

Tantangan Penegakan Hukum dan Upaya Mitigasi atas Hadirnya Deepfake Porn sebagai Jenis Tindak Pidana Digital pada Era Artificial Intelligence

Diyanggi Priya Romaito Pane^{1*}, Alexandro Wiranto Tambe²

^{1,2}Universitas Padjadjaran, Indonesia

Email: diyanggipriya1611@gmail.com¹, tambesandro@gmail.com²

Alamat: Jl. Raya Bandung Sumedang KM.21, Hegarmanah, Kec. Jatinangor, Kabupaten Sumedang, Jawa Barat, Indonesia

Korespondensi penulis: diyanggipriya1611@gmail.com*

Abstract. Technological developments in the modern era have experienced rapid growth, one of which is through the advancement of Artificial Intelligence (AI). This technology has now become an integral part of people's daily lives because it can provide convenience, efficiency, and innovation in various fields. However, behind the benefits offered, AI also carries potential risks, especially when misused. One of the most worrying forms of misuse is deepfakes, namely AI-based digital content manipulation that can convincingly imitate a person's voice, face, and movements. Deepfakes have triggered various digital crimes, such as identity forgery, the creation and distribution of non-consensual pornographic content including sexual exploitation, blackmailing, the spread of fake news (hoaxes), digital terror, fraud, and defamation. The increasingly sophisticated level of AI in manipulating data demands swift action, appropriate regulations, and effective oversight strategies from the government to anticipate its negative impacts. This research uses a normative juridical method with a statute approach and a conceptual approach. This approach allows for a comprehensive analysis of the existing legal framework, the concept of legal protection, and the urgency of establishing new regulations related to AI technology. The research findings indicate that the government needs to take a number of strategic steps, including: (1) drafting specific regulations governing the use and limitations of AI, particularly regarding deepfakes; (2) developing and implementing effective deepfake detection technology; (3) providing protection, recovery, and rehabilitation mechanisms for victims; and (4) implementing widespread public education to raise public awareness of the risks of AI misuse.

Keywords: artificial intelligence, deepfake porn, digital crimes, law enforcement, mitigation

Abstrak. Perkembangan teknologi pada era modern mengalami peningkatan yang pesat, salah satunya melalui kemajuan Artificial Intelligence (AI). Teknologi ini kini telah menjadi bagian integral dalam kehidupan sehari-hari masyarakat karena mampu memberikan kemudahan, efisiensi, dan inovasi di berbagai bidang. Namun, di balik manfaat yang ditawarkan, AI juga membawa potensi risiko, terutama ketika disalahgunakan. Salah satu bentuk penyalahgunaan yang paling mengkhawatirkan adalah deepfake, yaitu manipulasi konten digital berbasis AI yang mampu meniru suara, wajah, dan gerak seseorang secara meyakinkan. Deepfake telah memicu berbagai tindak pidana digital, seperti pemalsuan identitas, pembuatan dan penyebaran konten pornografi non-konsensual termasuk eksploitasi seksual, pemerasan (*blackmailing*), penyebaran berita bohong (*hoax*), teror digital, penipuan, hingga pencemaran nama baik. Tingkat kecanggihan AI yang semakin akurat dalam memanipulasi data menuntut adanya langkah cepat, regulasi yang tepat, dan strategi pengawasan yang efektif dari pemerintah untuk mengantisipasi dampak negatifnya. Penelitian ini menggunakan metode yuridis normatif dengan pendekatan peraturan perundang-undangan (*statute approach*) dan pendekatan konseptual (*conceptual approach*). Pendekatan ini memungkinkan analisis yang komprehensif terhadap kerangka hukum yang ada, konsep perlindungan hukum, serta urgensi pembentukan regulasi baru terkait teknologi AI. Hasil penelitian menunjukkan bahwa pemerintah perlu melakukan sejumlah langkah strategis, meliputi: (1) penyusunan regulasi khusus yang mengatur penggunaan dan batasan AI, terutama terkait deepfake; (2) pengembangan dan penerapan teknologi deteksi deepfake yang efektif; (3) penyediaan mekanisme perlindungan, pemulihan, dan rehabilitasi bagi korban; serta (4) pelaksanaan edukasi publik secara luas untuk meningkatkan kesadaran masyarakat terhadap risiko penyalahgunaan AI.

Kata kunci: kecerdasan buatan, deepfake porn, tindak pidana digital, penegakan hukum, mitigasi

1. LATAR BELAKANG

Laju perkembangan teknologi di era *society 5.0* sungguh pesat, bahkan hampir tidak terkendali. Salah satu bentuk progresivitas tersebut adalah ekspansi teknologi yang mampu melampaui kemampuan manusia, yakni *Artificial Intelligence* (AI). Kemunculan AI menjadi sebuah fenomena yang menguntungkan sekaligus merugikan. Umumnya, cara kerja AI adalah mereplikasi otak manusia dalam mengelola informasi mulai dari menerima, mengolah, menyimpan, memutus serta mengubah informasi tersebut menjadi bentuk lain (Soeprajitno, 2019). AI dapat juga berperilaku layaknya manusia serta meniru kecerdasan manusia dalam menyelesaikan berbagai tugas hingga menggantikan manusia dalam pekerjaan tertentu (Pakpahan, 2021).

Perkembangan AI memang tidak dapat dibendung, kini AI telah menjadi bagian teknologi masa kini dan dapat dengan mudah ditemukan dalam berbagai bidang kehidupan, termasuk aktivitas sehari-hari. Misalnya pada sektor hukum, beberapa firma hukum telah menggunakan AI untuk membantu kuasa hukum dalam memecahkan masalah pada kasus-kasus tertentu, seperti program AI bernama ROSS pada firma hukum Baker Hostetler di Amerika Serikat (Shravan & Bhora, 2019). Contoh lain pada industri perfilman, yakni film *Fast and Furious 7* yang menggunakan *face tracking* dan Computer-Generated Imagery pada aktor yang memerankan Brian O'Conner (DeRuvo & McCormick, 2024). Kemampuan AI seperti ini menjadi terobosan baru yang memberikan dampak positif. Akan tetapi, perkembangan AI tidak selalu bergerak ke arah positif karena kecanggihannya berpotensi menghasilkan jenis kejahatan baru, seperti manipulasi wajah, audio dari teks, dan pembuatan karya 3D dengan tingkat kemiripan yang hampir sama dengan buatan manusia atau bahkan melampauinya.

Salah satu kejahatan AI yang paling mengkhawatirkan masyarakat dan sudah tidak asing lagi adalah *deepfake*. Istilah *deepfake* berasal dari gabungan dua kata, yakni *deep learning*, yang merujuk pada teknologi pembelajaran mesin tingkat lanjut, dan *fake*, yang berarti palsu atau tiruan (Banke & Gandrova, 2023). *Deepfake* dapat menganalisis *big data* untuk meniru mimik wajah, perilaku seseorang, audio, dan intonasi suara seseorang menggunakan teknologi *Generative Adversarial Network* (Banke & Gandrova, 2023). Lahirnya *deepfake* sangat berpengaruh dalam kehidupan sehari-hari karena seringkali memunculkan hasil karya berupa duplikasi atau rekayasa yang memanfaatkan foto, video, atau audio seseorang dari internet tanpa izin dari pihak yang bersangkutan. Lebih lanjut, *deepfake* terbagi menjadi 5 (lima) kategori utama (Naitali, Ridouani, Salahdine, & Kaabouch, 2023): (1) *Attribute manipulation* hanya memanipulasi bagian yang relevan dengan atribut untuk mengubah penampilan wajah

dengan melepas atau mengenakan kacamata, memperbaiki kulit, bahkan mengubah usia atau jenis kelamin. (2) *Entire face synthesis* adalah jenis manipulasi yang melibatkan pembuatan gambar wajah manusia yang tidak ada dalam kehidupan nyata. (3) *Lip-syncing* akan menghasilkan wajah target tampak otentik dan disinkronkan dengan *input* teks atau audio yang diberikan, sehingga gerakan bibir menjadi akurat dan ekspresi wajah selaras dengan sumber suara. (4) *Face reenactment* adalah teknik manipulasi yang berfokus pada pengubahan ekspresi wajah seseorang dalam video. (5) *Identity swap* adalah bentuk manipulasi yang mengganti wajah seseorang dalam video dengan wajah orang lain.

