

# IMPLIKASI HUKUM PENYALAHGUNAAN ARTIFICIAL INTELLIGENCE TERHADAP KEKERASAN SEKSUAL DEEPFAKE BERBASIS DIGITAL BERDASARKAN TEORI PERLINDUNGAN DATA PRIBADI

LEGAL IMPLICATIONS OF ARTIFICIAL INTELLIGENCE  
ABUSE FOR DIGITAL-BASED DEEPFAKE SEXUAL  
VIOLENCE BASED ON PERSONAL DATA PROTECTION  
THEORY

M. Fahmi Sidiq Hamdani<sup>1\*</sup>. M. Rifqy Hakim. Nabila Filfaberi. Revita Putri Sadewi.

<sup>1</sup>UIN Syarif Hidayatullah Jakarta

\*Korespondensi: E-Mail: [fhmalsafy@gmail.com](mailto:fhmalsafy@gmail.com)

DETAIL ARTIKEL	ABSTRACT
Vol. 1, No. 1 (2025) UIN Law Review Hal. 74-92.  Diajukan: 08-05-2025 Ditelaah: 13-05-2025 Direvisi: 20-05-2025 Diterbitkan: 30-06-2025  Handling editor:  <b>Key Words:</b> Artificial Intelligence; Deepfake; Foreign National; Human Rights.	<p><i>Indonesia as a country of law that places the constitution as the highest legal basis in the administration of the state and the constitution guarantees human rights in writing to every citizen, but nevertheless not a few Indonesian and foreign citizens use artificial intelligence (AI) and violate these fundamental values. This study aims to analyze and find out law enforcement to foreign nationals who abuse AI and the urgency of establishing a special law on AI abuse. This study uses a type of normative juridical legal research, the data processing process is carried out by data collection, data presentation, data analysis, ideas and conclusions. Law enforcement carried out by the government against foreigners is carried out in two ways: deportation and court. If the violation or crime committed by the foreigner is not too serious, the punishment given is in the form of administrative sanctions in the form of deportation, if the violation or crime committed by the foreigner is serious enough, the punishment given to the foreigner can lead to detention or fine. The urgency of forming a special law on the misuse of artificial intelligence is very important based on the findings of Sensity, where AI-based crimes are increasing every year and the impact of losses experienced by victims is very serious to the extent that it has an impact on the psychological and emotional of the victim.</i></p>
<b>Kata Kunci:</b> Slat bukti; DNA; Pembunuhan.	<p><b>ABSTRAK</b>            Indonesia sebagai negara hukum yang menempatkan konstitusi sebagai dasar</p>

# UIN Law Review

hukum tertinggi dalam penyelenggaraan negara dan konstitusi menjamin hak asasi manusia secara tertulis kepada setiap warga negara, namun demikian tidak sedikit warga negara Indonesia dan asing yang menggunakan kecerdasan buatan (AI) dan melanggar nilai-nilai fundamental tersebut. Penelitian ini bertujuan untuk menganalisis dan mengetahui penegakan hukum kepada warga negara asing yang menyalahgunakan AI dan urgensi pembentukan undang-undang khusus tentang penyalahgunaan AI. Penelitian ini menggunakan jenis penelitian hukum yuridis normatif, proses pengolahan data dilakukan dengan pengumpulan data, penyajian data, analisis data, gagasan dan kesimpulan. Penegakan hukum yang dilakukan pemerintah terhadap orang asing dilakukan dengan dua cara: deportasi dan pengadilan. Jika pelanggaran atau kejahatan yang dilakukan oleh orang asing tidak terlalu berat, maka hukuman yang diberikan berupa sanksi administratif berupa deportasi, jika pelanggaran atau kejahatan yang dilakukan oleh orang asing tersebut cukup berat, maka hukuman yang diberikan kepada orang asing tersebut dapat berujung pada penahanan atau denda. Urgensi pembentukan undang-undang khusus tentang penyalahgunaan kecerdasan buatan sangat penting berdasarkan temuan Sensity, dimana kejahatan berbasis AI meningkat setiap tahunnya dan dampak kerugian yang dialami korban sangat serius sampai-sampai berdampak pada psikologis dan emosional korban.

## 1. PENDAHULUAN

Sejak awal, istilah manusia dan hak asasi manusia telah dikaitkan erat karena keduanya merujuk pada hak-hak dasar manusia. Menurut filsafat John Locke, semua manusia memiliki hak alamiah yang tidak dapat dibatalkan, termasuk hak untuk hidup, kebebasan, dan kepemilikan. Negara tidak memiliki kewenangan atas ketiga hal ini, karena Pemahaman filosofis menekankan hak-hak tersebut bersifat melekat, tidak dapat dicabut dan harus dilindungi oleh negara dan dihormati sesama individu. Hak Asasi Manusia (HAM) adalah hak universal yang dimiliki

semua orang di seluruh dunia, tanpa memandang ras, agama, suku, atau kewarganegaraan<sup>1</sup>. Mereka tidak dapat diambil alih dan bersifat universal.

Indonesia sebagai negara yang memegang teguh HAM telah mengamanahkan dalam Pasal 28D Undang Undang Dasar Negara Republik Indonesia Tahun 1945 (UUD NRI Tahun 1945) secara gamblang menyebutkan bahwa : "setiap orang berhak atas pengakuan, jaminan, perlindungan, dan kepastian hukum yang adil serta perlakuan yang sama di mata hukum.". Setiap privasi seseorang baik di dunia Maya ataupun secara lahiriah tetap berhak untuk dilindungi serta mendapatkan keadilan oleh negara & hukum seperti mencerminkan apa yang ada pada sila ke-5 Pancasila.

Salah satu prinsip utama Pasal 12 Deklarasi Universal Hak Asasi Manusia (DUHAM) hak atas privasi dan perlindungan data pribadi, menyatakan bahwa "tidak boleh ada campur tangan sewenang-wenang terhadap privasi atau komunikasi siapapun." Di balik konsep ini terdapat masalah hak asasi manusia yaitu hak atas privasi dan perlindungan data pribadi. Hak atas privasi tidak disebutkan secara tegas dalam pasal ini. Hal itu dapat dimasukkan sebagai bagian dari hak atas perlindungan hukum yang adil dan kepastian hukum juga dapat diartikan. Setiap orang berhak atas kerahasiaan data pribadinya. Oleh karena itu, negara memiliki kewajiban untuk melindungi privasi semua individu, baik dalam kehidupan sehari-hari maupun di ruang digital. Ada kemajuan berkelanjutan dalam kecerdasan buatan.

Kecerdasan buatan atau Artificial Intelligence (AI) adalah bidang ilmu yang berhubungan dengan penciptaan sistem komputer yang dapat melakukan tugas-tugas yang biasanya memerlukan kecerdasan manusia. Menurut John McCarthy seorang pelopor AI, kecerdasan buatan adalah proses menciptakan mesin cerdas melalui prinsip-prinsip rekayasa. Tujuan utama pengembangan AI mencakup peningkatan efisiensi operasional, penghematan proses, dan membantu teknologi memecahkan masalah yang kompleks. Selain manfaatnya, AI juga membawa tantangan baru, terutama terkait perlindungan dan keamanan data.

Salah satu bentuk kejahatan dan penyalahgunaan AI yang paling umum adalah deepfake. Deepfake adalah teknik manipulasi media digital yang menggunakan algoritma AI seperti Generative Adversarial Networks (GAN) untuk membuat berkas video dan audio palsu yang tampak realistik. Deepfake sering digunakan untuk menyebarkan informasi palsu, melakukan penipuan, dan Kekerasan Gender Berbasis Online (KGBO). Teknologi ini telah digunakan untuk membuat materi pornografi tanpa persetujuan individu yang bersangkutan, yang tidak hanya melanggar privasi tetapi juga dapat merusak reputasi korban hingga mengakibatkan trauma psikologis dan konsekuensi sosial yang signifikan<sup>2</sup>.

