studi Putusan Nomor: 125/Pid.Sus/2019/PN Bjn)." *Recidive: Jurnal Hukum Pidana dan Penanggulangan Kejahatan*, Vol. 11, No. 1, 2022.

Noviantama, D. "Deepfake: A Review from The Victimology Perspective." *CICL Journal*, 2024.

INTERNET

Hukumonline. "Potensi Pelanggaran Hak Konstitusional dalam Penggunaan Kecerdasan Buatan." *Hukumonline.com*, 15 Mei 2025.

Kumparan. "Arti Perspektif dalam Bahasa Indonesia." *Kumparan.com*. https://kumparan.com/ragam-info/arti-perspektif-dalam-bahasa-indonesia-20cQLj7Cwn8. Diakses pada 2026.

Mahkamah Agung. "Artificial Intelligence: Peluang dan Tantangan Pemanfaatannya." *Marinews Mahkamah Agung*, 23 Juli 2025.

Mahkamah Agung. "Kejahatan Siber Deepfake di Era Kecerdasan Buatan." *Marinews Mahkamah Agung*, 7 Mei 2025.

Repository Poltekkes Tanjungkarang. "BAB II." *repository.poltekkes-tjk.ac.id*. https://repository.poltekkes-tjk.ac.id/id/eprint/6984/6/6.%20BAB%20II.pdf. Diakses pada 2026.

Tim Redaksi Bola.com. "Arti Perspektif dalam Berbagai Bidang." *Bola.com*. https://www.bola.com/ragam/read/5245364/arti-perspektif-dalam-berbagai-bidang. Diakses pada 2026.

Tim Redaksi KBBI. "Perspektif." *KBBI Daring*. https://kbbi.web.id/perspektif. Diakses pada 2026.

FAKULTAS HUKUM UNSRAT 2026