

PENEGAKKAN HUKUM TERHADAP PENYALHUNAAN KECERDASAN BUATAN DENGAN CARA MEMANIPULASI WAJAH SESEORANG KE DALAM GAMBAR ATAU VIDEO PORNO¹

Oleh :
Natanael Hiskia Mongkau²
Herlyanty Y. A. Bawole³
Altje A. Musa⁴

ABSTRAK

Penelitian ini bertujuan untuk mengetahui aturan mengenai penyalahgunaan kecerdasan buatan dengan cara memanipulasi wajah seseorang ke dalam gambar atau video porno dan untuk mengkaji penegakan hukum terhadap penyalahgunaan kecerdasan buatan dengan cara memanipulasi wajah seseorang ke dalam gambar atau video porno. Metode yang digunakan adalah penelitian normatif, dengan kesimpulan yaitu: 1. Di Indonesia, penyebab ketidakselesaian kasus-kasus ini adalah kurangnya pengaturan komprehensif untuk perlindungan data pribadi, serta tidak adanya harmonisasi antara lembaga pemerintah. Hal ini mengakibatkan penegak hukum ragu dalam menerapkan sanksi, menciptakan ketidakpastian hukum, dan menyulitkan korban untuk mengajukan tuntutan. UU ITE yang ada saat ini tidak mencakup pelaku pembuatan video deepfake pornografi. 2. Hukuman seharusnya dapat menghentikan tindak pidana penyalahgunaan *deepfake*. Namun, kekurangan undang-undang yang jelas tentang deepfake dapat menyebabkan ketidakpastian hukum. Hal ini disebabkan oleh ketidakjelasan tentang cara mencegah dan menanggulangi kejahatan *deepfake* dan kecerdasan buatan. Dalam kasus tersebut Hakim tidak mempertimbangkan motif Terdakwa dalam melakukan pembuatan foto rekayasa yang bermuatan pornografi untuk tujuan pengancaman. Pasal yang diterapkan dianggap terlalu jauh dan tidak berdampak signifikan terhadap Korban. Seharusnya, Hakim lebih memperhatikan Pasal 29 Undang-Undang Republik Indonesia Nomor 44 Tahun 2008 tentang Pornografi yang terdapat dalam Dakwaan Subsidiar Penuntut Umum, serta menghukum Terdakwa atas pemalsuan informasi/dokumen elektronik yang diatur dalam Pasal 51 Ayat (1) jo Pasal 35 Undang-Undang ITE. Selain itu, dari berbagai tindakan yang dilakukan oleh Terdakwa, Hakim juga seharusnya menerapkan ketentuan Concursus dengan sistem pidanaan Absorpsi Dipertajam untuk mencapai keadilan.

Kata Kunci : *penegakan hukum, deep fake*

PENDAHULUAN

A. Latar Belakang

Perkembangan teknologi informasi dan komunikasi berkembang sangat pesat di Indonesia. Dari masa ke masa kemajuan teknologi informasi telah perubahan dan pergeseran yang sangat cepat dan pesat dalam kehidupan yang tanpa batas sekalipun.

Hadirnya teknologi juga memberikan manfaat bagi kesejahteraan dan kemajuan. Dengan membawa dampak yang cukup besar bagi penggunaanya berupa dampak positif karena dengan teknologi semakin terbuka dan tersebarnya informasi pengetahuan dari seluruh dunia yang menembus batas ruang dan waktu. Begitu juga diikuti dampak negatif, perkembangan kejahatan dengan berbagai modus menggunakan teknologi dan informasi membuat terjadinya perubahan nilai,

moral, dan norma yang bertentangan dengan kehidupan masyarakat .

Salah satu perbuatan yang melanggar hukum melalui jaringan internet yang marak terjadi adalah kejahatan di bidang siber. Kejahatan dalam dunia maya atau internet ini disebut dengan istilah *Cyber Crime*⁵. Kejahatan siber (*cybercrime*) merupakan salah satu bentuk baru dari kejahatan di dunia modern yang berbasis kecanggihan teknologi yang bersifat universal dimensional dalam lingkup dunia maya yang berdampak negatif pada realitas kehidupan manusia yang sesungguhnya. Kejahatan siber (*cybercrime*) ini banyak digunakan sebagai sarana pelecehan seksual, penyebaran berita hoaks, sampai kejahatan yang merujuk kepada tindak pidana pornografi. Adanya kejahatan siber (*cybercrime*) telah menjadi ancaman stabilitas, sehingga pemerintah sulit mengimbangi teknik kejahatan yang dilakukan dengan teknologi

¹ Artikel Skripsi

² Mahasiswa Fakultas Hukum Unsrat, NIM 20071101241

³ Fakultas Hukum Unsrat, Doktor Ilmu Hukum

⁴ Fakultas Hukum Unsrat, Doktor Ilmu Hukum

⁵ Dista Amalia Arifah, "Kasus Cyber Crime Di Indonesia", Jurnal Bisnis dan Ekonomi Vol.18 No. 2 hlm 187

komputer. Tindak pidana pornografi sendiri merupakan salah satu contoh kejahatan siber yang saat ini paling marak terjadi di Indonesia.⁶

Perkembangan teknologi di dunia bahkan di Indonesia sudah semakin pesat. Kecerdasan Buatan atau *artificial intelligence* salah satu bukti perkembangan teknologi di era digital yang dapat memberikan dampak positif di berbagai aspek kehidupan, bukan hanya teknologi yang mengandalkan kecerdasan manusia, tetapi teknologi sendiri juga sudah memiliki kecerdasan sendiri atau disebut dengan AI (*Artificial intelligence*). Sebagai salah satu bagian dari sistem pengolahan berbasis komputer yang mempelajari dan melakukan pekerjaan seperti dan sebaik manusia bahkan bisa lebih baik dibandingkan dengan yang dilakukan oleh manusia⁷. *Artificial intelligence* ditengah-tengah kehidupan masyarakat memiliki pengaruh yang kuat. Namun, saat ini *artificial intelligence* banyak disalahgunakan oleh para penjahat siber yang disebut *Artificial Intelligence-Crime* (AIC)⁸. Salah satu turunan dari penggunaan teknologi buatan manusia adalah *Deepfake*. *Deepfake* ini merupakan penggunaan dari istilah *deep learning* and fakes. *Deepfake* dipergunakan untuk memalsukan/memanipulasi (Fakes) gambar atau video dalam sebuah peristiwa dengan menggunakan teknik pemindaian menyeluruh dan mendasar terhadap citra manusia. Siapapun dapat mengakses aplikasi *deepfake* serta membuat video atau gambar editan sesuai dengan yang diinginkan. Tujuan awal dari penggunaan *Deepfake* yaitu untuk hiburan di televisi maupun media sosial. Akan tetapi *deepfake* sendiri bisa membuat kejahatan di dunia maya (*cybercrime*).

Deepfake bisa menjadi alat untuk menyesatkan orang menyebarkan informasi palsu. *Deepfake* memiliki potensi untuk mengikis kepercayaan masyarakat, terutama apabila hal tersebut berhubungan dengan orang besar dan ternama. Tidak hanya soal video palsu, reputasi seseorang juga dapat rusak dengan mudah dengan teknologi ini. Banyak orang menyebarkan konten negatif dengan adanya aplikasi *deepfake*, seperti

halnya penyebaran berita hoaks ataupun adanya manipulasi data yang dilakukan dengan mudah⁹.

Adapun kejahatan-kejahatan yang dapat terjadi dengan memanfaatkan teknologi *deepfake*, yaitu:¹⁰

1. Pemalsuan identitas;
2. Konten pornografi non-konsensual dan eksploitasi seksual;
3. Pemerasan (*blackmailing*);
4. Penyebaran informasi palsu dan menggiring opini publik;
5. Menyebarkan teror;
6. Penipuan;
7. Pencemaran nama baik;

Deepfake Porn yang terlanjur tersebar bisa megancam kedudukan dan pekerjaan seseorang. Kejahatan *deepfake porn* menimbulkan kerugian bagi banyak orang, tidak hanya dari kalangan selebriti, tokoh ternama, seperti politisi juga bisa kena.