<sup>1</sup> John Locke, *Two Treatises of Government*, ed. Peter Laslett (Cambridge: Cambridge University Press, 1988).

<sup>2</sup> VIDA, "Deepfake AI: Jenis, Risiko, Dan Solusi Untuk Menghadapinya," vida.id, n.d., <https://vida.id/id/blog/deepfake-ai>.

Hal ini menciptakan perlombaan teknologi antara pihak yang mencoba melindungi sistem dan pihak yang berusaha merusaknya. Data pribadi, seperti foto atau video yang diunggah ke media sosial, seringkali menjadi sumber bagi pelaku untuk membuat konten deepfake. Penyalahgunaan data ini menunjukkan betapa rentannya informasi pribadi di era digital, terutama ketika digunakan untuk tujuan yang merugikan.

Penyalahgunaan tersebut semakin membuat cemas dengan temuan Sensity, sebuah perusahaan yang meneliti deepfake dan ancamannya, yang pada bulan Desember 2020 mendeteksi sekitar 85.000 video palsu beredar, dan sebanyak 96% dari video yang beredar adalah konten pornografi deepfake<sup>3</sup>. Hal ini menunjukkan betapa rentannya teknologi terhadap penyalahgunaan untuk kepentingan eksploitasi. Dampak langsung yang diberikan dari maraknya fenomena ini adalah ancaman terhadap reputasi dan nama baik seseorang, karena deepfake dapat digunakan untuk menciptakan konten palsu yang mencemarkan kehormatan dan citra mereka. Meskipun demikian, para ahli menetapkan kehormatan dan nama baik seseorang harus berada dalam perlindungan hukum.

Rekayasa foto atau video yang dihasilkan deepfake dan disebarluaskan kepada khalayak publik, mengubah pandangan masyarakat tentang diri korban. Tindakan tersebut dapat mengundang bullying dan perundungan, sehingga korban dapat menderita secara psikologis dan emosional. Hal tersebut bukan sesuatu yang mudah untuk dipulihkan. Oleh karena itu, korban deepfake harus mendapatkan perlakuan khusus dalam penanganannya, karena korban akibat kekerasan tersebut dapat mengalami trauma, kehilangan harga diri, perendahan martabat dan berbagai bentuk stigma masyarakat yang tidak mendukung untuk mendapatkan keadilan bagi korban.

Berkenaan dengan maraknya ancaman yang ditimbulkan oleh Deepfake, hasil riset VIDA Penyelenggara Sertifikat Elektronik (PSrE) telah menemukan peningkatan yang signifikan terkait penyalahgunaan deepfake. VIDA Mengungkapkan peningkatan tersebut mencapai 1540% dari tahun 2022 hingga 2023. Besarnya persentase mencerminkan maraknya penyalahgunaan teknologi dengan berbagai macam modus kejahatan digital. Salah satu contohnya, contohnya kasus deepfake pada Nagita Slavina seorang selebritis Tanah Air<sup>4</sup> Rekayasa video berdurasi 61 detik itu mempertontonkan tindakan tidak senonoh. Kemudian kasus serupa juga terjadi pada siswi SMP, sebanyak 16 siswi SMP di Malang dan sekelompok perempuan sebanyak 17 orang yang terdiri dari teman dekat dan mantan kekasih pelaku, menjadi korban penyebaran Deepfake foto. Diri mereka dibuat menjadi tidak pantas dan disebar tanpa ada izin dari korban terkait. Kedua

<sup>3</sup> A S Putri, S Noerdajasakti, and F Sulistio, "RTBF as an Effort to Establish Legal Protection for Victims of Deepfake Pornography in Indonesia," *International Journal of Social Science and Human Research* 6, no. 6 (2023).

<sup>4</sup> "Pengaturan Hukum Teknologi Deepfake Di Indonesia – ALO," alchemistgroup.co, 2024, <https://alchemistgroup.co/pengaturan-hukum-teknologi-deepfake-di-indonesia/>.

kasus tersebut menggambarkan bahayanya penyalahgunaan teknologi deepfake dalam merugikan korban.

Terjadinya peningkatan kasus kejahatan kekerasan seksual deepfake di Indonesia tentunya suatu ancaman bagi perlindungan setiap warga Indonesia. Kejahatan deepfake yang merupakan kejahatan berbasis digital ini pun tentunya menimbulkan kerugian di berbagai aspek. Hal ini menimbulkan urgensi terhadap suatu regulasi yang memadai dan solutif untuk menjadi payung hukum bagi penegak hukum dalam menyelesaikan serta melindungi korban dari ancaman kasus deepfake. Kita ketahui bersama kejahatan digital akan menyebar luas dan sulit untuk dihentikan. Upaya yang dapat dilakukan pemerintah dengan pemblokiran situs pun tidak akan cukup, maka pertanggungjawaban oleh pelaku deepfake baik warga negara indonesia maupun asing mesti sepadan dan dapat mengurangi kerugian yang ditimbulkan kepada korban.

Kejahatan berbasis digital dalam kekerasan seksual deepfake saat ini belum ada regulasi yang mengatur secara rinci dan khusus akan karakteristik delik, dan perlindungan bagi korban mengenai deepfake. hal ini tidak menjadi alasan hukum untuk tidak memberikan tindakan. Upaya pemerintah untuk merespon penyalahgunaan teknologi deepfake yang merupakan bagian dari AI hanya berupa regulasi yang mengatur sanksi kejahatan digital secara umum dalam KUHP pada Buku kedua tentang kejahatan dimana menyebutkan penyebaran konten atau gambar yang melanggar kesusilaan pelaku dapat dijerat pada pasal 282 KUHP dengan denda dan sanksi yaitu penjara paling lama sembilan bulan dan denda hanya empat ribu lima ratus rupiah. Hal ini menjelaskan bahwa sanksi yang dijatuhan kepada pelaku terlalu ringan dibanding dengan kerugian korban yang menderita secara fisik, mental juga financial. Sedangkan dalam kasus deepfake sebagai tindak pidana pencemaran nama baik seharusnya juga memiliki aturan khusus tersendiri selain dari pada pedoman hukum oleh penegak hukum dengan menggunakan KUHP. Apalagi kejahatan deepfake yang memanipulasi wajah korban dengan postur tubuh orang lain dengan gambar yang tak pantas. Pemerintah diharapkan lebih memperkuat regulasi terkait perlindungan data pribadi, penanganan, dan pemulihan korban kekerasan gender akibat deepfake pornografi.

Selain itu dalam Undang-Undang Nomor 1 Tahun 2024 Tentang Informasi dan Transaksi Elektronik (UU ITE) pada pasal 27 ayat 1 menyebutkan seseorang yang menyebarkan informasi/dokumen elektronik yang memiliki muatan yang melanggar kesusilaan dapat dikenakan pidana berdasarkan UU ITE. Pasal ini menjelaskan bahwa melanggar kesusilaan yang dimaksud adalah melakukan perbuatan mempertunjukkan ketelanjangan, alat kelamin, dan aktivitas seksual yang bertentangan dengan nilai-nilai yang hidup dalam masyarakat di tempat dan waktu perbuatan tersebut dilakukan. Penafsiran dari pengertian kesusilaan disesuaikan dengan standar yang berlaku pada masyarakat dalam waktu dan tempat tertentu (contemporary community standard). Kemudian dilanjutkan pada pasal 45 ayat 1 UU ITE menyatakan bahwa pelaku penyebar informasi yang

melanggar kesesilaan diberat dengan hukuman pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah)<sup>5</sup>.