Secara umum, *identity swap*, *face reenactment*, dan *lip-syncing* menjadi jenis *deepfake* yang paling sering digunakan. Akan tetapi, kepraktisan *deepfake* ini justru dipandang sebagai peluang untuk berbuat kejahatan oleh sebagian orang, sehingga melahirkan berbagai bentuk tindak pidana digital, seperti pemalsuan identitas, konten pornografi non-konsensual termasuk eksploitasi seksual, pemerasan (*blackmailing*), penyebaran berita bohong, penyebaran teror, penipuan, pencemaran nama baik, dan lain-lain (Banke & Gandrova, 2023).

Secara historis, *deepfake* marak digunakan pada tahun 2017 ketika disalahgunakan dan disebarkan pada *platform* Reddit. Para pengguna aplikasi saling berbagi video porno hasil manipulasi *deepfake* yang menampilkan artis-artis *hollywood* setelah tubuhnya diganti dengan tubuh artis porno (Pertiwi & Riyanto, 2022). Bahkan, berita terbaru melaporkan adanya penipuan dengan menggunakan teknologi *deepfake* terhadap seorang pegawai keuangan di sebuah perusahaan multinasional di Hongkong, sehingga korban mengalami kerugian senilai Rp401 miliar (Retno, 2024).

Sementara itu, jumlah pengguna *platform online* di Indonesia terus meningkat menjadi 221.563.479 orang dari 278.696.200 total penduduk pada tahun 2023 (APJII, 2025). Jumlah ini mengakibatkan potensi terjadinya *deepfake* semakin luas di Indonesia. Banyaknya jumlah pengguna tersebut didorong oleh kemudahan yang ditawarkan teknologi dalam melakukan berbagai pekerjaan yang selama ini terkendala, misalnya mempertimbangkan efisiensi waktu, tuntutan global, kondisi geografis yang kompleks, pandemi COVID-19, dan kendala lainnya (Sawitri & Wacika, 2023). Hal ini membuat perkembangan teknologi di Indonesia cenderung mengarah ke transformasi digital, sehingga setiap hari hampir semua pengguna media *online* berhubungan dengan internet.

Jumlah pengguna internet yang begitu masif ini pada faktanya berpengaruh pada peningkatan *deepfake* di Indonesia. Pada Oktober 2023, muncul sebuah video yang menampilkan Presiden Joko Widodo sedang berpidato dengan menggunakan bahasa mandarin yang begitu fasih. Kementerian Komunikasi dan Digital (Kemkomdigi) kemudian menyatakan

bahwa video tersebut merupakan tiruan yang diproduksi menggunakan teknologi *deepfake* (Mediana, 2023). Lebih berbahaya lagi, teknologi ini seringkali digunakan untuk konten-konten seksual, seperti kasus video seksual beberapa selebriti Indonesia yang sebenarnya adalah *deepfake* (Nistanto & Hardiansyah, 2022).

Berbagai kasus tersebut hanya segelintir contoh dari masifnya kejahatan *deepfake* di seluruh dunia. Pada skala internasional, sejak tahun 2019 sampai 2023 terjadi peningkatan luar biasa sebesar 400% dalam pembuatan *deepfake*. Peningkatan ini didominasi oleh *deepfake porn* sebesar 98% yang hampir semuanya menargetkan wanita (YahooFinance, 2024). Sementara skala nasional, pada tahun 2022, LBH APIK Jakarta melaporkan 440 kasus Kekerasan Berbasis Gender Online (KBGO) yang 49 kasusnya termasuk *non consensual intimate imagery*, yaitu penyebaran konten intim tanpa konsensual (Maharani, Sabili, Septia, Magistravia, & Tobing, 2023) dengan *deepfake porn* sebagai salah satu jenis teknologi yang digunakan di dalamnya (Maharani, Sabili, Septia, Magistravia, & Tobing, 2023). Kumpulan survei tersebut ternyata menunjukkan wanita rentan menjadi objek sasaran dari aksi pornografi yang umumnya dibuat oleh dan untuk para lelaki (Kasita, 2022).

Data-data peningkatan *deepfake*, baik skala internasional maupun nasional menjadi urgensi bagi pemerintah untuk mengambil langkah preventif dan represif dalam mengatasi *deepfake porn*. Kondisi ini diperparah dengan keamanan *cyber* di Indonesia yang belum maksimal dengan angka kasus serangan *malware* yang memprihatinkan. Mengacu pada data Badan Siber dan Sandi Negara, terdapat lebih dari 700 juta serangan siber yang didominasi *ransomware* dan *malware* terjadi di Indonesia pada 2022 (Admin CSIRT Banten, 2022). Pesatnya perkembangan AI yang semakin canggih dan teliti dalam memanipulasi data mewajibkan adanya regulasi dan upaya pemerintah yang lebih efektif untuk mengimbangi perkembangan AI. Akan tetapi, kenyataan menunjukkan bahwa cakupan regulasi Indonesia belum mampu memberikan perlindungan hukum yang akurat terkait AI, sehingga menghalangi penegakan hukum atas tindak pidana digital yang salah satunya adalah *deepfake porn*. Berdasarkan fakta di atas, penulis akan membahasnya lebih lanjut dengan judul tulisan “Tantangan Penegakan Hukum dan Upaya Mitigasi atas Hadirnya *Deepfake Porn* sebagai Jenis Tindak Pidana Digital pada Era *Artificial Intelligence*”. Hal ini didasari oleh dominasi kejahatan *deepfake* adalah konten pornografi, sehingga penegakan hukum terhadap *deepfake porn* memiliki urgensi masif untuk segera ditangani oleh pemerintah.

Adapun tujuan dari penelitian ini adalah untuk mengkaji secara kritis fenomena *deepfake porn* sebagai salah satu bentuk kejahatan digital yang berkembang seiring dengan kemajuan teknologi *Artificial Intelligence*. Fokus utama tulisan ini adalah untuk mengidentifikasi

tantangan-tantangan yang dihadapi dalam upaya penegakan hukum terhadap kejahatan tersebut, mulai dari ketertinggalan regulasi, kesulitan dalam proses pembuktian, hingga keterbatasan kapasitas aparat penegak hukum dalam memahami teknologi yang digunakan. Selain itu, tulisan ini juga menyoroti dampak sosial dan psikologis yang ditimbulkan terhadap korban, serta memperlihatkan celah hukum yang memungkinkan pelaku lolos dari jerat hukum. Melalui pendekatan yuridis-normatif, tulisan ini menawarkan alternatif solusi berupa penguatan kebijakan, peningkatan literasi digital, serta kolaborasi antara negara, sektor swasta, dan masyarakat sipil dalam mengembangkan mekanisme mitigasi dan pencegahan yang adaptif terhadap perkembangan teknologi. Diharapkan, kajian ini dapat memberikan kontribusi bagi pengembangan sistem hukum yang lebih responsif dalam menghadapi bentuk-bentuk baru tindak pidana di era digital.