Dari banyak kasus *deepfake porn* ini, salah satu contoh Studi Kasus Putusan Nomor 125/Pid.sus/2019/PN Bjn yang terjadi di Desa Beji RT. 01 RW. 01 Kecamatan Kedewan Kabupaten Bojonegoro atas nama Terdakwa Eko Purwanto yang dituduh telah mengirimkan foto-foto bugil dengan wajah mirip para saksi korban yaitu saksi Eny Nur Alisa Binti Muntari, saksi Tata Nur Diana Binti Hamim, saksi Jovi Lidyawati binti Kuswo, saksi Rina Dewi Anggreani Binti Suparwo, saksi Nila Nungraini binti Kariman sedangkan badan yang ada didalam foto tersebut diperoleh dari foto – foto bugil dengan menggunakan aplikasi *friends blender* telah mengubah atau mengedit 4 foto bugil yang disimpannya kemudian dengan melakukan manipulasi digital mengubah dan mengganti wajah dalam foto bugil tersebut dengan wajah dari masing-masing saksi korban yang kemudian foto – foto editan tersebut dikirim oleh Terdakwa kepada masing - masing saksi korban, disertai dengan chat “akan menyebarkan foto bugil dan video para saksi korban ke media sosial apabila para saksi korban berusaha memblokir nomor WhatsApp Terdakwa dan memviralkannya“

⁶ Eva Istia Utawi, Neni Ruhaeni, Penegakan Hukum Terhadap Tindak pidana Pornografi Menurut Peraturan Perundang- Undangan Tentang Pornografi Melalui Media Sosial, Jurnal Bandung Conference Series 3 (1) Januari 2023, hlm 365

⁷ Muhammad Faqih Faaturrahman, Enni Soerjati Priorwirjanto Pengaturan Pertanggungjawaban Pelaku Penyalahgunaan Deepfakes Dalam Teknologi Kecerdasan Buatan Pada Konten Pornografi Berdasarkan Hukum Positif Indonesia, Jurnal Indonesia Sosial Teknologi 11 (3) November 2022, hlm 1159

⁸ Thomas C.King, "Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and solution", *Sci Eng Ethics* 26 (14 Februari 2019), <https://s11948-018-000->

⁹ Heny Novyanti, Pudji Astuti, Jerat Hukum Penyalahgunaan Aplikasi Deepfake Ditinjau Dari Hukum Pidana, Jurnal Hukum, 1 (1) Desember 2021, hlm 2

¹⁰ Shanon Gandrova, Ricky Banke, Penerapan Hukum Positif Indonesia Terhadap Kasus kejahatan Dunia Maya Deepfake, Jurnal Ilmiah Multidisipliner, Vol 1 (10) November 2023, hlm 653

Tindak pidana pornografi terkait *Deepfake porn* masih tergolong baru di Indonesia, Seringkali para aparat penegak hukum kesulitan untuk menyelediki identitas dari pelaku, khususnya pembuat video *Deepfake porn*¹¹.

Permasalahan *deepfake* di Indonesia tentu saja tidak sesuai dengan peraturan perundang-undangan di Indonesia, yakni Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Dan Transaksi Elektronik di dalamnya juga mengatur mengenai larangan penyebaran konten pornografi. Dalam undang-undang tersebut menyebut bahwa setiap orang yang menyebarkan informasi elektronik ataupun dokumen elektronik yang memiliki muatan yang melanggar kesusilaan, dipidana dengan pidana penjara paling lama 6 (enam) tahun ataupun denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah). Diketahui bahwa video pornografi merupakan bentuk informasi elektronik yang memiliki muatan yang melanggar kesusilaan, sehingga pelaku pembuat maupun penyebar video pornografi dapat dipidana dengan pidana yang telah diuraikan dalam undang-undang tersebut.

B. Rumusan Masalah

1. Bagaimana pengaturan penyalahgunaan kecerdasan buatan dengan cara memanipulasi wajah seseorang ke dalam gambar atau video porno?
2. Bagaimana penegakan hukum terhadap penyalahgunaan kecerdasan buatan dengan cara memanipulasi wajah seseorang ke dalam gambar atau video porno?

C. Metodologi Penelitian

Metode penelitian yang digunakan dalam penyusunan skripsi ini ialah metode penelitian hukum normatif.

PEMBAHASAN

A. Pengaturan Penyalahgunaan Kecerdasan Buatan dengan Cara Memanipulasi Wajah Seseorang Kedalam Gambar atau Video Porno

Persoalan yang perlu adanya suatu kepastian hukum adalah mengenai Kecerdasan Buatan. Penggunaan kecerdasan buatan (AI) untuk memanipulasi wajah seseorang ke dalam gambar

atau video pornografi, sering disebut sebagai *deepfake pornography*, merupakan salah satu bentuk penyalahgunaan kecerdasan buatan yang mengkhawatirkan.

Teknologi ini menggunakan algoritma pembelajaran mendalam (*deep learning*) untuk mengubah wajah asli dalam gambar atau video dengan wajah orang lain, sehingga tampak sangat realistis. Fenomena ini memunculkan banyak tantangan etis, sosial, dan hukum yang harus dihadapi untuk melindungi privasi dan martabat individu yang menjadi korban. Berikut ini adalah beberapa pendekatan pengaturan dan pencegahan yang bisa dilakukan.

Semakin meningkatnya penggunaan teknologi informasi dan komunikasi terutama di media sosial menghasilkan berbagai jenis kejahatan berbasis siber (*cybercrime*). Salah satu contohnya yaitu kejahatan siber manipulasi atau dikenal *cybercrime deepfake*, merupakan salah satu jenis baru kejahatan di dunia modern yang didasarkan pada kecanggihan teknologi yang sifatnya universal di dalam lingkup dunia maya sehingga memberikan dampak negatif yang tidak dirasakan secara fisik namun sama merugikannya seperti perbuatan pidana yang lain.¹²

Teknologi kecerdasan buatan adalah awal dari produksi dan manajemen, dan memasuki area terancang dengan sistem otomatis dan digital. Meskipun kecerdasan buatan muncul pada tahun 1956, konsep yang mengarah pada kecerdasan buatan telah ada sejak tahun 1941, ketika istilah kecerdasan buatan diciptakan pada tahun 1956 pada konferensi Dartmouth¹³. Kecerdasan buatan telah merasuk ke berbagai aspek kehidupan manusia, mulai dari perangkat rumah tangga pintar hingga chatbot di smartphone, kendaraan, dan teknologi *deepfake*. *Deepfake*, yang merupakan hasil dari kecerdasan buatan, menciptakan tiruan manusia yang realistis. Teknologi ini memanfaatkan jaringan *Generative Adversarial Network (GAN)* untuk menggabungkan dan mengganti gambar dan video dengan yang lain. Popularitas *deepfake* dimulai pada tahun 2017 melalui forum Reddit. *Generative Adversarial Network (GAN)*, yang dikembangkan melalui *TensorFlow* milik Google, awalnya digunakan untuk menempelkan wajah tokoh publik ke tubuh perempuan dalam film porno. Pada Januari 2018, aplikasi *deepfake* bernama *FakeApp* diluncurkan,

¹¹ Antika Setia Dewi, Dian Alan Setiawan, Penegakan Hukum Terhadap Pelaku Video Deepfake Porn Dihubungkan Dengan Hukum Pidana Positif Indonesia, Bandung Conference Series: Law Studies, Vol 4 (1), Januari 2024

¹² Andreas Agung, Hafrida, Erwin, "Pencegahan Kejahatan Terhadap CyberCrime", PAMPAS: Journal of Criminal, Vol.3 No.2 (2022). Hlm. 213

¹³ Sutojo, T. Kecerdasan Buatan. Edisi Pertama. (ANDI OFFSET. Bandung, 2011), 3.

memungkinkan siapa pun untuk membuat *deepfake*. Hal ini membuka jalan bagi penyebaran konten pornografi *deepfake*, baik dalam bentuk video maupun foto¹⁴