Instrumen yang memungkinkan dapat digunakan sama halnya dengan UU-ITE adalah Undang-Undang Perlindungan Data Pribadi (UU-PDP). Lebih tepatnya pada pasal 66 UU- PDP menyatakan bahwa: "Setiap orang dilarang membuat Data Pribadi palsu atau memalsukan Data Pribadi dengan tujuan untuk menguntungkan diri sendiri atau orang lain yang dapat merugikan pihak lain.". Termasuk dari data pribadi yang dimaksud dalam peraturan demikian adalah kehidupan seks seseorang. Teknik manipulasi visual dari Artificial Intelligence mencitrakan seolah-olah korban melakukan kegiatan seks yang sebenarnya tidak pernah terjadi. Pelaku menggunakan visual baik berupa foto atau video biasanya digunakan oleh pelaku untuk diperjualbelikan dalam saluran media sosial tertentu yang tertutup. Frasa kerugian dalam pasal 66 tersebut mencakup kerugian bersifat materil maupun immateril, termasuk psikis korban.

Tanggung jawab pelaku kekerasan seksual deepfake tidak berhenti setelah dipidana oleh majelis hakim, pelaku berkewajiban mempertanggungjawabkan jejak digital yang tersebar di dunia maya. Penghapusan jejak digital dari korban deepfake diatur dalam Permen Kominfo Nomor 5 Tahun 2020. Pengguna Sistem Elektronik dalam hal ini adalah pelaku pembuatan manipulasi visual dari deepfake berkewajiban untuk memutus segala akses terhadap konten yang telah disebarluaskan. Bukan hanya kontennya, segala fasilitas yang dapat mengantarkan kepada konten tersebut termasuk kewajiban pelaku. Jika konten deepfake berada dalam suatu saluran media sosial, maka saluran tersebut turut dihapus. Langkah ini dilakukan sebagai upaya represif pelaku kekerasan seksual berbasis deepfake. Peraturan tersebut merupakan turunan dari Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Hingga saat ini belum ada peraturan komprehensif yang mengumpulkan poin-poin yang ada dalam UU-ITE dan UU-PDP sebagai satu kesatuan.

Berdasarkan problematika tersebut, terlihat bahwa perlindungan data pribadi seseorang dari kejahatan deepfake merupakan hak bagi semua orang yang harus dilindungi oleh negara sebagai bentuk dari perlindungan HAM. Oleh karena itu menjadi suatu urgensi bagi pemerintah untuk mencari solusi yang efektif demi penyelesaian kasus Deepfake. Merujuk pada pemaparan latar belakang masalah di atas, sehingga dapat ditarik dua rumusan masalah yang dapat dikaji dalam penelitian ini, yaitu bagaimana pertanggungjawaban hukum bagi pelaku WNA terhadap pemulihian hak korban dalam kasus pornografi Deepfake dan mengapa urgensi pembentukan regulasi khusus terkait KBGO dalam kasus Deepfake? Maka pembahasan terkait problematika kejahatan digital deepfake perlu dibahas lebih komprehensif bagaimana implikasi hukum di indonesia untuk menangani kasus deepfake terlebih pelaku seorang WNA dengan gagasan pembentukan Deepshield system serta pembentukan UU khusus deepfake dengan judul "Implikasi Hukum

<sup>5</sup> R C Auli and S.H., "Bunyi Pasal 27 Ayat (1) UU ITE 2024 Tentang Kesesilaan," hukumonline.com, 2024, <https://www.hukumonline.com/klinik/a/bunyi->.

Penyalahgunaan Artificial Intelligence terhadap Kekerasan Seksual Deepfake Berbasis Digital berdasarkan Teori Perlindungan Data Pribadi.

## 2. METODE PENELITIAN

Penelitian ini menggunakan tipe penelitian hukum normatif. Jenis penelitian yang dipergunakan yaitu jenis penelitian yuridis normatif, Yang dimaksud dengan jenis penelitian hukum normatif adalah Suatu proses untuk menemukan suatu aturan hukum, prinsip prinsip hukum, maupun doktrin-doktrin hukum untuk menjawab permasalahan hukum yang dihadapi. Penelitian hukum normatif dilakukan untuk menghasilkan argumentasi, teori atau konsep baru sebagai preskripsi dalam menyelesaikan masalah yang dihadapi Penelitian ini melalui pendekatan undang-undang (statute approach), kasus (case approach), dan Historis (Historical Approach)<sup>6</sup>.

Adapun yang dengan data sekunder terdiri dari : a) bahan hukum primer, yaitu bahan- bahan hukum yang mengikat seperti Pasal 28D Undang Undang Dasar Negara Republik Indonesia Tahun 1945 (UUD NRI Tahun 1945), pasal 282 KUHP, UU Nomor 1 Tahun 2024 tentang Perubahan Atas Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE), pasal 66 Undang-Undang Perlindungan Data Pribadi (UU- PDP), Permen Kominfo Nomor 5 Tahun 2020, dan Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik ; b) bahan hukum sekunder, yaitu bahan-bahan hukum yang memberikan penjelasan terhadap bahan hukum primer, seperti doktrin, karya-karya ilmiah para sarjana, jurnal, dan tulisan-tulisan lain yang bersifat ilmiah. Penelitian terhadap bahan hukum sekunder ini dimaksudkan untuk menganalisis dan memahami bahan hukum primer, dan c) bahan hukum tersier, yaitu bahan-bahan hukum yang memberikan petunjuk maupun penjelasan terhadap bahan hukum primer dan bahan hukum sekunder<sup>7</sup>. Contohnya data internet yang berkaitan dengan masalah dalam tulisan ini.

## 3. HASIL DAN PEMBAHASAN

### 3.1. Pertanggungjawaban hukum bagi pelaku WNA terhadap pemulihan hak korban dalam kasus pornografi Deepfake

Kata 'Porno' atau 'Pornografi' sudah tidak terdengar asing bagi Masyarakat Indonesia dengan stigma negative karena suatu hal yang berkaitan dengan seks. Kata pornografi berasal dari Bahasa Yunani yang memiliki arti penggambaran tubuh manusia atau perilaku seksualitas manusia secara terbuka (eksplisit) dengan tujuan membangkitkan birahi (gairah seksual) atau biasa kita sebut zina dan kata grafe yang artinya kitab suci atau tulisan. Jenis-jenis pornografi tersebut berupa tulisan (Majalah, buku, dan lainnya), produk elektronik (DVD, VCD, kaset video, dan

<sup>6</sup> Soerjono Soekanto and Sri Mamudji, *Penelitian Hukum Normatif: Suatu Tinjauan Singkat* (Jakarta: RajaGrafindo Persada, 2003).

<sup>7</sup> R.S.K.U.H.P. Grafika, *Kitab Undang-Undang Hukum Pidana Undang-Undang RI Nomor 1 Tahun 2023* (Jakarta: Sinar Grafika, 2023).

lainnya), gambar-gambar bergerak, program TV atau TV Kabel, cyber-porno melalui internet, dan audio-porno yang melalui telepon. Selain itu, kemudahan mengakses pornografi dapat mencontoh aktivitas seksual sesuai dengan apa yang telah ditontonnya. inilah penyebab banyaknya dampak negatif yang akan timbul dari pornografi salah satunya ialah kekerasan seksual

Menurut Besar Bahasa Indonesia (KBBI) mengartikan bahwa 'Kekerasan' adalah perbuatan seseorang atau kelompok orang yang menyebabkan cedera atau matinya orang lain atau menyebabkan kerusakan fisik atau barang orang lain. sedangkan 'seksual' adalah segala sesuatu yang berhubungan dengan alat reproduksi, jenis kelamin, serta persetubuhan antara laki-laki dan perempuan. Jika didefinisikan 'Kekerasan

'Seksual' adalah setiap tindakan seksual, usaha melakukan tindakan seksual, komentar atau menyarankan untuk berperilaku seksual yang tidak disengaja ataupun sebaliknya, tindakan pelanggaran untuk melakukan hubungan seksual dengan paksaan kepada seseorang. Secara luas Kekerasan Seksual telah dikategorikan yang diurai dalam klasifikasi internasional tentang kekerasan dikategorikan menjadi dua jenis, yaitu Kekerasan Seksual Kontak dan Kekerasan Seksual Non-Kontak.