2. KAJIAN TEORITIS

Konsep Artificial Intelligence

AI merupakan suatu sistem teknologi yang dirancang untuk meniru dan melaksanakan fungsi-fungsi kognitif manusia, seperti belajar, menganalisis, mengambil keputusan, serta memecahkan masalah. AI bekerja berdasarkan kemampuan pemrosesan data dalam jumlah besar yang dikombinasikan dengan algoritma pembelajaran mesin (*machine learning*) dan jaringan saraf tiruan (*neural networks*), yang secara bertahap memungkinkan sistem tersebut untuk melakukan tugas secara otomatis dan adaptif tanpa campur tangan manusia secara langsung (Russel & Norvig, 2021).

Dalam konteks kejahatan digital, AI berperan sebagai teknologi penggerak utama dalam pembuatan *deepfake*. Deepfake merupakan hasil manipulasi visual dan audio dengan memanfaatkan *deep learning*, sub-bidang dari AI, yang mampu mempelajari ekspresi wajah, gerakan bibir, dan suara dari seseorang, lalu menanamkannya pada wajah orang lain secara digital. Akibatnya, AI mampu menghasilkan konten visual yang *photorealistic* atau tampak sangat nyata, sehingga sulit dibedakan dari video asli (Koopman, Rodriguez, & Geradts, The Detection of Deepfake Videos Using Convolutional Neural Networks, 2020). Kecanggihan ini yang menjadikan AI sebagai alat potensial sekaligus berbahaya, terutama dalam konteks penyalahgunaan konten pornografi dan pencemaran nama baik.

Dalam perkembangan hukum, kemampuan AI yang semakin kompleks memunculkan urgensi akan pentingnya regulasi teknologi. Hal ini sejalan dengan pandangan *governance of technology*, yaitu bahwa teknologi tidak dapat dibiarkan berkembang tanpa kendali, karena berpotensi menimbulkan dampak etis, sosial, dan hukum yang luas (Floridi, et al.,

2018). Maka dari itu, negara perlu merumuskan kerangka hukum yang tidak hanya bersifat reaktif terhadap tindak pidana, tetapi juga bersifat preventif dan adaptif terhadap kemungkinan penyalahgunaan AI.

Definisi AI dalam hukum Indonesia sendiri masih terbatas dan belum diatur secara eksplisit. UU ITE melalui Pasal 1 angka 8 menyebut istilah “agen elektronik” sebagai sistem otomatis yang menjalankan perintah terhadap informasi elektronik. Akan tetapi, definisi ini belum mencakup kompleksitas AI modern, terutama dalam hal kemampuan belajar sendiri dan menghasilkan konten baru (*generative AI*). Oleh karena itu, penting adanya revisi atau pembentukan regulasi baru yang mendefinisikan AI secara komprehensif serta menetapkan batas-batas etis dan legal dalam pengembangannya..

Dengan demikian, konsep AI tidak hanya relevan secara teknologis, tetapi juga memiliki implikasi hukum yang mendesak untuk diakomodasi oleh sistem peraturan perundang-undangan. Tanpa regulasi yang jelas, kejahatan berbasis AI seperti *deepfake porn* akan semakin sulit ditindak, baik dalam aspek pembuktian, identifikasi pelaku, maupun perlindungan korban.

Cara Kerja Artificial Intelligence dalam Menghasilkan Deepfake Porn

Artificial Intelligence (AI) merupakan sistem cerdas buatan manusia yang didesain untuk meniru dan bahkan menyamai kemampuan kognitif manusia, seperti belajar, menganalisis data, menyelesaikan masalah, dan membuat keputusan secara mandiri. Dalam konteks *deepfake*, AI bekerja melalui teknologi *machine learning* dan *deep learning*, terutama dengan algoritma bernama Generative Adversarial Networks (GANs), yang memungkinkan penciptaan konten visual secara realistis namun sepenuhnya hasil rekayasa digital (Goodfellow, et al., 2014).

Sistem GAN terdiri atas dua komponen: generator dan discriminator. *Generator* bertugas menciptakan gambar atau video tiruan, sedangkan *discriminator* bertugas membedakan mana konten yang asli dan mana yang palsu. Kedua sistem ini berinteraksi dalam proses kompetisi yang konstan, sehingga menghasilkan peningkatan kualitas konten tiruan hingga sangat menyerupai bentuk asli (Rana, Nobi, Murali, & Sung, 2023). Dalam kasus *deepfake porn*, wajah seseorang (biasanya korban) ditempelkan secara digital pada tubuh dalam video pornografi, dengan sinkronisasi ekspresi dan gerak bibir yang presisi, sehingga tampak meyakinkan secara visual.

Kemampuan ini kemudian digunakan untuk tujuan-tujuan ilegal, termasuk produksi konten seksual tanpa persetujuan korban, yang merupakan bentuk kekerasan berbasis gender berbasis digital (KBGO). Menurut laporan dari *Deeprtrace Lab*, 96% dari seluruh

video *deepfake* yang beredar di internet mengandung konten pornografi, dan sebagian besar menargetkan perempuan sebagai korban utama (Ajder, Patrini, Cavalli, & Cullen, 2019).

Kecanggihan AI dalam menghasilkan *deepfake porn* menjadikannya tantangan serius dalam konteks hukum. Karena teknologi ini dapat memanipulasi realitas secara halus, maka muncul kesulitan dalam aspek pembuktian kejahatan, validasi identitas pelaku, serta penetapan unsur kesengajaan. Terlebih, perkembangan AI yang bersifat *open-source* memungkinkan siapa pun dengan literasi teknologi dasar untuk mengakses dan mengoperasikan perangkat lunak *deepfake*, sehingga potensi penyalahgunaannya sangat tinggi (Koopman, Rodriguez, & Geradts, The Detection of Deepfake Videos Using Convolutional Neural Networks, 2020).

Untuk itu, pemahaman terhadap cara kerja AI ini sangat krusial bagi sistem hukum agar mampu merumuskan regulasi yang akurat, tanggap teknologi, dan memberikan perlindungan hukum yang memadai bagi korban. Pendekatan ini juga sejalan dengan gagasan hukum progresif Satjipto Rahardjo, yang mendorong sistem hukum agar senantiasa mengikuti dinamika perubahan sosial dan teknologi untuk tetap relevan dalam menegakkan keadilan (Rahardjo, Ilmu Hukum: Paradigma Baru dan Dinamika Sosial, 2010).

Regulasi yang Mengatur Mengenai *Deepfake Porn*

Adapun peraturan perundang-undangan yang dapat dijadikan acuan penegakan hukum meskipun belum secara eksplisit mengatur mengenai *deepffake* adalah sebagai berikut:

1. Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana (“KUHP”)
2. Undang-Undang Nomor 44 Tahun 2008 tentang Pornografi, Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi (“UU Telekomunikasi”)
3. Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE)
4. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP)
5. Undang-Undang Nomor 44 Tahun 2008 tentang Pornografi dan Undang-Undang Nomor 12 Tahun 2022 tentang Tindak Pidana Kekerasan Seksual (UU TPKS).