Indonesia saat ini masih kekurangan aturan yang jelas dan lengkap untuk menangani penyalahgunaan teknologi kecerdasan buatan dalam pembuatan konten porno *deepfake*. Meskipun begitu, penggunaan teknologi *deepfake* untuk tujuan yang merugikan dapat dikategorikan sebagai kejahatan dunia maya atau *cybercrime*, mengingat konten yang dihasilkan disebarluaskan melalui internet. Dalam era transformasi digital, hampir semua aspek kehidupan terkoneksi secara *online*, mulai dari bisnis dan keuangan hingga layanan kesehatan serta infrastruktur kritis. Keberadaan data digital yang sangat berharga dan sensitif membuat masyarakat rentan terhadap serangan kejahatan siber yang dapat merugikan secara finansial, merusak reputasi, bahkan mengancam keamanan nasional. Pelaku kejahatan siber, yang dapat berupa individu jahat, kelompok terorganisasi, atau bahkan negara-negara dengan niat jahat, dapat melancarkan serangan dengan Tingkat kompleksitas yang tinggi. Mereka dapat mencuri data pribadi, meretas sistem keamanan, atau menyebabkan kerusakan pada infrastruktur kritis, seperti sistem kelistrikan atau jaringan telekomunikasi.

Teknologi kecerdasan buatan memang tidak diatur secara khusus di Indonesia. Dalam pendekatan hukum terkait sistem elektronik, penerapan kecerdasan buatan dapat didasarkan pada Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Kecerdasan buatan dapat digolongkan sebagai sistem elektronik, yaitu kumpulan perangkat dan prosedur elektronik yang bekerja untuk mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, menginformasikan, mengirimkan, dan/atau mendistribusikan informasi elektronik. Penyelenggara sistem elektronik adalah setiap orang, penyelenggara negara, pengusaha, dan

masyarakat yang memasok, mengolah, dan/atau mengurus sistem elektronik, baik sendiri maupun secara bersama-sama kepada pengguna sistem elektronik untuk dirinya sendiri atau orang lain.

Data BSSN (Badan Sandi dan Siber Negara) menunjukkan bahwa serangan siber di Indonesia melonjak hingga nyaris 190 juta pada delapan bulan awal tahun 2020, naik empat kali dari 39 juta pada periode yang sama di tahun sebelumnya. Pada bulan April 2020, Polri mencatat ada 937 kasus yang dilaporkan. Kasus provokatif, konten kebencian, dan ujaran kebencian mendominasi dengan 473 kasus, diikuti penipuan *online* dengan 259 kasus dan konten pornografi dengan 82 kasus¹⁵.

Mengutip data Badan Sandi dan Siber Negara, sepanjang bulan Januari hingga Juli 2021, tercatat 741.441.648 ancaman siber telah terjadi di Indonesia. Berbagai Tindakan kejahatan yang sering terjadi adalah seperti *hacking*, *cracking*, kejahatan *carding* (*credit card fraud*), *ATM skimming*, *phising* (*internet banking fraud*), *cybersquatting*, *malware* (*virus/bots/worm*), terorisme, *human trafficking*, dan pinjaman *online*. Tindakan-tindakan tersebut dapat dengan mudah dilakukan, yaitu dengan memanfaatkan jaringan internet dan kemajuan teknologi di era sekarang.

Teknologi informasi dan komunikasi saat ini terus mengalami perkembangan yang pesat sehingga informasi dapat disebarluaskan dengan mudah melalui internet dan teknologi informasi. Jumlah pengguna internet pun terus meningkat setiap tahunnya. Survei rutin APJII (Asosiasi Penyelenggara Jasa Internet Indonesia) mengungkapkan bahwa pengguna internet di Indonesia terus bertambah dari 88 juta orang pada 2014 menjadi 132,7 juta orang pada 2016. Pada 2017, angka ini naik kembali menjadi 143,26 juta orang. Pada 2018, jumlah pengguna internet mencapai puncaknya dengan 171,17 juta orang¹⁶.

Menangani peningkatan kejahatan siber adalah hal yang penting untuk dilaksanakan.¹⁷ Semua pihak yang terkait, termasuk pemerintah dan masyarakat, harus bekerja sama untuk memberantas kejahatan siber yang memiliki dampak buruk.¹⁸ Kejahatan siber memiliki

¹⁴ Kasita, I. D. 2022. "Deepfake Pornografi Tren Kekerasan Gender Berbasis Online (KGBO) Di Era Pandemi Covid-19. *Jurnal Wanita Dan Keluarga*, 3(1), juli 2022, 20

¹⁵ Ilham Hakim et al., "Meningkatkan Kewaspadaan terhadap Kejahatan Cyber di Era Digital di SMK Negeri 8 Kabupaten Tangerang", *APPA: Jurnal Pengabdian Kepada Masyarakat*, 1(4), 2023, hlm. 188-194.

¹⁶ APJII, "Penetrasi dan Profil Perilaku Pengguna Internet Indonesia", di akses 20 Desember 2023

¹⁷ Jacqueline M. Drew "A study of cybercrime victimization and prevention: Exploring the use of online crime

prevention behaviours and strategies", *Journal of Criminological Research, Policy and Practice*, 6(1), 2020, hlm. 17-33.

¹⁸ Mandlenkosi Richard Mphatheni dan Witness Maluleke, "Cybersecurity as a response to combating cybercrime: Demystifying the prevailing threats and offering recommendations to the African regions", *International Journal of Research in Business and Social Science* (2147-4478), 11(4), 2022, hlm. 384-396.

karakteristik khusus, yaitu tidak ada kontak langsung antara korban dan pelaku di lokasi kejadian.¹⁹ Dalam beberapa situasi, korban dan pelaku bahkan bisa berada di negara yang berlainan. Hal ini menunjukkan bahwa kejahatan siber adalah salah satu jenis kejahatan yang melintasi batas negara (*transnational crime*), tidak terbatas (*borderless*), tanpa kekerasan (*non-violence*), tanpa kontak fisik (*no physically contact*), dan tanpa identitas (*anonymity*).²⁰

Regulasi internasional yang telah mengatur terkait kejahatan siber adalah aturan-aturan hukum yang dibuat oleh negara-negara atau organisasi internasional untuk mencegah, mengendalikan, dan menindak kejahatan yang dilakukan melalui internet atau jaringan komputer.

Dampak *Artificial Intelligence* (AI) dalam skala internasional.

1. Kurangnya Transparansi: Sistem *Artificial Intelligence* atau AI sering kali tidak dapat dijelaskan, menyulitkan penegakan hukum.
2. Pelanggaran Privasi: Penggunaan *Artificial Intelligence* atau AI dapat mengancam privasi individu dan data pribadi.
3. Tanggung Jawab Hukum: Sulit menentukan siapa yang bertanggung jawab atas tindakan *Artificial Intelligence* atau AI.
4. Penyalahgunaan Teknologi: *Artificial Intelligence* atau AI dapat digunakan untuk kejahatan siber dan manipulasi sosial.
5. Ketidakadilan dan Bias: Algoritma *Artificial Intelligence* atau AI dapat memperkuat bias yang ada, merugikan kelompok tertentu.
6. Perubahan dalam Perang: Penggunaan senjata otonom dapat mengubah dinamika konflik bersenjata dan hukum humaniter.
7. Regulasi Global yang Lemah: Kurangnya kesepakatan internasional mengenai penggunaan dan pengaturan *Artificial Intelligence* atau AI.

Perlindungan data pribadi adalah hak asasi yang sangat penting. Di zaman digital ini, Indonesia mengalami perkembangan teknologi yang tak terelakkan. Oleh karena itu, regulasi sangat dibutuhkan untuk menunjang dan menyesuaikan kegiatan masyarakat Indonesia dalam memberikan perlindungan dan keamanan pada penggunaan data pribadi. Undang-Undang

Perlindungan Data Pribadi yang sudah ditetapkan oleh pemerintah diharapkan dapat mengurangi terjadinya pelanggaran atau penyalahgunaan data pribadi warga negara Indonesia, menghindari terjadinya pelanggaran atau penyalahgunaan data pribadi, serta makin memperkuat posisi peraturan. Undang-Undang Perlindungan Data Pribadi dengan adanya hukuman yang ditentukan dalam Undang-Undang Perlindungan Data Pribadi²¹.