Kekerasan seksual non-kontak termasuk dalam Kejahatan Cyber atau Kejahatan dunia maya (cybercrime) adalah istilah yang merujuk kepada aktivitas kejahatan dengan komputer atau jaringan komputer menjadi alat, sasaran atau tempat terjadinya kejahatan. Zaman sekarang cyber porno yang berkembang secara pesat dan kuat, oleh karena itu dibutuhkan kolaborasi antara pemerintah dan Masyarakat untuk mengurangi dan memberantas adanya konten pornografi untuk memberantas kekerasan seksual berbasis digital dan memberantas adanya Tindakan Pidana Pornografi. Tentunya pemerintah harus menertibkan dan memperketat lagi apa yang seharusnya sesuai dengan hukum.

Penegakan hukum di Indonesia menghadapi kejahatan fisik dan kejahatan terkait digital yang dikenal sebagai cybercrime. Kejahatan fisik tampaknya jauh lebih mudah. Kebanyakan orang tahu apa yang harus dilakukan karena kejahatan fisik terjamin bertanggung jawab dan memberikan ketegasan sekejap apa yang telah terjadi, entah itu pencurian atau kekerasan. Namun, cybercrime adalah kasus yang berbeda karena merupakan jenis kejahatan abstrak dan bisa diketahui perkembangannya dengan cara yang membahayakan identitas orang yang suka luka. Kejahatan ini sulit ditindak oleh prinsip-prinsip keadilan distributif, yang berarti bahwa kita sosialisasi banyak kecakapan bahwa hukum harus ia susun dan melindungi kita dari kejah. Posisinya di mana aspeknya banyak orang yang perlu disayangkan. ini adalah ketidakberhasilan komit risti, tapi juga merupakan titik kunci bahwa hukum tak hanya membantu orang tidak hanya masalah yang lalu, dan sehingga membantu dengan masalah digital.

Cybercrime telah menjadi tantangan signifikan dalam penegakan hukum pidana di Indonesia, salah satu pendekatan yang dapat digunakan adalah hukum progresif.

Menurut Satjipto Rahardjo, seorang pakar hukum progresif, hukum tidak semestinya bersifat kaku dan harus mampu beradaptasi dengan perkembangan masyarakat, termasuk dalam ranah teknologi informasi. Hukum progresif menekankan pentingnya keadilan sosial dan perlindungan terhadap hak asasi manusia, yang sangat relevan dalam konteks kejahatan siber yang semakin marak. penegakan hukum pidana harus mampu merespons dinamika ini dengan inovasi hukum yang lebih adaptif. Hukum pidana tradisional sering kali tidak cukup untuk mengatasi kompleksitas kejahatan siber, sehingga diperlukan pendekatan progresif yang memadukan peraturan hukum baru dengan pemahaman konteks sosial. terkait dengan pertanggungjawaban pelaku kejahatan siber, penting untuk mengaitkannya dengan hak perlindungan korban.

Dalam kasus kejahatan cyber, seringkali korban mengalami kerugian yang signifikan, baik secara material maupun psikologis. Menurut Sri Puguh Budi Utami, perlindungan kepada korban harus menjadi perhatian utama dalam penegakan hukum, terutama karena banyak korban kejahatan siber merasa tidak memiliki akses kepada keadilan. Dengan hukum progresif, diharapkan ada upaya lebih besar untuk melindungi hak-hak korban dan memberikan mereka pemulihan yang layak. Sebagai contoh, dalam kejahatan penipuan online, pelaku seringkali berusaha menyembunyikan identitas mereka, sehingga penegakan hukum menjadi sulit. Namun, dengan memanfaatkan teknologi dan pendekatan hukum yang inovatif, aparat penegak hukum dapat lebih efektif dalam menciptakan akuntabilitas untuk pelaku kejahatan siber<sup>8</sup>. Penerapan hukum progresif ini juga mendorong kolaborasi antara lembaga penegak hukum dan masyarakat, untuk menciptakan lingkungan yang lebih aman.

Tantangan yang dihadapi oleh penegakan hukum pidana di era digital membutuhkan pemikiran yang progresif. Hukum harus dapat menghormati hak-hak korban dan memastikan pertanggungjawaban pelaku kejahatan siber. Pendekatan hukum yang adaptif dan progresif menjadi kunci untuk menghadapi tantangan ini, sehingga sistem hukum Indonesia dapat lebih responsif terhadap kejahatan yang terus berkembang di dunia maya. Berdasarkan teori keadilan John Rawls memberikan kerangka penting dalam memahami kesenjangan antara pelaku dan korban crime. Menurut Rawls, prinsip keadilan memerlukan bahwa struktur masyarakat harus memperhatikan posisi mereka yang kurang beruntung, termasuk korban kejahatan. Dalam konteks ini, perlunya penegakan hukum yang adil dan perlindungan atas hak-hak korban menjadi sangat krusial. Kesenjangan ini seringkali terjadi ketika sistem hukum lebih berfokus pada pelaku ketimbang memberikan keadilan kepada korban, sehingga fungsi rehabilitatif dan restitusi terhadap korban sering terabaikan.

Mengenai perlindungan data pribadi, terdapat hubungan erat dengan hak asasi manusia (HAM). UU Perlindungan Data Pribadi di Indonesia, yang mengatur bagaimana data pribadi harus dilindungi, sejalan dengan prinsip-prinsip HAM yang

<sup>8</sup> Sri Puguh Budi Utami, *Perlindungan Korban Kejahatan Dalam Perspektif Hukum Progresif* (Jakarta: Prenadamedia Group, 2020).

mengutamakan hak atas privasi dan perlindungan informasi pribadi. Hal ini penting dalam era digital saat ini, di mana data pribadi seringkali disalahgunakan, membawa dampak negatif bagi individu. Dalam hal ini, keadilan tidak hanya harus diterapkan pada pelaku dan korban kejahatan, tetapi juga dalam perlindungan terhadap data pribadi, yang merupakan aspek fundamental dari martabat manusia.

Indonesia merupakan negara yang memiliki kekayaan alam dan ketertarikan terhadap negara asing, menimbulkan banyak kedatangan warga negara asing. Kedudukan Warga Negara Asing (WNA) dalam penegakan hukum di Indonesia merupakan isu yang kompleks. WNA sering kali menghadapi tantangan yang berbeda dibandingkan dengan warga negara Indonesia, karena berpotensi menghadapi diskriminasi, baik dalam proses hukum maupun perlindungan hak-hak mereka. Dalam konteks keadilan, penting untuk memastikan bahwa WNA juga diberikan hak yang setara dalam sistem hukum, sehingga kesenjangan antara pelaku dan korban dapat diminimalisir, termasuk ketika pelakunya adalah WNA yang beraksi di tanah air. Kedudukan WNA di Indonesia sangat bergantung pada status mereka, misalnya sebagai pekerja, turis, atau pemegang izin tinggal. Mereka mempunyai hak untuk dilindungi dari tindakan sewenang-wenang dan diskriminasi dalam proses hukum, namun pada saat yang sama, mereka juga dibatasi oleh hukum Indonesia. Artinya, jika mereka melanggar hukum, mereka dapat dikenakan sanksi dan peraturan yang berlaku di negara ini. Kedudukan ini menunjukkan bahwa Indonesia mengakui hak WNA, tetapi juga menegaskan bahwa mereka harus mematuhi hukum lokal yang berlaku.