3. METODE PENELITIAN

Dalam menyusun penelitian ini, metode penelitian yang digunakan adalah yuridis normatif. Pengumpulan data dalam penelitian hukum normatif dilakukan dengan cara studi pustaka berupa data sekunder sebagai bahan dasar untuk diteliti dengan cara mengadakan penelusuran terhadap peraturan-peraturan dan literatur lain berkaitan dengan permasalahan yang diteliti atau sering disebut sebagai penelitian hukum kepustakaan (Soekanto & Mahmudji, 2003). Penelitian hukum normatif merupakan jenis penelitian yang bersumber dari studi kepustakaan dengan memanfaatkan data sekunder sebagai bahan utamanya (Supranto, 2003). Secara umum, penelitian hukum normatif menggunakan beberapa pendekatan, antara lain pendekatan undang-undang (*statute approach*), pendekatan konseptual (*conceptual approach*), pendekatan historis (*historical approach*), pendekatan kasus (*case approach*), serta pendekatan perbandingan (*comparative approach*) (Diantha, 2016). Kelima pendekatan tersebut dapat dikombinasikan, sehingga dalam pelaksanaan penelitian yuridis normatif dimungkinkan untuk mengadopsi dua atau lebih pendekatan yang dianggap relevan. Dalam penelitian ini sendiri, digunakan pendekatan peraturan perundang-undangan serta pendekatan konseptual. Pendekatan perundang-undangan ditempuh melalui analisis terhadap berbagai peraturan dan regulasi yang berkaitan dengan permasalahan hukum yang menjadi fokus pembahasan (Peter & Marzuki, 2005). Penelitian ini akan fokus membahas permasalahan hukum yang berkaitan dengan upaya penegakan hukum terhadap kemunculan konten pornografi berbasis teknologi *deepfake*. Sementara itu, pendekatan konseptual diterapkan ketika peneliti tetap berfokus pada norma hukum yang sudah ada, terutama karena belum terdapat atau tidak ada peraturan hukum yang mengatur masalah yang sedang dianalisis (Peter & Marzuki, 2005). Dalam penelitian ini, terdapat kekosongan hukum terkait penegakan hukum dari *deepfake porn*, sehingga diperlukan pendekatan yang mengacu pada pemahaman teori dan konsep-konsep yang menjadi dasar penelitian ini.

4. HASIL DAN PEMBAHASAN

Tantangan Penegakan Hukum terhadap *Deepfake Porn*

Artificial Intelligence didesain dengan cara kerja dan sistem yang kompleks untuk mengerjakan tugas tertentu bermodalkan kemampuannya dalam meniru kemampuan otak dan penalaran manusia terutama dalam menganalisis data, menyelesaikan masalah, serta mengambil keputusan (Anshori, 2022). Sistem kerja tersebut yang menjadikan AI memiliki kemampuan di atas rata-rata dan sulit dibedakan dengan kemampuan manusia dalam menghasilkan suatu karya (Haida, 2024). Dengan demikian, *output* AI berbasis *deepfake*

adalah tantangan nyata bagi penegakan hukum di Indonesia mengingat *deepfake* yang berkembang saat ini merupakan hasil manipulasi dengan keterlibatan AI di dalamnya (Singarimbun, 2024). Marissa Koopman, Andrea Macarulla Rodriguez, dan Zeno Geradts berpendapat bahwa *deepfake* bekerja dengan algoritma yang dapat mengganti wajah seseorang dalam suatu video dengan wajah dari tokoh yang berbeda, sehingga menghasilkan video baru dengan bentuk yang *photorealistic* (Koopman, Rodriguez, & Geradts, Detection of Deepfake Video Manipulation. University of Amsterdam & Netherlands Forensic Institute, 2018).

Alih-alih digunakan sebagai terobosan di berbagai sektor, kerealistisan *deepfake* justru melahirkan kejahatan pornografi jenis baru yang dapat dimanfaatkan untuk tujuan tertentu. Awalnya, hanya ada kategori Kekerasan Berbasis Gender (KBG) terkait isu pornografi ini. Akan tetapi, kemunculan AI membuka pintu masuk untuk menambah kategori baru, seperti KBGO, Kekerasan Berbasis Gender Siber, atau Kekerasan terhadap Perempuan. Terlepas dari istilah yang berbeda, KBGO sebenarnya sama dengan KBG sebagaimana pengertian KBG menurut United Nations High Commissioner for Refugees, yaitu kekerasan langsung berbasis gender pada seseorang berdasarkan seks atau gender (Kusuma & Arum). Perbedaan di antara keduanya hanyalah keterlibatan teknologi AI dalam KBGO. Tindakan kekerasan tersebut harus dilakukan dengan tujuan atau niat untuk melecehkan korban berdasarkan jenis kelamin atau orientasi seksual (Kusuma & Arum). Apabila tidak ada niat seperti itu, maka dapat digolongkan sebagai kekerasan umum dalam konteks daring (Kusuma & Arum).

Kasus kejahatan *deepfake* di Indonesia yang semakin hari bertambah parah mengisyaratkan perlunya sebuah regulasi khusus. Kebutuhan ini menjadi keniscayaan mengingat *deepfake* belum mendapatkan tempat untuk diatur secara spesifik dan komprehensif dalam hukum positif Indonesia. Kejahatan *deepfake* seringkali dihubungkan dengan tindakan kriminal di dunia maya atau *cybercrime* karena melahirkan konten ilegal yang melanggar hukum meskipun terjadi di realitas baru dengan internet sebagai media komunikasinya. Untuk kejahatan siber seperti *deepfake* acuan utama yang mengakomodasi bentuk kejahatan tersebut seringkali dikaitkan pada beberapa peraturan seperti UU Telekomunikasi, UU ITE, UU PDP, dan UU TPKS. Misalnya dalam hal terjadi pencemaran nama baik atau penipuan identitas, rujukan peraturan yang sering digunakan adalah Pasal 32 ayat (1) UU ITE yang menjelaskan bahwa tindakan mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu informasi elektronik dan/atau dokumen elektronik milik orang lain atau milik publik merupakan perbuatan melawan hukum.

Selain UU ITE, terdapat UU PDP yang dapat dijadikan dasar hukum apabila terjadi penyalahgunaan informasi pribadi yang disebarluaskan oleh *deepfake*. Sebagai contoh, Pasal 68 UU PDP dapat menjerat pelaku kejahatan *deepfake* yang berusaha untuk memalsukan data pribadi untuk tujuan tertentu dengan merugikan orang lain. Lebih lanjut, menurut Pasal 14 ayat 1 UU TPKS, kekerasan seksual berbasis elektronik juga dapat terjadi apabila seseorang mentransmisikan Informasi atau dokumen elektronik bermuatan seksual tanpa meminta persetujuan dari penerima informasi tersebut. Pada Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana, penyebaran konten *deepfake* berhubungan dengan Pasal 407 yang mengatur tentang produksi konten dan penyebaran pornografi.