Indonesia saat ini masih kekurangan aturan yang jelas dan lengkap untuk menangani penyalahgunaan teknologi kecerdasan buatan dalam pembuatan konten porno *deepfake*. Meskipun begitu, penggunaan teknologi *deepfake* untuk tujuan yang merugikan dapat dikategorikan sebagai kejahatan dunia maya atau *cybercrime*, mengingat konten yang dihasilkan disebarluaskan melalui internet. Pornografi telah diatur dalam beberapa Undang-Undang di Indonesia yang berkaitan dengan informasi elektronik, kesusilaan, pornografi, dan defamasi. Oleh karena itu, dalam kasus penyebaran konten palsu melalui *deepfake* Undang-Undang Informasi dan Transaksi Elektronik dapat diterapkan sebagai hukum khusus yang mengatur transaksi elektronik, termasuk distribusi konten pornografi yang menggunakan teknologi *deepfake*, melecehkan atau memfitnah.²²

Deepfake pornografi memanfaatkan kecerdasan buatan dalam programnya, melanggar Pasal 27 Ayat (1) Undang-Undang Informasi dan Transaksi Elektronik yang berbunyi: "Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan

Pasal 27 ayat (1) Undang-Undang Informasi dan Transaksi Elektronik sebagai pengafirmasi rumusan pidana inti atau rumusan perbuatan yang dilarang. Pasal 27 ayat (1) Undang-Undang Informasi dan Transaksi Elektronik menentukan bahwa tindakan mendistribusikan, mentransmisikan atau membuat dapat diaksesnya konten elektronik yang memiliki muatan asusila termasuk sebagai ketentuan pidana atau tindakan yang dilarang. Pengenaan pidana atas berbagai perbuatan ini dapat dilakukan secara kumulatif atau bersamaan dan dapat juga dilakukan

¹⁹ Petrus Golose, "Penegakan Hukum Cybercrime dalam Sistem Hukum Indonesia", dalam Seminar Pembuktian dan Penanganan Cybercrime di Indonesia, FHUI Jakarta, 2007, hlm. 12.

²⁰ Alfiyan Umbara dan Dian Alan Setiawan, "Analisis Kriminologis terhadap Peningkatan Kejahatan Siber di Masa Pandemi Covid-19", Jurnal Riset Ilmu Hukum, 2(2), 2022, hlm. 81-88.

²¹ Evelyn Angelita Pinondang Manurung dan Emmy Febriani Thalib, "Tinjauan Yuridis Perlindungan Data Pribadi Berdasarkan UU Nomor 27 Tahun 2022", Jurnal Hukum Saraswati, hlm. 139-148

²² Zenifa Siti Hafsyari, dkk. "Korban Deepfake Pornografi Evaluasi Efektivitas Hukum Positif Dan Kebutuhan akan Reformasi Hukum"

pemidanaan secara fakultatif atau terhadap perbuatan tertentu saja dari tiga jenis perbuatan tersebut. Oleh karena itu, setiap penggunaan kecerdasan buatan dengan tujuan atau maksud menyebarkan informasi yang berbau pornografi atau mengandung unsur pornografi atau bahkan membuat konten dimaksud dengan menggunakan bantuan kecerdasan buatan yang disebarkan melalui media elektronik apapun sepanjang masih diselenggarakan atau diinstruksikan oleh manusia, dapat dikenakan sanksi pidana atasnya menurut hukum positif Indonesia yang dalam hal ini adalah Undang-Undang Informasi dan Transaksi Elektronik dan peraturan turunannya serta berbagai peraturan perundangan lainnya yang mengatur terkait pornografi di Indonesia.²³

Undang - Undang Nomor 1 Tahun 2024 tentang Informasi dan Transformasi Elektronik pasal 27 ketentuan hukum yang paling terkait dan memenuhi persyaratan dalam kasus *deepfake* pornografi , karena pasal tersebut secara spesifik menyinggung informasi elektronik atau dokumen elektronik terkait penyebaran konten pornografi melalui teknologi *deepfake*.

Tindakan pornografi yang mengkolaborasikan teknologi kecerdasan buatan tidak diatur secara gramatikal dalam Undang-Undang Informasi dan Transaksi Elektronik. Implementasi Undang-undang Informasi dan Transaksi Elektronik (UU ITE) juga mengalami beberapa tantangan atau hambatan sebab sulit untuk melakukan pembuktian hukum dan memperoleh bukti yang cukup untuk menuntut pelaku karena kompleksitas teknologi yang rumit dapat menyembunyikan jejak digital mereka, membuat para aparat penegak hukum sulit untuk mengidentifikasi dan menuntut pelaku. Selain itu, tantangan penerapan Undang-Undang Informasi dan Transaksi Elektronik pada kasus *deepfake* juga harus memperhatikan keseimbangan antara perlindungan privasi dan kebebasan berekspresi karena perlindungan terhadap korban harus diupayakan tanpa mengorbankan hak privasi dan kebebasan berekspresi individu secara luas.

Deepfake pornografi berhubungan dengan tindak kriminal pornografi, Pelarangan penyebarluasan muatan pornografi diatur dalam Pasal 4 ayat (1) Undang- Undang Pornografi, yaitu: Setiap orang dilarang memproduksi, membuat, memperbanyak, menggandakan, menyebarkan, menyiarkan, mengimpor, mengekspor, menawarkan, memperjualbelikan,

menyewakan, atau menyediakan pornografi yang secara eksplisit memuat: a. persenggamaan, termasuk persenggamaan yang menyimpang; b. kekerasan seksual; c. masturbasi atau onani; d. ketelanjangan atau tampilan yang mengesankan ketelanjangan; e. alat kelamin; atau f. pornografi anak

Di dalam Kitab Undang Hukum Pidana Indonesia, ketetapan tentang aksi pidana pornografi juga tercantum dalam bagian keempat belas tentang Kejahatan Terhadap Kesusilaan yang meliputi Pasal 281 hingga Pasal 283 KUHP. Pornografi tergolong dalam aksi pidana yang menyalahi norma kesusilaan. Kejahatan terhadap kesusilaan dalam hukum pidana di Indonesia telah diatur dalam Pasal 281 dan Pasal 282 KUHP. Dalam Pasal 281 KUHP: “Mengancam para pelaku dengan ancaman pidana paling lama 2 (dua) tahun 8 (delapan) bulan atau pidana denda paling banyak Rp. 400.000,- (empat ratus ribu rupiah) yaitu barang siapa dengan sengaja dan terbuka melanggarkesusilaan dan barang siapa dengan sengaja dan di depan orang lain yang ada di situ bertentangan dengan kehendaknya, melanggar kesusilaan.”

B. Penegakan Hukum terhadap Penyalahgunaan kecerdasan buatan dengan cara memanipulasi wajah seseorang ke dalam gambar atau video porno

Sebagai sebuah negara yang berlandaskan hukum, Indonesia memiliki regulasi terkait pornografi yang di atur baik dalam Kitab Hukum Pidana maupun Undang-Undang khusus.