## UIN Law Review

Kementerian Imigrasi dan Pemasyarakatan mencatat adanya peningkatan deportasi Warga Negara Asing (WNA). Sebanyak 1.503 Warga Negara Asing (WNA) telah dideportasi oleh Ditjen Imigrasi pada tahun 2024. Angka tersebut mengalami peningkatan dibandingkan tahun 2023 sebanyak 1.165 yang dideportasi, jumlah ini meningkat sebesar 135,21%. Adapun Tujuan dari adanya deportasi menurut undang-undang No. 6 tahun 2011 yaitu untuk memulangkan warga negara asing ke negara asalnya sebagai upaya penegakan hukum terhadap warga negara asing tersebut. Warga negara asing yang dipulangkan ke negara asalnya disebabkan adanya kegiatan yang membahayakan keamanan dan ketertiban negara yang dilakukan oleh warga negara asing tersebut sehingga menjadikannya dipulangkan dengan tidak hormat. Salah satu kasus yang menyumbang peningkatan tersebut terjadi pada tanggal 28 Mei 2024 di sebuah penginapan wilayah kuta, seksi intelijen dan penindakan keimigrasian Bali mengamankan 3 WNA asal Nigeria. Berdasarkan hasil pemeriksaan ketiga WNA tersebut, dilakukan pengembangan dan terungkap 19 WN Nigeria, 1 WN Ghana dan 1 WN Tanzania. KANWIL KEMENKUM Bali menjelaskan para WNA tersebut melanggar izin tinggal keimigrasian dan 7 lainnya tidak dapat menunjukkan paspor. Dari total 24 WNA yang diamankan, 7 WNA dideportasi, 9 WNA dialihkan ke Rumah Detensi Imigrasi dan 8 WNA lainnya dilakukan prokostisasi.

Berdasarkan hal ini, menjadi sebuah tantangan bagi pemerintah ketika pelaku berada di luar wilayah Indonesia tapi melancarkan kejahatan di Indonesia, seperti

kasus kejahatan cybercrime dan, penegakan hukum terhadap pelaku tentu berbeda dengan hanya sebatas melanggar ketentuan imigrasi. Berdasarkan hal tersebut hukum pidana Indonesia menganut asas teritorial yang berlaku bagi WNA maupun WNI ketika berbuat kejahatan yang mengancam keamanan Indonesia. Prinsip ini diatur dalam pasal 2 KUHP yang menjelaskan ketentuan pidana Indonesia berlaku bagi setiap orang yang melakukan tindak pidana di wilayah Indonesia. Sebagai Contoh sebuah kasus, Pembobolan data bansos yang dilakukan warga negara Amerika Serikat di Indonesia, pelaku membuat sebuah web palsu yang disebarluaskan ke penduduk Amerika dan mendapatkan keuntungan dari dana bansos. kejahatan tersebut menimbulkan kerugian sebesar \$500 juta, dengan bantuan Mabes Polri dan FBI kasus ini terungkap pada bulan April 2021. Pelaku mendapat dakwaan dengan pasal 32 ayat (2) jo Pasal 48 ayat (2) UU RI Nomor 19 tahun 2016 tentang perubahan UU ITE Nomor 11 tahun 2008 jo Pasal 55 ayat (1) KUHP, dan mendapat ancaman pidana 9 tahun dan denda paling banyak 3 miliar. Berdasarkan kasus tersebut menggambarkan upaya pemerintah Indonesia yang tidak tinggal diam ketika pertahanan dan keamanan negara diganggu oleh orang asing dan bertindak selaras dengan prinsip asas teritorial Pasal 2 KUHP.

### **3.2. Asas Ekstrateritorial hukum pada UU ITE terhadap Penyelesaian Kasus Kejahatan Deepfake bagi WNA**

Pemulihan terhadap kerugian yang ditimbulkan oleh korban erat kaitannya dengan seberapa besar tanggung jawab pelaku kejahatan deepfake, sebagaimana yang kita tau kejahatan deepfake yang merupakan kejahatan dunia digital sulit untuk dihentikan penyebarannya. Para penegak hukum pun kadang kali kesulitan untuk menyelesaikan kasus ini dikarenakan selain belum ada regulasi yang mengatur secara spesifik juga kesulitan dalam mengakses siapa pelaku tersebut, karena kejahatan deepfake cenderung beridentitas anonim. Permasalahan lain pun juga menghambat proses pemeriksaan apabila pelaku seorang WNA. Pertanyaan yang muncul setelahnya bagaimana hukum di indonesia dapat mengadili yang bukan WNI. Hal ini sangat erat kaitannya dengan kejahatan digital seperti deepfake yang sangat memungkinkan yang mana pelaku bisa saja berasal dari berbagai negara yang mengambil data para korban dari sosial media ataupun pencurian data ilegal atau disebut para Hacker. Di Indonesia sendiri dalam peraturannya terkait kejahatan berbasis digital baik dalam KUHP, UU ITE, UU TPKS, dan peraturan terkait pidana lainnya menerapkan asas teritorial hukum.

Penerapan Asas teritorial bertujuan untuk menjangkau segala aspek yang menimbulkan hambatan bagi penegak hukum dalam implementasi regulasi indoneia contohnya dalam kasus deepfake yang berbasis digital ini cenderung dalam konteks lintas negara yang membutuhkan yurisdiksi internasional. Penerapan yurisdiksi menjadi masalah hukum internasional bila dalam suatu kasus ditemukan unsur asing. Misalnya kewarganegaraan pelaku dan/korban yang warga negara asing, atau tempat perbuatan atau peristiwa terjadi di luar negeri. Secara umum yurisdiksi Internasional terdapat dua bagian yaitu yurisdiksi teritorial dan ekstrateritorial . Yurisdiksi teritorial adalah hukum yang dibatasi oleh wilayah negara dan yurisdiksi ekstrateritorial adalah yurisdiksi dari negara yang diterapkan

di luar jangkauan batas wilayah negara itu sendiri dan laut bebas. Jurisdiksi internasional merupakan solusi dari aparat penegak hukum terhadap penyidikan masalah lintas negara yang menekankan mereka pada kerja sama hukum dengan aparat negara lain untuk menindak suatu tindak pidana dan dijustifikasi dengan peraturan perundang-undangan Indonesia<sup>9</sup>. Oleh karena itu Indonesia menjadi salah satu negara yang menggunakan asas lain dalam peraturan pidana yang dalam kondisi tertentu tidak dapat dijangkau asas teritorial terkhusus pada kasus deepfake yaitu asas Ekstrateritorial.

Keberlakuan asas teritorial undang-undang pidana di Indonesia terdapat dalam KUHP yang berlaku secara internasional yaitu pasal 2 KUHP dan perluasan asas ini diatur dalam pasal 3 KUHP. Sedangkan Asas ekstrateritorial hukum dalam peraturan di Indonesia yaitu dalam UU ITE. Pada pasal 2 UU ITE menyatakan setiap orang yang melakukan perbuatan melawan hukum sebagaimana yang diatur baik berada dalam wilayah hukum Indonesia maupun diluar wilayah hukum Indonesia yang mana hal ini menyebabkan timbulnya akibat hukum dalam wilayah hukum Indonesia maupun di luar wilayah hukum Indonesia serta menimbulkan kerugian bagi kepentingan Indonesia. Sehingga dapat dikatakan bahwa perbuatan tindak pidana kejahatan khususnya Deepfake yang diperbuat oleh WNI ataupun WNA yang dilakukan di dalam atau diluar wilayah hukum Indonesia baik badan hukum Indonesia maupun badan hukum asing selama mengakibatkan kerugian dapat ditindak dengan UU ITE.