Mochtar Kusumaatmadja menyatakan bahwa tujuan hukum adalah untuk mencapai ketertiban dan keadilan dalam masyarakat. Hukum harus berfungsi sebagai alat utama untuk menjaga ketertiban sekaligus mendorong pembaharuan sehingga hukum perlu dikembangkan sedemikian rupa agar dapat memberikan ruang bagi perubahan dalam masyarakat (Kusumaatmadja, 2002). Selain itu, hukum menurut pandangan Satjipto Rahardjo dalam teori hukum progresif menjelaskan bahwa hukum bukan merupakan sesuatu yang bersifat final melainkan terus bergerak dan berkembang mengikuti dinamika masyarakat. Oleh karena itu, hukum perlu digali dengan upaya-upaya progresif untuk mencapai kebenaran dan keadilan (Rahardjo, Penegakan Hukum Progresif, 2010). Hal penting dalam hukum progresif adalah adanya pembaharuan hukum yang beradaptasi dengan perkembangan zaman dan dinamika masyarakat, sehingga hukum sebagai pedoman utama harus memiliki kemampuan beradaptasi. Berdasarkan hal tersebut, hukum seharusnya bersifat responsif terhadap keadaan dan kebutuhan masyarakat Indonesia.

Laju perkembangan teknologi yang tidak dapat diprediksi mengharuskan hukum untuk selangkah lebih maju guna memberi ruang nyaman bagi pengguna teknologi sekaligus menjadi tameng dampak perkembangan teknologi. Langkah tersebut perlu ditegakkan apabila berbicara tentang perkembangan *deepfake* yang semakin cepat dan tidak dapat diakomodasi lebih lanjut oleh hukum positif yang sekarang berlaku di Indonesia. Mengingat kejahatan *deepfake* diproduksi oleh kecerdasan buatan maka diperlukan peraturan baru di sektor *artificial intelligence* khususnya dalam hal pemanfaatan algoritma *deepfake*. Aturan baru ini akan menjadi kiblat yang mengatur dan menentukan pemanfaatan AI sekaligus mendefinisikan AI dalam tatanan hukum nasional. Selama ini, definisi AI masih dihubungkan dengan frasa agen elektronik yang dimuat dalam Pasal 1 Angka 8 UU ITE yang didefinisikan sebagai [...] *perangkat dari suatu sistem elektronik yang dibuat untuk melakukan suatu tindakan terhadap Informasi Elektronik tertentu secara otomatis yang diselenggarakan oleh orang*". Definisi

agen elektronik ini belum mewakili pengaturan AI yang tepat dan komprehensif karena belum mencantumkan definisi AI secara rinci dan belum memberikan penggolongan terkait tingkatan AI seperti apa yang aman untuk digunakan. Hal ini penting untuk diatur agar *developer* AI memiliki pondasi utama dalam mengembangkan teknologi yang mendahulukan etika manusia. Mewujudkan ini memang tidak mudah, tetapi wajib diatur agar memberi batasan yang jelas terkait pengembangan AI serta mencegah kemampuan tertentu AI yang dapat membahayakan manusia.

Lebih lanjut, regulasi juga dibutuhkan dalam proses penegakan hukum terutama pada pemeriksaan alat bukti. Pada proses pembuktian di pengadilan, pembuatan surat dakwaan oleh jaksa penuntut umum harus disertai dengan keabsahan alat bukti sesuai dengan ketentuan Pasal 183 KUHAP, sekurang-kurangnya berjumlah dua alat bukti dan disertai dengan keyakinan hakim (Harahap, 2014). Meskipun, KUHAP belum mengatur tentang alat bukti elektronik tetapi Pasal 5 ayat 2 UU ITE telah memperluas cakupan alat bukti dengan memasukkan informasi elektronik dan/atau dokumen elektronik dan/atau hasil cetaknya sebagai salah satu alat bukti dalam pembuktian perkara. Hal tersulit dalam proses ini adalah menentukan apakah alat bukti yang digunakan merupakan karya AI atau bukan. Dalam rangka mengkonkretkan hal tersebut, maka diperlukan suatu Peraturan Mahkamah Agung (PERMA) yang mewajibkan setiap alat bukti elektronik harus diperiksa terlebih dahulu di Laboratorium Forensik Polisi Republik Indonesia dengan dukungan teknologi canggih yang dapat mendeteksi hasil ciptaan AI untuk menentukan keaslian alat bukti yang diajukan dalam perkara.

Kemudian, dalam hal menemukan pelaku kejahatan yang keberadaannya sulit dilacak atau *IP-Adress*-nya telah dimanipulasi, dibutuhkan kerja sama penegakan hukum dengan negara lain atau dibuatkan suatu peraturan berskala internasional yang mengatur tentang penanganan pelaku kejahatan siber lintas negara khususnya pada jenis kejahatan berbasis *deepfake*. Peraturan internasional ini dapat mencakup keselarasan hukum nasional terkait standar etika penggunaan AI untuk tujuan tertentu, kerangka hukum yang sama, dan prosedur penyelidikan yang konsisten.

Pencegahan, Perlindungan, dan Edukasi Terkait Kejahatan *Deepfake Porn*

Fakta memperlihatkan bahwa regulasi terkait *deepfake porn* tidak akan optimal tanpa disertai pembuatan teknologi yang dapat mendeteksi *deepfake* itu sendiri. Inovasi teknologi ini menjadi krusial untuk mengimbangi laju algoritma *deepfake* yang semakin pesat dan tidak terkendali. Indonesia dapat bercermin kepada negara-negara yang terlebih dahulu berusaha menciptakan teknologi yang dapat mengalahkan *deepfake*. Sebagai contoh, Amerika Serikat sedang berupaya mengalahkan teknik otomatis dalam pembuatan *deepfake* dengan teknik

forensik sebagai pendeteksi (Stanton, 2019). Pendeteksi ini merupakan sebuah aplikasi yang dapat mendeteksi suatu video, foto, atau audio apakah hasil dari *deepfake* atau bukan, khususnya *deepfake porn*.

Inovasi tersebut akan menjadi kewenangan dari Kemenkomdigi yang dapat berkolaborasi dengan Kepolisian Negara Republik Indonesia (Polri) dan Komisi Nasional Anti Kekerasan terhadap Perempuan (Komnas Perempuan). Pada proses pembuatannya, Kemenkomdigi dapat melakukan kolaborasi, misalnya bersama perguruan tinggi di Indonesia, perusahaan, instansi, lembaga, atau badan hukum manapun untuk merealisasikan pembuatan aplikasi ini. Aplikasi ini juga harus melakukan kerja sama dengan berbagai *platform online* yang sering digunakan di Indonesia, seperti Twitter, Facebook, Instagram, TikTok, dan *platform* lainnya yang berpotensi menjadi media penyebaran *deepfake porn*. Kerja sama ini berguna untuk keperluan penghapusan konten *deepfake* serta pencegahan penyebarannya yang lebih luas. Masyarakat juga harus memperoleh kemudahan dalam mengakses aplikasi ini termasuk upaya preventif dan represif dalam menangani *deepfake porn*. Secara rinci, cara kerja dari aplikasi tersebut adalah sebagai berikut:

1. Pada halaman pertama aplikasi ini akan memerlukan pengisian beberapa data diri secara *multiple choice* untuk memudahkan para pengguna, yaitu:
 - a. Umur untuk mengidentifikasi apakah korban sudah dewasa atau masih anak-anak.
 - b. Objek dalam video, foto, atau audio tersebut apakah diri sendiri, diri sendiri dengan orang lain, atau orang lain.
 - c. Deskripsi video, foto, atau audio tersebut apakah kegiatan seksual atau non seksual.
 - d. Konfirmasi apakah video, foto, atau audio tersebut telah tersebar, belum tersebar, atau belum diketahui penyebarannya.
2. Pada halaman kedua akan menampilkan fitur untuk meng-*upload* video atau audio yang diduga sebagai *deepfake porn*. Kemudian, korban akan diminta melakukan *scanning* wajah dan suara melalui aplikasi ini untuk menjadi penguji apakah video atau audio yang di-*upload* termasuk *deepfake* atau bukan. Hasil pemindaian wajah dan suara ini juga tidak akan disimpan dalam aplikasi, melainkan hanya digunakan selama proses pendeteksian, setelahnya aplikasi akan secara otomatis menghapus data tersebut. Selanjutnya, melalui teknik *face recognition* aplikasi ini akan mendeteksi apakah video atau audio ini merupakan hasil *deepfake* atau bukan yang dibagi menjadi 3 (tiga) kategori, yaitu:

- a. *Non-deepfake*. Artinya, video atau audio yang di-*input* bukan merupakan hasil dari *deepfake*, sehingga aplikasi tidak melakukan tindak lanjut apapun.
 - b. *Deepfake*. Artinya, video atau audio yang di-*input* merupakan hasil *deepfake*. Akan tetapi, video atau audio tersebut tidak mengandung konten pornografi.
 - c. *Deepfake porn*. Artinya, video atau audio yang di-*input* merupakan hasil *deepfake* yang mengandung konten pornografi.
3. Pada halaman ketiga, aplikasi ini akan menampilkan sebuah *hash* atau *digital fingerprint* dari *deepfake* tersebut. Hal ini ditujukan untuk menghindari penyebaran lebih luas dari foto atau video tersebut serta tetap memprioritaskan perlindungan korban dari kemungkinan buruk yang dapat terjadi. Selanjutnya, aplikasi akan mencari kecocokan dari *hash* tersebut dan menghapusnya dari sistem media sosial yang terhubung dengan aplikasi ini. Berikutnya, aplikasi ini secara otomatis akan mencari *IP address* dari penyebar pertama kali video atau audio *deepfake* tersebut. Pelacakan *IP address* bertujuan menemukan detail lokasi dari pelaku penyebaran pertama kali untuk dapat dikenakan upaya penegakan hukum sesuai regulasi yang berlaku, baik lingkup nasional maupun internasional. Sekalipun ternyata pencipta video atau audio *deepfake* tersebut bukan orang yang sama dengan pelaku penyebaran pertama kali, penemuan lokasi ini akan sangat membantu arah gerak polisi untuk menemukan pelaku sebenarnya.
4. Pada halaman keempat, pengguna akan diminta memasukkan beberapa digit *Personal Identification Number* (PIN) untuk akses keamanan, sehingga yang dapat mengakses laporan tersebut hanyalah pemilik PIN. Akan tetapi, PIN ini tidak dapat dipulihkan apabila pemiliknya lupa karena dirancang untuk tidak disimpan dalam sistem aplikasi guna keamanan laporan. Maka dari itu, aplikasi akan menawarkan untuk mengirimkan salinan laporan melalui email tanpa harus menyimpan email sekalipun dalam sistem aplikasi, termasuk media sosial yang bekerja sama dengan aplikasi ini.
5. Pada halaman kelima, akan ditampilkan *review* dari laporan yang telah dibuat, beberapa konfirmasi persetujuan untuk keperluan pelaporan sebelum akhirnya dapat di-*submit*.
6. Setelah di-*submit*, halaman selanjutnya akan menampilkan nomor laporan yang juga harus diingat oleh pengguna untuk keperluan pengecekan status laporan. Apabila, laporan ini akan ditindaklanjuti, maka pada tampilan status laporan akan muncul arahan bagi pelapor untuk menghubungi kepolisian guna penindakan secara hukum terhadap kejahatan tersebut, baik melalui *restorative justice* maupun melalui pengadilan.

Sementara itu, di balik krusialnya regulasi yang komprehensif dan teknologi yang mutakhir dalam mengimbangi *deepfake*, terdapat fokus pemerintah dan masyarakat yang tidak kalah penting, yakni perlindungan dan pemulihan korban. Video, foto, atau audio hasil *deepfake* yang disebarluaskan sangat merugikan korban karena dapat menghasilkan stigma negatif dari masyarakat terhadap korban sekalipun konten tersebut adalah palsu. Tak hanya itu, *deepfake porn* juga dapat membuka jalan untuk terjadinya perundungan, baik secara *online* maupun *offline* yang akan mengganggu kesehatan psikis dan jasmani korban, misal kasus yang dialami wanita bernama Kate Isaacs (McDermott & Sarah, 2022) dan wanita pemilik akun QTCinderella di Platform Twitch (Ryu, 2023). Bahkan, di Indonesia terdapat kegiatan jual-beli barter konten *deepfake porn* (Asshafa, 2023). Hal ini dapat menimbulkan depresi, kilas balik, dan Post-Traumatic Stress Disorder yang sulit untuk dipulihkan (RAINN). Seperti halnya korban-korban KBG, korban KBGO juga membutuhkan perhatian khusus dan penanganan yang tepat karena korban ini juga merasakan trauma, ketidakpercayaan diri, kehilangan martabat, dan pandangan buruk dari lingkungan sekitar. Merujuk pada buku panduan tentang KBGO, berikut berbagai dampak yang mungkin dialami korban (Kusuma & Arum):

1. Dampak psikologis, yaitu korban merasakan depresi, kecemasan, dan perasaan takut. Pada tahap tertentu, korban bahkan merasa terdesak hingga berpikir untuk mengakhiri hidupnya.
2. Keterasingan sosial, yaitu korban mengasingkan diri dari keluarga dan lingkungan sekitar, khususnya wanita yang foto dan videonya disebarluaskan tanpa izin, sehingga korban merasa dikecam di depan umum.
3. Dampak ekonomi, yaitu korban dipecat dari tempat kerjanya, sehingga tidak memiliki pendapatan.
4. Terbatasnya ruang gerak, yaitu korban kurang mampu bergerak leluasa dan berkontribusi di ruang publik, baik secara daring maupun luring.
5. Sensor diri, yaitu akibat kekhawatiran akan menjadi korban dan lenyapnya rasa aman dalam memanfaatkan teknologi digital. Menjauhkan diri dari dunia maya memiliki dampak lanjutan misalnya membatasi diri dari informasi, pelayanan elektronik, dan komunikasi sosial atau profesional.

Banyak korban dari kasus kejahatan media maya mengalami depresi dan takut untuk melaporkan peristiwa kejahatan ke pihak berwenang. Fenomena yang ditemukan di masyarakat hampir semua korban takut melapor karena dianggap aib atau memalukan. Ini diperparah dengan peraturan di Indonesia yang cenderung bias karena beberapa pasal karet pada peraturan

perundang-undangnya, seperti UU ITE yang justru dapat menjerat korban. Maka dari itu, di samping diperlukan adanya teknologi pendeteksi, upaya perlindungan korban juga perlu melibatkan keterbukaan dan kenyamanan akses layanan hukum maupun layanan teknis yang berhubungan dengan perlindungan korban.