Lembaga yang memiliki peran yang sangat penting adalah Badan Siber dan Sandi Negara (BSSN). BSSN merupakan salah satu lembaga yang ada di Indonesia dan perlu melakukan evaluasi pelaksanaan Sistem Pemerintahan Berbasis Elektronik (SPBE). Berdasarkan Peraturan Presiden Nomor 28 Tahun 2021 tentang Badan 2021 tentang Badan Siber dan Sandi Negara atau BSSN, Lembaga ini memiliki tugas pokok dalam melaksanakan urusan pemerintahan di sektor keamanan siber dan persandian untuk memberikan dukungan kepada Presiden dalam menjalankan tugas pemerintahan negara. Sebagai bagian dari tanggung jawab utamanya, Badan Siber dan Sandi Negara atau BSSN menyediakan berbagai layanan public elektronik dan aplikasi berbasis internet, antara lain Sistem Akuntabilitas Kinerja Instansi Pemerintah (SAKIP), Jaringan

²³ Raisa Safinah, “Kajian Yuridis Penggunaan Kecerdasan Artifisial pada Pembuatan dan Penyebaran Konten Pornografi di Media Sosial dalam Hukum Positif

Indonesia”. MANDUB: jurnal Politik, Sosial, Hukum dan Humaniora. Vol 2, hlm 302-313

Dokumentasi dan Instansi Hukum (JDIH), absen elektronik, Sistem Informasi Kepegawaian (SIMPEG0, *e-mail*, website, portal, *Secure Ekectronic Document Management System* (SEDMS), dan Sistem Informasi Manajemen Aset (SIMAS). Tugas pengelolaan seluruh data dari aplikasi- aplikasi tersebut secara terpusat berada di bawah tanggung jawab Badan Siber dan Sandi Negara atau BSSN²⁴

Dalam KUHP Indonesia, Tindak Pidana Pornografi diatur Bab XIV tentang Kejahatan Terhadap Kesusilaan dalam pasal 281- 283 KUHP. Pornografi merupakan kejahatan yang termasuk golongan tindak pidana melanggar (*zedelijkheid*).

Pasal 281 Kitab Undang-undang Hukum Pidana disebutkan bahwa:

Diancam dengan pidana penjara paling lama dua tahun delapan bulan atau pidana denda paling banyak empat ribu lima ratus rupiah:

ke-1 barang siapa dengan sengaja dan terbuka melanggar kesusilaan;

ke-2 barang siapa dengan sengaja dan di depan orang lain yang ada di situ bertentangan dengan kehendaknya, melanggar kesusilaan.

Selain itu delik yang berkaitan dengan pornografi juga diatur dalam Pasal 282 KUHP, yang bunyinya sebagai berikut:

- 1) Barangsiapa menyiarkan, mempertunjukkan atau menempelkan, gambaran atau benda, yang diketahui isinya dan melanggar kesusilaan, atau barangsiapa dengan maksud untuk disiarkan, dipertunjukkan atau ditempelkan di muka umum, membikin tulisan, gambaran atau benda tersebut, memasukkan ke dalam negeri, meneruskannya, mengeluarkannya dari negeri, atau mempunyai dalam persediaan, ataupun barangsiapa secara terang-terangan atau dengan mengedarkan surat tanpa diminta, menawarkannya atau menunjukkannya sebagai bisa didapat. Diancam dengan pidana penjara paling lama satu tahun enam bulan atau denda paling tinggi tiga ribu rupiah.
- 2) Barangsiapa menyiarkan, mempertunjukkan atau menempelkan di muka umum tulisan, gambaran atau benda yang melanggar kesusilaan atau barangsiapa dengan maksud" untuk disiarkan, dipertunjukkan atau ditempelkan di muka umum, membikinnya, memasukkannya ke dalam negeri, meneruskan, mengeluarkannya dan negeri atau mempunyai dalam persediaan, atau

barangsiapa secara terang-terangan atau dengan mengedarkan surat tanpa diminta, menawarkan atau menunjukkan sebagai bisa didapat, diancam jika ada alasan kuat baginya untuk menduga bahwa tulisan, gambaran atau benda itu melanggar kesusilaan dengan pidana penjara paling lama sembilan bulan atau denda paling banyak tiga ratus rupiah.

- 3) Kalau yang bersalah, melakukan kejahatan tersebut dalam ayat pertama, sebagai pencaharian atau kebiasaan, dapat dijatuhi pidana penjara paling lama dua tahun delapan bulan atau denda paling banyak lima ribu rupiah.

Penyalahgunaan *deepfake* dengan menggabungkan foto atau video salah satunya dapat berupa konten pornografi, Kasus Putusan Nomor 125/Pid.sus/2019/PN Bjn yang terjadi di Desa Beji RT. 01 RW. 01 Kecamatan Kedewan Kabupaten Bojonegoro atas nama Terdakwa Eko Purwanto Als Mblu Bin Kasmin, Tempat/tgl Lahir: Bojonegoro, 25 Maret 1984, Jenis Kelamin: Laki-laki, Kebangsaan: Indonesia, Tempat Tinggal: Desa Beji RT. 01 RW. 01 Kecamatan Kedewan Kabupaten Bojonegoro, Agama: Islam, Pekerjaan: Jurnalis, dikenakan Pasal 29 dalam Putusan Nomor 125/Pid.Sus/2019/PN Bjn

Dalam kasus tersebut, Terdakwa Eko Purwanto Alias Mazblupada tahun 2019 di warung Desa Kedewan Kecamatan Kedewan Kabupaten Bojonegoro dan di DesaBeji Kecamatan Kedewan Kabupaten Bojonegoro telah melanggar Undang-undang no 19 tahun 2016 pasal 29 yaitu "dengan sengaja dan tanp hak mengirimkan Informatika Elektronik dan / atau Dokumen Elektronik yang berisi ancaman kekerasan atau menakut –nakuti yang ditujukan secara pribadi",dengan perbuatan sendiri tanpa bantuan orang lain berikut kejahatan yang dilakukan terdakwa dengan cara sebagai berikut :

Terdakwa menggunakan akun Facebook Bernama Mazblu ketika berada disebuah warung Desa Kedewan Kecamatan KedewanKabupaten Bojonegoro, ia membuka Facebook dan kemudian mencatat nomor WhatsApp atas nama Eny Nur Alisa, tata Nur Diana, Putri Nur Sela, Mariyatul Qibthiyah, Jovi Lidyawati, Rina Dewi Angraenidi Hand Phone milik terdakwa lalu terdakwa menghubungi para saksi.karena tidak dihiraukan terdakwa membuka aplikasi Google yaitu " kemudian muncul gambar perempuan bugil dengan beberapa poseyang menggoda. Kemudian

²⁴ Jefferson Benyamin et al., "Manajemen Resiko Keamanan Informasi dalam Meminimalisasi Ancaman Siber pada Pusat Data dan Teknologi Informasi Komunikasi Badan

Siber dansandi Negara Guna Meningkatkan Pertahanan dan Keamanan Siber", 9(1), 2023, hlm. 40-54

terdakwa tanpa sepengetahuan dari para saksi telah mengambil foto dari facebook para saksi lalu fotonya terdakwa di edit dan dipindahkan ke aplikasi "FriendBlender" sehingga secara otomatis wajah dari para saksi menyatu dengan bagian tubuh yang bergambar pose wanita bugil. Saksi Eny Nur Alisa pada tanggal 02 februari 2019 sekitar pukul 14.40 Wib di rumahnya Desa Dolokgede Kecamatan Tambakrejo Kabupaten Bojonegoro, terkejut ketika membuka WhatsApp dari nomor 085784620762 yaitu terdakwa eko purwanto yang mengaku bernama Rio, saksi Eny mendapat kiriman 4 (empat) foto bugil yang wajahnya mirip dengan wajahnya lalu disertai ancaman akan menyebarkan foto bugil tersebut di media sosial apabila saksi berusaha memblokir nomor terdakwa. Halini juga terjadi pada saksi Tata Nur Diana pada tanggal 1 Februari 2019 sekitar pukul 13.00 Wib mendapat kiriman 2 (dua) foto bugil dengan disertai ancaman akan menyebarkan foto tersebut apabila tidak membalas pesan pribadi dari nomor 085784620762 yaitu terdakwa eko purwanto yang mengaku bernama Antok. Sama halnya dengan Saksi Putri Nur Sela pada tahun 2019 juga menerima kiriman 2 (dua) foto bugil dengan nomor WhatsApp 085784620762 atas nama Antok. Saksi Mariyatul Qibthiyah tanggal 12 Pebruari 2019 sekitar pukul 13.00 Wib menerima foto bugil yang wajahnya mirip dengan dirinya disertai ancaman akan menyebarkan foto tersebut dari orang yang tidak dikenal dengan nomor WhatsApp 081216084993. Saksi Jovi Lidyawati pada tanggal 29 Januari 2019 sekitar pukul 11.30 Wib menerima pesan dari nomor 085784620762 berupa 2 (dua) foto bugil dengan wajah mirip saksi disertai ancaman akan menyebarkan foto bugil, kemudian Saksi Rina Dewipada tanggal 29 Januari 2019 menerima kiriman 3 (tiga) foto bugil yang wajahnya mirip dengan dirinyadari nomor 085784620762 dengan ancaman akan menyebar luaskan foto tersebut. Dan juga terjadi pada saksi Nila Nurangraini di HandPhononya menerima kiriman foto bugil yang wajahnya mirip denganya dari WhatsApp