Asas ekstrateritorial dalam peraturan perundang-undangan tidaklah cukup dalam menanggulangi kekerasan seksual berbasis deepfake. Asas ini bekerja berbarengan dengan perjanjian internasional. Perjanjian Internasional tersebut dapat berupa bilateral seperti yang tercantum dalam ratifikasi undang-undang nomor 42 tahun 2007 tentang Perjanjian Ekstradisi antara Republik Indonesia dan Republik Korea, atau multilateral seperti yang tercantum dalam undang-undang nomor 7 tahun 2006 tentang Pengesahan United Nations Convention Against Corruption, 2003 (Konvensi Perserikatan Bangsa-Bangsa Anti Korupsi, 2003). Ekstradisi dalam hal ini adalah berasal dari kata "ex" artinya keluar dan "tradere" artinya memberikan. Cherif Bassiouni mengatakan ekstradisi adalah "proses hukum berdasarkan perjanjian, hubungan timbal balik, rasa hormat, atau hukum nasional, dimana satu negara memberikan atau mengirimkan ke negara lain, seorang yang didakwa atau dihukum karena tindak kejahatan terhadap hukum negara yang meminta atau yang melanggar hukum pidana internasional agar diadili atau dihukum di negara peminta sehubungan dengan kejahatan yang dinyatakan dalam permintaan". Perjanjian Internasional perlu diratifikasi apabila ada kehendak dari pemerintah. Hal ini ditekankan dalam pasal 11 UUD NRI 1945 yang berbunyi; "Presiden dalam membuat perjanjian internasional yang menimbulkan akibat yang luas dan mendasar bagi kehidupan rakyat, yang terkait dengan beban keuangan negara, dan/atau mengharuskan perubahan atau pembentukan undang-undang,

<sup>9</sup> Ian Brownlie, *Principles of Public International Law*, 7th ed. (Oxford: Oxford University Press, 2008).

harus memperoleh persetujuan dari DPR". Dengan demikian perihal ekstradisi ini merupakan salah satu hajat yang diperlukan dalam perlindungan data pribadi rakyat Indonesia.

Penerapan konsep ekstradisi pidana dapat digunakan dalam menanggulangi kekerasan seksual berbasis deepfake, meskipun tidak mudah dilakukan oleh banyak negara. Ekstradisi sejurnya merupakan konsep yang sulit dilakukan dan banyak negara menghindarinya. Proses administrasi yang terlalu lama adalah salah satu alasan mengapa beberapa negara enggan melakukan ekstradisi. Indonesia termasuk yang memiliki rapor merah akan hal ini pasca permohonan ekstradisi ke negara Singapura. Indonesia pada saat itu meminta ekstradisi atas kasus Turco Westerling yang kabur ke negara Singapura yang termasuk negara persemaikan Inggris. Indonesia telah meminta ekstradisi kepada Inggris namun kenyataannya ditolak dengan alasan belum adanya perjanjian internasional antara negara Locus Delicti dan negara yang diminta mengenai ekstradisi tersebut<sup>10</sup>. Ekstradisi dapat dilakukan tanpa perjanjian internasional, hanya saja memerlukan asas resiprositas. Negara bisa saja meminta pelaku kriminal untuk dideportasi, asalkan negara yang diminta melakukan hal yang sama ketika berlaku sebaliknya. Berdasarkan hal ini warga negara asing yang melakukan tindak pidana kekerasan seksual berdasarkan deepfake dapat diproses berdasarkan UU ITE atau UU PDP yang berlaku di Indonesia.

## UIN Law Review

### 3.3. Penerapan Konsep Cyber Shield System dalam penanganan Deepfake

Kecerdasan Buatan (Artificial Intelligence/AI) telah memberikan dampak besar dalam kehidupan kita, baik dalam meningkatkan efisiensi maupun membuka peluang baru. Namun, tanpa regulasi yang jelas, teknologi ini dapat disalahgunakan untuk tujuan yang merugikan masyarakat, bahkan menimbulkan ancaman serius terhadap privasi, keamanan, dan kehidupan bermasyarakat. Kejahatan siber berbasis deepfake semakin berkembang di Indonesia, oleh karena itu di Indonesia sendiri terdapat regulasi dari Direktorat Tindak Pidana Siber (Dittipidsiber) adalah satuan kerja yang berada di bawah Bareskrim Polri dan bertugas untuk melakukan penegakan hukum terhadap kejahatan siber.

Secara umum, Dittipidsiber menangani dua kelompok kejahatan, yaitu computer crime dan computer-related crime. Dittipidsiber juga melayani pemeriksaan barang bukti digital dari berbagai satuan kerja, baik dari tingkat Mabes hingga Polsek. Selain itu, Dittipidsiber juga menjalin kerja sama dengan berbagai instansi, baik dalam dan luar negeri, guna memudahkan koordinasi dalam pengungkapan kejahatan siber yang bersifat transnasional dan terorganisir. Guna mendukung pembuktian kejahatan siber, Dittipidsiber dilengkapi dengan beragam kemampuan dan fasilitas pendukung, salah satunya yaitu laboratorium digital forensic, yang memenuhi standar mutu dalam hal manajerial dan teknis pemeriksaan barang bukti digital. Namun regulasi yang dibuat pemerintah saat ini

<sup>10</sup> I.Wayan Parthiana, *Ekstradisi Dalam Hukum Internasional Dan Hukum Nasional Indonesia* (Bandung: Mandar Maju, 2004).

masih belum memadai untuk menyelesaikan permasalahan Cybercrime terlebih khusus terhadap kasus deepfake.

Tanpa regulasi yang memadai, ekosistem digital di Indonesia menjadi medan yang rawan untuk penyalahgunaan teknologi AI. Saat ini, belum ada kerangka hukum yang spesifik untuk mengatur atau mencegah penyalahgunaan AI, sehingga pelaku kejahatan dapat beroperasi dengan bebas. Hal ini meninggalkan masyarakat tanpa perlindungan hukum yang jelas dan memadai. Ketidakamanan ini berpotensi memperburuk kepercayaan publik terhadap teknologi, yang pada akhirnya akan memperlambat adopsi dan inovasi yang seharusnya membawa manfaat dan Perlindungan Data Pribadi Masyarakat.

Karena Perlindungan Data Pribadi (PDP) terdapat hubungan erat dengan hak asasi manusia (HAM). UU Perlindungan Data Pribadi di Indonesia, yang mengatur bagaimana data pribadi harus dilindungi, sejalan dengan prinsip-prinsip HAM yang mengutamakan hak atas privasi dan perlindungan informasi pribadi. Hal ini penting dalam era digital saat ini, di mana data pribadi seringkali disalahgunakan, membawa dampak negatif bagi individu. Dalam hal ini, keadilan tidak hanya harus diterapkan pada pelaku dan korban kejahatan, tetapi juga dalam perlindungan terhadap data pribadi, yang merupakan aspek fundamental dari martabat manusia.