Selain upaya-upaya di atas, penanganan kejahatan *deepfake* tidak bisa terus-menerus berada di posisi mengobati, tetapi harus mampu meminimalisasi permasalahan. Cara terbaik untuk mewujudkan hal tersebut adalah mengedukasi masyarakat selaku subjek hukum yang bertanggung jawab atas terjadinya kejahatan tersebut. Masyarakat harus dihimbau untuk bijaksana dalam menggunakan teknologi dan meningkatkan kesadaran untuk lebih berhati-hati dalam memposting video, foto, atau audio di media manapun. Sosialisasi ini dapat dicanangkan dalam bentuk kampanye secara holistik dengan menggaet beberapa lembaga dan/atau instansi terkait seperti Komisi Nasional Hak Asasi Manusia Perempuan, kepolisian dan institusi pendidikan. Koordinasi antar institusi pendidikan perlu untuk bersama keluarga dan masyarakat mewujudkan lingkungan yang nyaman bagi anak-anak atau generasi muda untuk bijaksana dalam menggunakan teknologi.

Ironisnya, anak-anak pun dapat terkena imbas *deepfake* karena tergolong sebagai pengguna aktif berbagai *platform online*. Menurut data dari Kementerian Pemberdayaan Perempuan dan Perlindungan Anak, sebanyak 62,3% anak perempuan dan 66,6% anak laki-laki di Indonesia terpapar konten pornografi dari Internet (Kusuma & Arum). Selain itu, setidaknya masyarakat harus mengetahui cara membedakan antara video, foto, atau audio hasil manipulasi *deepfake* atau bukan. Sosialisasi juga dapat dilakukan melalui iklan di televisi, *platform online* yang sering digunakan masyarakat, *billboard* di jalanan, atau dapat melalui program di daerah atau sekolah yang disosialisasikan secara langsung kepada masyarakat, sehingga akan lebih intens dalam mencegah kejahatan *deepfake*.

5. KESIMPULAN DAN SARAN

Kesimpulan

Revolusi teknologi memiliki segudang manfaat di setiap sektor kehidupan manusia, seperti sektor sosial-budaya, sektor ekonomi, sektor pertahanan dan keamanan, sektor pemerintahan, dan masih luas lagi. Namun demikian, kemajuan ini disertai konsekuensi yang tidak dapat diabaikan, yaitu meningkatnya intensitas dan kompleksitas kejahatan digital. Di antara populernya kejahatan digital, salah satu yang kerap kali disoroti masyarakat adalah *deepfake*, khususnya *deepfake porn*. *Deepfake* mampu memunculkan hasil karya berupa duplikasi atau rekayasa yang memanfaatkan masukan dari data visual dan audio seseorang di

internet tanpa izin dari pihak yang bersangkutan. Teknologi seperti ini yang kemudian disalahgunakan untuk memproduksi konten pornografi hasil olahan *deepfake*. *Deepfake* sendiri terbagi menjadi 5 (lima) kategori utama, yaitu: *Attribute manipulation*, *entire face synthesis*, *lip-syncing*, *face reenactment*, dan *identity swap*. Merujuk pada tipe tersebut, *deepfake porn* termasuk *identity swap*, yaitu manipulasi identitas. Berbagai kasus yang terjadi dengan mayoritas korbannya adalah wanita menandakan bahwa sangat diperlukannya penegakan hukum yang akurat untuk mengatasi *deepfake porn*. Beberapa hal yang sangat krusial mengenai isu *deepfake porn* ini adalah belum adanya regulasi yang secara khusus mengatur mengenai AI (termasuk *deepfake porn*), kurang mutakhirnya teknologi yang tersedia untuk mendeteksi *deepfake* termasuk *deepfake porn*, kurang terfokusnya perlindungan dan pemulihan korban, dan edukasi yang masih kurang menyeluruh terhadap berbagai lapisan masyarakat.

Saran

Berdasarkan penelitian ini, penulis mengajukan beberapa saran: Pertama bagi pemerintah dalam menyikapi hal ini perlu melakukan aksi nyata, yaitu (1) Membuat regulasi khusus yang mengatur tentang AI yang mencakup sekurang-kurangnya tentang definisi, ruang lingkup, klasifikasi, sanksi, serta penegasan tentang status AI sebagai subjek hukum atau objek hukum. Selain itu, diperlukan juga peraturan lain, seperti PERMA bagi internal penegak hukum untuk mewajibkan adanya pemeriksaan alat bukti elektronik guna membedakan dan memastikan apakah alat bukti yang digunakan merupakan ciptaan AI atau bukan. Sifat AI yang *borderless* pun mengharuskan adanya kerjasama internasional untuk memetakan pelaku penyebaran *deepfake* dan penegakan hukumnya. (2) Diperlukan teknologi khusus yang dapat mendeteksi *deepfake*, termasuk *deepfake porn* dengan pengaturan yang memprioritaskan perlindungan dan kenyamanan korban. Selain mendeteksi, aplikasi ini juga sekaligus dapat melacak *IP address* dan membuat aduan untuk selanjutnya ditindaklanjuti oleh Polri. (3) Pemerintah juga harus membagi fokusnya terhadap perlindungan dan pemulihan korban karena banyaknya dampak negatif *deepfake porn* bagi korban. (4) Dibutuhkan edukasi kepada masyarakat secara menyeluruh sebagai upaya preventif untuk meminimalisasi *deepfake*, khususnya *deepfake porn*.

Selanjutnya bagi masyarakat, individu, orang tua dan anak harus sangat berhati-hati dalam menggunakan teknologi dan media sosial, terutama yang melibatkan data pribadi. Terutama untuk orang tua, sangat penting untuk memantau penggunaan teknologi atau media sosial oleh anak. Selain itu, masyarakat juga sebaiknya tidak langsung percaya begitu saja terhadap foto, video, dan/atau audio bermuatan pornografi sebelum terkonfirmasi kebenaran

dari objek tersebut. Kemudian, masyarakat juga harus bekerja sama saling menciptakan ruang aman agar membantu korban untuk berani berbicara dan melapor kepada pihak berwajib.

DAFTAR PUSTAKA

- Admin CSIRT Banten. (2022, July 20). RI dihantam 700 juta serangan siber di 2022 modus pemerasan dominan. *BantenProv-CSIRT*. <https://csirt.bantenprov.go.id/portal/articles/read/ri-dihantam-700-juta-serangan-siber-di-2022-modus-pemerasan-dominan>
- Ajder, H., Patrini, G., Cavalli, F., & Cullen, L. (2019). *The state of deepfakes: Landscape, threats and impact*. Deeptrace Lab.
- Anshori. (2022). Gagasan artificial intelligence dalam penerapan hukum di era 4.0 perspektif penyelesaian perkara model restorasi justice dan hukum progresif. *Legal Studies Journal*, 4(2). <https://doi.org/10.33650/lsj.v2i2.4190>
- Asosiasi Penyelenggara Jasa Internet Indonesia. (2025, March 12). Jumlah pengguna internet Indonesia tembus 221 juta orang. *APJII*. [https://apjii.or.id/berita/d/apjii-jumlah-pengguna-internet-indonesia-tembus-221-juta-orang#:~:text=Asosiasi%20Penyelenggara%20Jasa%20Internet%20Indonesia%20\(APJII\)%20mengumumkan%20jumlah%20pengguna%20internet,jiwa%20penduduk%20Indonesia%20tahun%202023](https://apjii.or.id/berita/d/apjii-jumlah-pengguna-internet-indonesia-tembus-221-juta-orang#:~:text=Asosiasi%20Penyelenggara%20Jasa%20Internet%20Indonesia%20(APJII)%20mengumumkan%20jumlah%20pengguna%20internet,jiwa%20penduduk%20Indonesia%20tahun%202023)
- Asshafa, S. (2023, June 30). Deepfake porn: Ketika AI jadi alat kejahatan seksual. *Akurat.co*. <https://www.akurat.co/infotech/1302419424/Deepfake-Porn-Ketika-AI-Jadi-Alat-Kejahatan-Seksual>
- Banke, R., & Gandrova, S. (2023). Penerapan positif Indonesia terhadap kasus kejahatan dunia maya deepfake. *Madani: Jurnal Ilmiah Multidisiplin*, 3(4), 651–660.
- DeRuvo, J., & McCormick, C. (2024, September 19). Furious 7: Which Brian O'Conner scenes weren't Paul Walker. *Screenrant*. <https://screenrant.com/furious-7-brian-scenes-not-paul-walker-brothers/>
- Diantha, I. (2016). *Metodologi penelitian hukum normatif dalam justifikasi teori hukum*. Kencana.
- Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Luetge, C., ... Vayena, E. (2018). AI4People—An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations. *Minds & Machines*, 28(4), 689–707. <https://doi.org/10.1007/s11023-018-9482-5>
- Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., ... Bengio, Y. (2014). Generative adversarial nets. *Advances in Neural Information Processing Systems*, 27.
- Haida, R. (2024). Urgensi pengaturan perlindungan hukum terhadap korban deepfake melalui artificial intelligence (AI) dari perspektif hukum pidana Indonesia. *Jurnal Respublica*, 2(1), 45–58.