Dalam amar putusan kasus tersebut, majelis hakim memandang adil apabila terdakwa Eko Purwanto dijatuhi hukuman sebagaimana yang disebutkan dalam amar putusan berikut:

1. Menyatakan Terdakwa Eko Purwanto Alias MazbluBin Kasmin, terbukti secara sah dan bersalah melakukan tindak pidana dengan sengaja dan tanpa hak mengirimkan informasi elektronik yang berisi menakut-nakuti yang ditujukan secara pribadi beberapa kali sebagaimana dalam dakwaan kesatu primair.

2. Menjatuhkan pidana kepada Terdakwa dengan pidana penjara selama 1 (satu) tahun 4 (empat) bulan dan denda sejumlah Rp 60.000.000,00 (enam puluh juta rupiah) dengan ketentuan apabila denda tersebut tidak dibayar diganti dengan pidana kurungan selama 1 (satu) bulan.
3. Menetapkan masa penangkapan dan penahanan yang telah dijalani terdakwa dikurangkan seluruhnya dari pidana yang dijatuhkan\
4. Menetapkan Terdakwa tetap ditahan
5. Menetapkan barang bukti berupa:
 - a) 1 (satu) buah HP merk Samsung Type J2 Prime warna hitam beserta dusbook merk Samsung type J2 Prime warna hitam, dirampas untuk Negara.
 - b) 1 (satu) bungkus perdana simpati tertera nomor 081216084993 di rampas untuk dimusnahkan
6. Membebaskan kepada Terdakwa membayar biaya perkara Rp. 2.000 (dua ribu rupiah).

Karena dakwaan dari Penuntut Umum bersifat gabungan alternatif subsidiaritas, maka setelah dakwaan Kesatu Primair terpenuhi, dakwaan selanjutnya tidak perlu dipertimbangkan. Berdasarkan fakta-fakta yang terungkap selama persidangan dalam perkara ini, Majelis Hakim tidak menemukan alasan yang dapat membebaskan terdakwa dari tanggung jawab pidana, baik sebagai alasan pembenar maupun alasan pemaaf. Oleh karena itu, Majelis Hakim menyimpulkan bahwa tindakan terdakwa harus dipertanggungjawabkan. Sebelum menjatuhkan pidana kepada terdakwa, perlu dipertimbangkan terlebih dahulu faktor-faktor yang memberatkan dan meringankan.

1. Keadaan yang memberatkan : Perbuatan Terdakwa telah merugikan secara immateriil saksi korban Eny Nur Alisa Binti Muntari, saksi Tata Nur Diana Binti Hamim, saksi Jovi Lidyawati binti Kuswo, saksi Rina Dewi Anggreani Binti Suparwo, dan saksi Nila Nungraini binti Kariman.
2. Keadaan yang meringankan : Terdakwa bersikap sopan dipersidangan; terdakwa mengakui perbuatannya dan berjanji untuk tidak mengulangi perbuatannya; terdakwa belum pernah dihukum.

Dalam memeriksa perkara ini, Majelis Hakim Pengadilan Negeri Bojonegoro tidak mengalami kesulitan karena keterangan dari saksi-saksi dan terdakwa semuanya sejalan dengan apa yang dijelaskan dalam surat dakwaan dari Penuntut Umum. Selain itu, terdakwa juga mengakui perbuatannya dan mengonfirmasi bahwa semua

barang bukti yang diajukan di persidangan adalah miliknya. Berdasarkan fakta hukum yang terungkap di lapangan dan pertimbangan yang cermat, Hakim memutuskan untuk menjatuhkan hukuman yang lebih ringan daripada tuntutan Jaksa Penuntut Umum

Dalam kasus tersebut, Terdakwa dijatuhi hukuman penjara selama 1 (satu) tahun dan 4 (empat) bulan, dengan ketentuan bahwa seluruh waktu yang dihabiskan Terdakwa dalam tahanan akan dikurangkan dari hukuman yang dijatuhkan. Tindak pidana yang terbukti dalam pasal tersebut adalah tindak pidana di bidang Informasi dan Transaksi Elektronik, di mana Terdakwa dengan sengaja dan tanpa hak mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi ancaman kekerasan atau menak-nakuti secara pribadi, sebagaimana diatur dalam Pasal 29 Undang-Undang No. 11 Tahun 2008.

Dalam kasus tersebut dalam penegakan atau efek jera terhadap terdakwa masih belum tepat yang Dimana penjatuhan hukuman terhadap Eko Purwanto masih ringan, hakim tidak memperhatikan segala perbuatan terdakwa yang sangat merugikan para korban.

Perbuatan foto rekayasa merupakan tindak pidana apabila hasil dari foto rekayasa tersebut digunakan untuk kepentingan-kepentingan yang dapat merugikan atau menyebabkan adanya korban. Rekayasa foto yang digunakan untuk kegiatan yang bersifat tindak pidana dapat menimbulkan beberapa tindak pidana yang sangat merugikan saksi²⁵. Tindakan memanipulasi, menciptakan, atau mengubah Informasi Elektronik dan/atau Dokumen Elektronik dengan maksud agar dianggap sebagai data yang sah, seperti pembuatan foto rekayasa yang mengandung unsur pornografi, merupakan tindak pidana yang diatur dalam Pasal 35 jo Pasal 51 Ayat (1) Undang-Undang Nomor 19 Tahun 2016 tentang Informasi Teknologi dan Elektronik, yang mengatur hal tersebut sebagai berikut:

Pasal 35 *“Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik”*.

Dalam Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), salah satu ketentuan hukum yang paling terkait dan memenuhi persyaratan dalam kasus pembuatan/ penyebarluasan deepfake pornografi, pasal 27 ayat (1) UU ITE Jo. Pasal 45 ayat (1) *“Setiap Orang dengan sengaja dan tanpa hak menyiarkan, mempertunjukkan, mendistribusikan, mentransmisikan, dan/atau membuat dapat diaksesnya Informasi Elektronik dan/ atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan untuk diketahui umum sebagaimana dimaksud pasal 27 ayat (1) di pidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp 1.000.000.000.00 (satu miliar rupiah)”*. Salah satu ketentuan hukum yang paling terkait dan memenuhi persyaratan dalam kasus deepfake pornografi, karena pasal tersebut secara spesifik menyinggung informasi elektronik atau dokumen elektronik terkait penyebaran konten pornografi melalui teknologi deepfake. Pasal 27 ayat (1) lebih fokus pada individu yang menyebarkan konten pornografi tersebut²⁶,

Hal lain yang perlu digaris bawahi adalah tidak semua orang menginginkan potret dirinya digunakan untuk keperluan tertentu apalagi dijadikan alat pengancam dan menak-nakuti, karena dapat mengganggu atau merendahkan reputasi. Apabila subjek yang dijadikan foto rekayasa bermuatan pornografi merasa kehormatan atau reputasinya dirugikan maka barulah dianggap muncul pelanggaran terhadap hak moral. Dengan demikian dapat disimpulkan bahwa perbuatan membuat foto rekayasa bermuatan pornografi melalui platform digital merupakan pelanggaran hak cipta yaitu pada hak moral apabila menggunakan potret milik orang lain tanpa izin dari pemiliknya²⁷.