Melihat dari negara dengan sistem keamanan terbaik terhadap kejahatan deepfake, yaitu China. Negara yang memiliki regulasi terkait deepfake adalah China melalui Provisions on the Administration of Deep Synthesis of Internet-based Information Service. China telah menyetujui "Deep Synthesis Provisions" pada tahun 2022, yang mengatur penggunaan teknologi deepfake. Peraturan ini disusun oleh Administrasi Siber Tiongkok (CAC). Salah satu lembaga terkuat di Tiongkok. Regulasi yang ditetapkan oleh Cyberspace Administration of China (CAC) pada Minggu malam 11 Desember mengatur agar individu dilindungi dari penyamaran tanpa izin mereka menggunakan deepfake, gambar yang sulit dibedakan dari yang asli, dan dapat digunakan dengan mudah untuk manipulasi atau informasi yang menyesatkan.<sup>11</sup> .

Regulasi ini melarang pemanfaatan teknologi untuk menyebarkan informasi dan mewajibkan penyedia layanan untuk memberi label pada konten yang dihasilkan oleh teknologi deepfake. Peraturan ini juga menetapkan tanggung jawab bagi penyedia layanan untuk menjaga data agar tetap aman dan melindungi informasi pribadi pengguna. Regulasi ini secara jelas melarang penerapan deepfake untuk tujuan yang melanggar hukum, seperti penipuan atau pencemaran nama baik. Latar belakang lahirnya regulasi ini pun dikarenakan kejahatan yang semakin mengancam privasi warga negara China dan penyalahgunaan data. Kemudian demi keseimbangan sektor ekonomi digital China yang menjadi fokus utama sebagian besar kebijakan nasional China.

---

<sup>11</sup> Giulia Interesse, "China to Regulate Deep Synthesis (Deepfake) Technology from 2023," [www.china-briefing.com, 2023, <https://www.china-briefing.com/2023/01/11/china-to-regulate-deep-synthesis-deepfake-technology-from-2023/>](https://www.china-briefing.com/2023/01/11/china-to-regulate-deep-synthesis-deepfake-technology-from-2023/)

Penyelesaian kasus deepfake di Indonesia seharusnya bisa kita pelajari dari negara Cina, di mana kita tahu bahwa Cina merupakan negara di Asia yang mempunyai sistem teknologi maju dan keamanan siber yang terus menjadi perhatian serta terus diperbaiki oleh pemerintahnya. Merujuk pada pengalaman China, Indonesia sebaiknya mempertimbangkan penerapan regulasi yang lebih terperinci mengenai teknologi deepfake. Sebagaimana deepfake bisa dimanfaatkan untuk tujuan negatif, seperti menyebarkan berita bohong atau melakukan penipuan, penting bagi Indonesia untuk menetapkan regulasi yang lebih ketat terhadap penggunaan teknologi ini. Aturan yang tegas akan membantu melindungi privasi orang, menjaga kepercayaan masyarakat, dan memastikan bahwa deepfake tidak dimanfaatkan untuk merugikan reputasi atau keamanan negara<sup>12</sup>

Perbedaan regulasi di cina serta indonesia pun memiliki beberapa perbedaan. Dimana china sebagai negara yang fokus terhadap teknologi modern lebih spesifik dalam menangani kasus deepfake ini. mereka memiliki regulasi yang spesifik terkait deepfake serta lembaga khusus yang menangani deepfake. Beberapa poin penting yang terdapat dalam regulasi yaitu Deep Synthesis Provisions terkait deepfake:

1. Pengguna perlu memberikan izin jika foto mereka akan dimanfaatkan dalam teknologi sintesis secara lebih mendetail dalam bentuk apa pun.
2. Layanan sintesis mendalam tidak diizinkan untuk memanfaatkan teknologi dalam menyebarkan informasi yang salah.
3. Layanan deepfake harus memverifikasi identitas asli penggunanya.
4. Konten deepfakes perlu menyertakan semacam peringatan untuk memberitahukan pengguna bahwa gambar atau video telah dimanipulasi menggunakan teknologi.
5. Konten yang melanggar peraturan yang berlaku dilarang, begitu juga konten yang mengancam keamanan serta kepentingan nasional, merusak reputasi negara atau mengganggu ekonomi.

Sedangkan regulasi yang berkaitan tentang deepfake di Indonesia meliputi Undang- Undang Nomor 19 Tahun 2016 mengenai Informasi dan Transaksi Elektronik (UU ITE), Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP 71/2019), serta Undang- Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). UU ITE melarang praktik manipulasi informasi elektronik, termasuk penciptaan dan distribusi konten yang tidak benar, namun belum terdapat regulasi yang secara khusus mengatur deepfake. UU PDP memberikan perlindungan bagi data pribadi, tetapi belum menguraikan secara rinci tanggung jawab penyedia dan pengguna teknologi.

---

<sup>12</sup> A Kharpal, "China Is About to Get Tougher on Deepfakes in an Unprecedented Way," [www.cnbc.com, 2022, https://www.cnbc.com/2022/12/23/china-is-bringing-in-first-of-its-kind-regulation-on-deepfakes.html](https://www.cnbc.com/2022/12/23/china-is-bringing-in-first-of-its-kind-regulation-on-deepfakes.html).

Dengan adanya problematika tersebut gagasan berupa Cyber shield system ini dapat menjadi solusi solutif dalam penanganan kasus deepfake serta metode yang lebih spesifik dalam mengontrol kejahatan deepfake di indonesia. Dimana Peraturan tersebut dapat meliputi tanggung jawab penyedia layanan deepfake, perlindungan data, keterbukaan, serta penegakan hukum yang lebih efisien. Selain itu, peraturan tersebut perlu memasukkan ketentuan terkait pelabelan konten deepfake guna mencegah penyebaran informasi palsu serta melindungi masyarakat dari kemungkinan penipuan atau kejahatan lain yang memanfaatkan teknologi.

Konsep Cyber Shield System sejatinya diadopsi dari regulasi china dalam deep synthesis regulation, namun penulis menyesuaikan konsep Cyber Shield System dengan norma dan hukum yang ada di indonesia. Kata cyber sendiri merujuk pada teknologi dan internet, shield berarti perisai atau pelindung dan system berarti komponen yang saling terkait. Sesuai dengan namanya Cyber Shield System ini dapat menjadi suatu solusi yang dapat menjaga keamanan sistem informasi dan data pribadi milik seseorang agar tidak disalahgunakan atau dicuri oleh pihak yang tidak bertanggung jawab. Untuk menunjang keberhasilan sistem ini akan dibentuk lembaga khusus pengawas yang dibawahi oleh kementerian komunikasi dan digital (KOMDIGI) yang juga akan bekerja sama dengan Badan siber dan sandi negara (BSSN)<sup>13</sup>.

Adanya Lembaga pengawas khusus deepfake yang bertugas untuk mengawasi dan membentuk website yang bernama Cyber Shield System ini. Cara kerja dari sistem ini yaitu dapat memeriksa setiap konten yang dihasilkan serta adanya verifikasi data lengkap pembuat konten. Lalu dilanjutkan dengan verifikasi persetujuan atas pemilik data yang digunakan oleh pembuat konten. Setelah verifikasi akan dilakukan pengecekan keaslian konten dari website terverifikasi yang dibentuk lembaga pengawas deepfake<sup>14</sup>. Apabila konten tersebut telah melalui pengecekan maka setiap konten akan diberikan Watermark atau label konten. Apabila konten tidak sesuai ketentuan dan melanggar kode etik serta mengandung unsur pornografi maka akan di take down. kemudian langkah yang dapat dilakukan oleh masyarakat yang merasa adanya konten pelecehan berdasarkan data pribadi mereka tanpa izin dapat melapor ke website lembaga pengawas deepfake untuk di take down.