- Harahap, M. (2014). *Pembahasan permasalahan dan penerapan KUHP penyidikan dan penuntutan*. Sinar Grafika.
- Kasita, I. (2022). Deepfake pornografi: Tren kekerasan gender berbasis online (KGBGO) di era pandemi Covid-19. *Jurnal Wanita dan Keluarga*, 2(1), 15–28. <https://doi.org/10.22146/jwk.5202>
- Koopman, M., Rodriguez, A., & Geradts, Z. (2018). Detection of deepfake video manipulation. *IMVIP*. University of Amsterdam & Netherlands Forensic Institute.
- Koopman, M., Rodriguez, A., & Geradts, Z. (2020). The detection of deepfake videos using convolutional neural networks. *Forensic Science International: Digital Investigation*.
- Kusuma, E., & Arum, N. (n.d.). *Memahami dan menyikapi kekerasan berbasis gender: Sebuah panduan*. SAFEnet.
- Kusumaatmadja, M. (2002). *Konsep-konsep hukum pembangunan*. Alumni.
- Maharani, A., Sabili, A., Septia, E., Magistravia, E., & Tobing, P. (2023, Desember 1). Deepfake artificial intelligence (AI): Metode baru dari wujud kekerasan berbasis gender online (KBGO). *Medium*. <https://medium.com>
- McDermott, S., & Sarah, J. (2022, Oktober 24). Mereka menggunakan wajah saya dalam video porno': Cerita aktivis perempuan menjadi korban 'deepfake'. *BBC News Indonesia*. <https://www.bbc.com/indonesia/articles/cg3lygdwj9zo>
- Mediana. (2023, November 6). Deepfake yang mencemaskan. *Kompas.id*. <https://www.kompas.id/baca/ekonomi/2023/11/05/deepfake-yang-mencemaskan>
- Naitali, A., Ridouani, M., Salahdine, F., & Kaabouch, N. (2023). Deepfake attacks: Generation, detection, datasets, challenges, and research direction. *Computers*, 12(10), 26. <https://doi.org/10.3390/computers12100216>
- Nistanto, R., & Hardiansyah, Z. (2022, Januari 19). Selebriti dan tokoh publik yang jadi korban video deepfake selain Nagita Slavina. *Kompas.com*. <https://tekno.kompas.com/read/2022/01/19/13160047/selebriti-dan-tokoh-publik-yang-jadi-korban-video-deepfake-selain-nagita?page=all>
- Pakpahan, R. (2021). Analisa pengaruh implementasi artificial intelligence dalam kehidupan manusia. *Journal of Information System*, 507.
- Pemerintah Indonesia. (2008). *Undang-undang Republik Indonesia nomor 11 tahun 2008 tentang informasi dan transaksi elektronik*. Kementerian Sekretariat Negara RI.
- Pertiwi, W., & Riyanto, G. (2022, Januari 18). Menilik teknologi "deepfake" di balik video diduga mirip Nagita Slavina. *Kompas.com*. <https://tekno.kompas.com/read/2022/01/18/15490077/menilik-teknologi-deepfake-di-balik-video-diduga-mirip-nagita-slavina?page=all>
- Peter, M., & Marzuki. (2005). *Metode penelitian hukum*. Mataram University Press.
- Rahardjo, S. (2010). *Ilmu hukum: Paradigma baru dan dinamika sosial*.

- Rahardjo, S. (2010). *Penegakan hukum progresif*. Kompas Media Nusantara.
- RAINN. (n.d.). Effects of sexual violence. RAINN. <https://www.rainn.org/effects-sexual-violence>
- Rana, M., Nobi, M., Murali, B., & Sung, A. (2023). Deepfake video detection: A systematic literature review. *ACM Computing Surveys*. <https://doi.org/10.1109/ACCESS.2022.3154404>
- Retno, A. (2024, Februari 5). Pekerja keuangan di Hong Kong kena tipu Rp 401 M, pelaku pakai deepfake. *detikFinance*. <https://finance.detik.com/berita-ekonomi-bisnis/d-7178019/pekerja-keuangan-di-hong-kong-kena-tipu-rp-401-m-pelaku-pakai-deepfake>
- Russel, S., & Norvig, P. (2021). *Artificial intelligence: A modern approach*. Pearson Education Limited.
- Ryu, J. (2023, Februari 14). She discovered a naked video of herself online, but it wasn't her: The trauma of deepfake porn. *USA Today*. <https://www.usatoday.com/story/life/health-wellness/2023/02/14/qtcinderella-deepfake-trauma-nonconsensual-porn/11222588002/>
- Sawitri, D., & Wacika, M. (2023). Peran teknologi dalam transformasi ketenagakerjaan: Analisis dampak dan tantangan di era digital. *Jurnal Kertha Wicara*, 88–101.
- Shravan, K., & Bhora, D. (2019). Demystifying the role of artificial intelligence in legal practice. *Nirma University Law Journal*, 7–8.
- Singarimbun, F. (2024). Implikasi hukum penggunaan AI dalam seni grafis terhadap hak kekayaan intelektual. *Jurnal Penelitian Pendidikan Indonesia*, 886–893. <https://doi.org/10.29210/020243889>
- Soekanto, S., & Mahmudji, S. (2003). *Penelitian hukum normatif: Suatu tinjauan singkat*. Jakarta: Rinneka Cipta.
- Soeprajitno, R. (2019). Potensi artificial intelligence (AI) menerbitkan opini auditor. *Jurnal Riset Akuntansi dan Bisnis Airlangga*, 4(1), 234. <https://doi.org/10.31093/jraba.v4i1.142>
- Stanton, C. (2019, Januari 28). How should countries tackle deepfakes? *Carnegie Endowment for International Peace*. <https://carnegieendowment-org.translate.goog/2019/01/28/how-should-countries-tackle-deepfakes-pub->
- Supranto, J. (2003). *Metode penelitian hukum statistik*. Jakarta: Rinneka Cipta.
- YahooFinance. (2024, Februari 22). More than 300 international experts release open letter demanding government leaders take immediate action to combat deepfake threats. *YahooFinance*.