Dasar Hakim dalam menjatuhkan putusan berdasarkan Pasal 29 Undang-Undang Informasi dan Transaksi Elektronik mengenai pengancam dan penakutan terhadap Terdakwa adalah karena Hakim hanya mempertimbangkan Dakwaan Penuntut Umum yang bersifat alternatif, tanpa memperhatikan ketentuan dalam Dakwaan lainnya. Di sisi lain, putusan hakim kurang memberatkan jika Terdakwa hanya dijatuhi

²⁵ Anies Mahanani, Sulistyanta, *Tinjauan Yuridis Tindak Pidana Pengancam dengan Foto Rekayasa Bermuatan Pornografi (STUDI PUTUSAN NOMOR: 125/PID.SUS/2019/PN BJJ)* (11), Hal 39.

²⁶ Olivia Novera, Yenny Fitri z, *“Analisis Pengaturan Hukum Pidana terhadap Penyalahgunaan Teknologi Manipulasi Gambar (Deepfake) dalam Penyebaran Konten Pornografi*

Melalui Akun Media Sosial, Jurnal Pemikiran dan Hukum Islam (10) 468, 2024

²⁷ Anies Mahanani, Sulistyanta, *Tinjauan Yuridis Tindak Pidana Pengancam dengan Foto Rekayasa Bermuatan Pornografi (STUDI PUTUSAN NOMOR: 125/PID.SUS/2019/PN BJJ)* (11), Hal 44.

hukuman berdasarkan pasal tersebut, karena dianggap terlalu ringan sehingga tidak berdampak signifikan terhadap Korban. Terdakwa melakukan beberapa tindak pidana yang seharusnya lebih tepat dan secara langsung merugikan Korban, terutama jika dilihat dari motif terdakwa. Dalam perkara ini, serta bukti-bukti yang terungkap selama persidangan, tindakan Terdakwa mencakup Pembuatan Foto Rekayasa yang bermuatan pornografi diatur pada Pasal 35 jo Pasal 51 Ayat (1) Undang-Undang Informasi dan Transaksi Elektronik dan Pembuatan Pornografi diatur pada Pasal 4 jo Pasal 29 Undang-Undang Pornografi, dan pengancaman melalui media sosial diatur pada Pasal 29 jo Pasal 45B Undang-Undang Informasi dan Transaksi Elektronik.

Dalam hukum pidana, jika terdakwa melakukan lebih dari satu tindak pidana atau beberapa tindak pidana secara perbarengan dikenal dengan istilah *concursum* yang tercantum dalam pasal KUHP

Terdakwa telah melakukan serangkaian tindak pidana (*Concursum*) sebagaimana diatur dalam Pasal 65 KUHP, yaitu *Concursum Realis* yang melibatkan beberapa tindak pidana pemalsuan informasi/dokumen elektronik Pasal 35 jo Pasal 51 Ayat (1) Undang-Undang ITE. Selain itu, berdasarkan kronologi kasus dan fakta-fakta yang terungkap Putusan Hakim juga akan lebih tepat jika Hakim mempertimbangkan dan menjatuhkan hukuman kepada Terdakwa berdasarkan Dakwaan Kedua dari Penuntut Umum, yang diatur dan diancam pidana dalam Pasal 29 Undang-Undang Republik Indonesia Nomor 44 Tahun 2008 tentang Pornografi jo Pasal 65 Ayat (1) KUHP, terkait dengan produksi, pembuatan, perbanyakan, penggandaan, penyebarluasan, atau penyediaan pornografi melalui aplikasi chatting, dengan ancaman hukuman penjara minimal 6 (enam) bulan dan maksimal 12 (dua belas) tahun. Pasal-pasal tersebut dianggap lebih tepat untuk diterapkan karena keduanya secara langsung merugikan Korban dan sesuai dengan motif kejahatan Terdakwa yang memang sejak awal berniat untuk menakut-nakuti Korban melalui ancaman. Di sisi lain, penerapan sistem Perbarengan Pidana/*Concursum* berdasarkan kedua pasal tersebut juga akan lebih memberatkan hukuman yang dijatuhkan, dan bahwa hal ini sebanding dengan tindakan Terdakwa serta semua kerugian yang dialami oleh Korban.

Selanjutnya, dalam kasus ini, Hakim juga perlu memberikan sanksi yang sesuai bagi Terdakwa yang telah melakukan tindak pidana

gabungan (*Concursum*). Mengingat berbagai tindak pidana yang dilakukan oleh Terdakwa, teori pemidanaan yang tepat adalah Sistem Absorpsi Dipertajam. Dalam sistem ini, hukuman yang dijatuhkan adalah yang terberat, tetapi harus ditambah dengan sepertiga dari maksimum hukuman terberat yang ditentukan. Dengan kata lain, jika diancam dengan pidana pokok sejenis, maka hanya satu pidana yang dikenakan, dengan ketentuan bahwa jumlah maksimum pidana tidak boleh melebihi jumlah maksimum terberat ditambah sepertiganya. Sistem ini diterapkan untuk gabungan tindak pidana berganda dengan ancaman hukuman pokok yang sejenis. Dasar yang digunakan adalah Pasal 65 KUHP.

Oleh karena itu, Terdakwa seharusnya dijatuhi pidana berdasarkan Pasal 35 jo Pasal 51 Ayat (1) dan Pasal 4 Undang-Undang Nomor 44 Tahun 2008 tentang Pornografi jo Pasal 65 KUHP, dengan ancaman hukuman penjara maksimal selama 16 tahun atau denda sebesar Rp. 12.000.000.000,- (dua belas miliar rupiah)

PENUTUP

A. Kesimpulan

1. Perkembangan teknologi kecerdasan buatan (*Artificial Intelligence*) di era digital membawa peluang dan tantangan baru dalam kriminologi, terutama terkait penyalahgunaan seperti *deepfake* pornografi dan pencurian data pribadi. Di Indonesia, penyebab ketidakselesaian kasus-kasus ini adalah kurangnya pengaturan komprehensif untuk perlindungan data pribadi, serta tidak adanya harmonisasi antara lembaga pemerintah. Hal ini mengakibatkan penegak hukum ragu dalam menerapkan sanksi, menciptakan ketidakpastian hukum, dan menyulitkan korban untuk mengajukan tuntutan. UU ITE yang ada saat ini tidak mencakup pelaku pembuatan video *deepfake* pornografi.
2. Hukuman seharusnya dapat menghentikan tindak pidana penyalahgunaan *deepfake*. Namun, kekurangan undang-undang yang jelas tentang *deepfake* dapat menyebabkan ketidakpastian hukum. Hal ini disebabkan oleh ketidakjelasan tentang cara mencegah dan menanggulangi kejahatan *deepfake* dan kecerdasan buatan. Dalam kasus tersebut Hakim tidak mempertimbangkan motif Terdakwa dalam melakukan pembuatan foto rekayasa yang bermuatan pornografi untuk tujuan pengancaman. Pasal yang diterapkan dianggap terlalu jauh dan tidak berdampak signifikan terhadap Korban. Seharusnya,

Hakim lebih memperhatikan Pasal 29 Undang-Undang Republik Indonesia Nomor 44 Tahun 2008 tentang Pornografi yang terdapat dalam Dakwaan Subsidiar Penuntut Umum, serta menghukum Terdakwa atas pemalsuan informasi/dokumen elektronik yang diatur dalam Pasal 51 Ayat (1) jo Pasal 35 Undang-Undang ITE. Selain itu, dari berbagai tindakan yang dilakukan oleh Terdakwa, Hakim juga seharusnya menerapkan ketentuan Concursus dengan sistem pemidanaan Absorpsi Dipertajam untuk mencapai keadilan.