Dengan hadirnya Konsep Cyber Shield System ini dapat lebih efektif dan sesuai dengan hukum di indonesia serta lebih sederhana dalam sistem kerja dibanding Deep Synthesis Provisions dari china. Hal ini karena Konsep Cyber Shield System dapat menyelesaikan dan mengawasi kejahatan digital deepfake serta lebih cepat dalam menemukan pelaku kejahatan deepfake ini. Walaupun sistem teknologi di

<sup>13</sup> I D Kasita, "Deepfake Pornografi: Tren Kekerasan Gender Berbasis Online (KGBO) Di Era Pandemi Covid-19," *Jurnal Wanita Dan Keluarga* 3, no. 1 (2022), <https://doi.org/10.22146/jwk.5202>.

<sup>14</sup> M A Jufri and A K Putra, "Aspek Hukum Internasional Dalam Pemanfaatan Deepfake Technology Terhadap Perlindungan Data Pribadi," *Uti Possidetis: Journal of International Law* 2, no. 1 (2021), <https://doi.org/10.22437/up.v2i1.11093>.

indonesia belum sehebat china dalam sektor teknologi digital namun penulis yakin bahwa ini dapat menjadi jalan baru bagi pemerintah untuk lebih teliti dan meningkatkan keamanan data warga negara indonesia. Selain Konsep Cyber Shield System juga diperlukan regulasi sebagai penunjang pemberantasan kejahatan deepfake yang akan menjadi payung hukum bagi aparat penegak. Pembentukan UU khusus terkait deepfake juga disarankan. UU ini akan membahas secara khusus terkait apa saja yang termasuk kejahatan deepfake, pengelolaan Konsep Cyber Shield System serta sanksi bagi pelaku kejahatan deepfake.

#### 4. KESIMPULAN

Berdasarkan pada pemaparan yang dianalisis secara holistik dalam pembahasan sebelumnya, maka dapat ditarik kesimpulan yang diantaranya:

1. Kejahatan digital seperti deepfake menambah kompleksitas dalam penegakan hukum di Indonesia, terutama karena pelaku seringkali anonim dan dapat berasal dari luar negeri. Kejahatan ini memerlukan pemulihan bagi korban yang seringkali kesulitan mendapatkan keadilan karena tantangan dalam melacak pelaku dan kurangnya regulasi yang mengatur secara spesifik. Untuk itu, Indonesia menerapkan asas teritorial dan ekstrateritorial dalam peraturan hukum pidana, yang memungkinkan hukum Indonesia berlaku bagi kejahatan yang terjadi di luar wilayah negara jika menimbulkan kerugian di Indonesia. Penerapan asas ekstrateritorial ini didukung oleh perjanjian internasional seperti ekstradisi yang memperkuat kerja sama lintas negara dalam menangani kejahatan siber. Namun, meskipun konsep ekstradisi penting, prosesnya sering kali menemui hambatan administratif, seperti yang terlihat dalam kasus-kasus sebelumnya. Oleh karena itu, Indonesia perlu terus memperkuat regulasi dan kolaborasi internasional untuk mengatasi tantangan penegakan hukum terhadap kejahatan digital, termasuk yang melibatkan WNA, guna melindungi hak-hak korban dan menjaga keamanan nasional.
2. Perlindungan data pribadi (PDP) sangat erat kaitannya dengan hak asasi manusia (HAM), terutama dalam konteks kejahatan digital seperti deepfake yang berpotensi merusak privasi dan martabat individu. Meskipun Indonesia telah memiliki regulasi terkait teknologi digital, seperti UU ITE dan UU PDP, regulasi yang mengatur deepfake secara spesifik masih kurang mendalam. Oleh karena itu, Indonesia dapat belajar dari China yang telah memiliki regulasi yang lebih terperinci mengenai deepfake melalui Provisions on the Administration of Deep Synthesis of Internet-based Information Service.

Berangkat dari pembahasan yang telah dipaparkan beserta kesimpulan yang disampaikan, maka terdapat beberapa rekomendasi yang dihasilkan yaitu:

1. Perlu dibentuk UU khusus yang menanggulangi kekerasan seksual berbasis deepfake beserta peraturan pelaksananya.
2. Perlu adanya divisi khusus dibawah BSSN yang menanggulangi kekerasan seksual berbasis deepfake yang berkoordinasi dengan Menkomdigi dalam hal pengawasan siber.

## REFERENSI

### Buku

- Brownlie, Ian. *Principles of Public International Law*. 7th ed. Oxford: Oxford University Press, 2008.
- Grafika, R.S.K.U.H.P. *Kitab Undang-Undang Hukum Pidana Undang-Undang RI Nomor 1 Tahun 2023*. Jakarta: Sinar Grafika, 2023.
- Locke, John. *Two Treatises of Government*. Edited by Peter Laslett. Cambridge: Cambridge University Press, 1988.
- Parthiana, I.Wayan. *Ekstradisi Dalam Hukum Internasional Dan Hukum Nasional Indonesia*. Bandung: Mandar Maju, 2004.
- Soekanto, Soerjono, and Sri Mamudji. *Penelitian Hukum Normatif: Suatu Tinjauan Singkat*. Jakarta: RajaGrafindo Persada, 2003.
- Utami, Sri Puguh Budi. *Perlindungan Korban Kejahanan Dalam Perspektif Hukum Progresif*. Jakarta: Prenadamedia Group, 2020.

### Artikel Jurnal

- Jufri, M A, and A K Putra. "Aspek Hukum Internasional Dalam Pemanfaatan Deepfake Technology Terhadap Perlindungan Data Pribadi." *Uti Possidetis: Journal of International Law* 2, no. 1 (2021). <https://doi.org/10.22437/up.v2i1.11093>.
- Kasita, I D. "Deepfake Pornografi: Tren Kekerasan Gender Berbasis Online (KGBO) Di Era Pandemi Covid-19." *Jurnal Wanita Dan Keluarga* 3, no. 1 (2022). <https://doi.org/10.22146/jwk.5202>.
- Kharpal, A. "China Is About to Get Tougher on Deepfakes in an Unprecedented Way." [www.cnbc.com, 2022. https://www.cnbc.com/2022/12/23/china-is-bringing-in-first-of-its-kind-regulation-on-deepfakes.html](https://www.cnbc.com/2022/12/23/china-is-bringing-in-first-of-its-kind-regulation-on-deepfakes.html).
- Putri, A S, S Noerdajasakti, and F Sulistio. "RTBF as an Effort to Establish Legal Protection for Victims of Deepfake Pornography in Indonesia." *International Journal of Social Science and Human Research* 6, no. 6 (2023).

### Website

- alchemistgroup.co. "Pengaturan Hukum Teknologi Deepfake Di Indonesia - ALO," 2024. <https://alchemistgroup.co/pengaturan-hukum-teknologi-deepfake-di-indonesia/>.
- Auli, R C, and S.H. "Bunyi Pasal 27 Ayat (1) UU ITE 2024 Tentang Kesusaian." [hukumonline.com, 2024. https://www.hukumonline.com/klinik/a/bunyi-](https://www.hukumonline.com/klinik/a/bunyi-).
- Interesse, Giulia. "China to Regulate Deep Synthesis (Deepfake) Technology from 2023." [www.china-briefing.com, 2023. https://www.china-briefing.com/news/china-](https://www.china-briefing.com/news/china-)

to-.

Kharpal, A. "China Is About to Get Tougher on Deepfakes in an Unprecedented Way." [www.cnbc.com, 2022. <https://www.cnbc.com/2022/12/23/china-is-bringing-in-first-of-its-kind-regulation-on-deepfakes.html>](https://www.cnbc.com/2022/12/23/china-is-bringing-in-first-of-its-kind-regulation-on-deepfakes.html).

VIDA. "Deepfake AI: Jenis, Risiko, Dan Solusi Untuk Menghadapinya." [vida.id, n.d.](https://vida.id/id/blog/deepfake-ai) <https://vida.id/id/blog/deepfake-ai>

# UIN Law Review