B. Saran

1. Sangat penting bagi pemerintah untuk membenahi, memperbarui, atau bahkan merancang peraturan baru guna memberantas kasus *deepfake* pornografi yang semakin meningkat. Pentingnya peraturan yang mengatur penggunaan kecerdasan buatan, terutama Algoritma *deepfake* dapat melindungi kerahasiaan informasi pribadi seseorang, teknologi *deepfake* merupakan salah satu kemajuan teknologi yang berdampak langsung pada data pribadi. Sampai saat ini, hukum positif Indonesia hanya dapat menjangkau aspek pengaturan kecerdasan buatan di beberapa jenis kecerdasan buatan saja, yaitu kecerdasan buatan yang Semi Otomatis dan kecerdasan buatan yang Sepenuhnya Otomatis karena masih melibatkan campur tangan manusia dalam hal masih didahului dengan pemberian instruksi
2. Perlu adanya kriminalisasi terkait penyalahgunaan aplikasi *deepfake*, mengingat penyalahgunaan *deepfake* memiliki dampak yang cukup signifikan dalam masyarakat, selain itu penetapan penyalahgunaan *deepfake* sebagai tindak pidana juga perlu diperhatikan, adanya tindak lanjut terkait hal tersebut maka pelaku dapat mempertanggungjawabkan perbuatannya sesuai dengan aturan hukum yang bersangkutan, dan Memberikan pemahaman dan keahlian pada aparat penegak hukum terkait upaya pencegahan.

DAFTAR PUSTAKA

Buku

- Adami Chazawi, *Tindak Pidana Pornografi*, (Malang: Bayumedia Publishing, 2013)
- Agus Raharjo, *Cyber Crime, Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, (Bandung: Citra Aditya Bakti, 2002).

- APJII, "Penetrasi dan Profil Perilaku Pengguna Internet Indonesia", di akses 20 Desember 2023
- Asrini Hanifah, "Pengaturan Penegakan Hukum Terhadap Pornografi di Internet (Cyberporn) Sebagai Kejahatan Mayantara", 2009
- Barda Nawawi Arief, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan*, (Jakarta: Kencana Predana Media Group, 2007).
- Barda Nawawi Arief, *Tindak Pidana Mayantara: Perkembangan Kajian Cybercrime di Indonesia*, (Jakarta: Raja Grafindo Persada, 2006)
- Dr. Sahat Maruli T. Situmeang, S.H., M.H, *Cyber Law*, (Bandung: Penerbit Cakra, 2020).
- Muhammad Isnaeni Puspito Adhi, S.H. M.H, Muhammad Widya Iswara Rizky Anugerah, S.H., M.Kn & Dr. Agus Wibowo, S.H., M.Si, *Kebijakan Hukum Pidana Dalam Upaya Penanggulangan Kejahatan Pornografi Online (Cyberporn) Di Indonesia*, (Semarang: STIEPARI Press, 2023).
- Soerjono Soekanto, *Faktor-faktor yang Mempengaruhi Penegak Hukum*. (Jakarta: Rajawali Pers, 2014)
- Petrus Golose, "Penegakan Hukum Cybercrime dalam Sistem Hukum Indonesia", dalam Seminar Pembuktian dan Penanganan Cybercrime di Indonesia, FHUI Jakarta, 2007, hlm. 12.
- Prof. Dr. Maskun, S.H, LL.M, *Cyber Law Kebijakan di Era Transformasi Digital*, (Refika, 2023)
- Wahid, Abdul dan Mohammad Labib, *Kejahatan Mayantara (Cyber Crime)*. (Jakarta: PT. Refika Aditama, 2005)

Jurnal

- Alfiyan Umbara dan Dian Alan Setiawan, "Analisis Kriminologis terhadap Peningkatan Kejahatan Siber di Masa Pandemi Covid-19", *Jurnal Riset Ilmu Hukum*, 2 (2), 2022, hlm. 81-88.
- Antika Setia Dewi dan Dian Alan Setiawan (2024). Penegakan Hukum terhadap Pelaku Video *Deepfake* Porn Dihubungkan dengan Hukum Pidana Positif di Indonesia. *Bandung Conference Series: Law Studies*, 4(1) 510-514.
- Andreas Agung, Hafrida, Erwin, "Pencegahan Kejahatan Terhadap CyberCrime",

- PAMPAS: Journal of Criminal, Vol.3 No.2 (2022).
- Arief Bakhtiar Darmawan, “Kedaulatan Negara dalam Kepemilikan Data Digital: Analisis Langkah Strategis Australia Menghadapi Facebook dan Google” *Jurnal Hubungan Internasional*, 16 (1), 2023, hlm. 221-228
- Eva Istia Utaw dan Neni Ruhaeni (2023, Januari) Penegakan Hukum Terhadap Tindak Pidana Pornografi Menurut Peraturan Perundang-Undangan Tentang Pornografi Melalui Media Sosial, Bandung Conference Series: Law Studies, Vol. 3 (1).
- Evelyn Angelita Pinondang Manurung dan Emmy Febriani Thalib, “Tinjauan Yuridis Perlindungan Data Pribadi Berdasarkan UU Nomor 27 Tahun 2022”, *Jurnal Hukum Saraswati*, hlm. 139-148
- Floridi, L., et al. (2018). AI4People—An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations. *Minds and Machines*, 28(4), 689-707
- Izil Hidayat Putra, Perlindungan Hukum Terhadap Korban Penyalahgunaan Artificial Intelligence (AI) Berupa Deepfake Pornografi Menurut Peraturan Perundang-Undangan, *UNJA Journal of Legal Studies*, 30 Juni 2023, 1 (2), 110-128
- Jacqueline M. Drew “A study of cybercrime victimization and prevention: Exploring the use of online crime prevention behaviours and strategies”, *Journal of Criminological Research, Policy and Practice*, 6(1), 2020, hlm. 17-33.
- Kasita, I. D. 2022. "Deepfake Pornografi Tren Kekerasan Gender Berbasis Online (KGBO) Di Era Pandemi Covid-19. *Jurnal Wanita Dan Keluarga*, 3 (1), Juli 2022, 20
- Mandlenkosi Richard Mphatheni dan Witness Maluleke, "Cybersecurity as a response to combating cybercrime: Demystifying the prevailing threats and offering recommendations to the African regions", *International Journal of Research in Business and Social Science* (2147-4478), 11(4), 2022, hlm. 384-396.
- Muhammad Faqih Faathurrahman dan Enni Soerjati Priowirjanto (2022, November). Pengaturan Pertanggungjawaban Pelaku Penyalahgunaan *Deepfakes* Dalam Teknologi Kecerdasan Buatan Pada Konten Pornografi Berdasarkan Hukum Positif Indonesia, *Jurnal Indonesia Sosial Teknologi*, Vol. 3, No. 11.
- Olivia Novera, Yenny Fitri z, “Analisis Pengaturan Hukum Pidana terhadap Penyalahgunaan Teknologi Manipulasi Gambar (Deepfake) dalam Penyebaran Konten Pornografi Melalui Akun Media Sosial, *Jurnal Pemikiran dan Hukum Islam* (10) 468, 2024
- Raisa Safinah, “Kajian Yuridis Penggunaan Kecerdasan Artifisial pada Pembuatan dan Penyebaran Konten Pornografi di Media Sosial dalam Hukum Positif Indonesia”. *MANDUB: jurnal Politik, Sosial, Hukum dan Humaniora*. Vol 2, hlm 302-313.
- Shannon Gandrova dan Ricky Banke (2023, November). Penerapan Hukum Positif Indonesia Terhadap Kasus Kejahatan Dunia Maya *Deepfake*, *Jurnal Ilmiah Multidisiplin*, Volume 1, Nomor 10.
- Sulistiyanta (2006). Problem Penegakan Hukum Tindak Pidana Pornografi di Era Global, *Jurnal Ilmu Hukum*, Volume 9 Nomor 1.
- Sutojo, T. Kecerdasan Buatan. Edisi Pertama. (ANDI OFFSET. Bandung, 2011), 3.
- Yolanda Frisky Amelia, Arfan Kaimuddin dan Hisbul Luthfi Ashsyarofi (2024, Januari). Pertanggungjawaban Pidana Pelaku Terhadap Korban Penyalahgunaan Artificial Intelligence *Deepfake* Menurut Hukum Positif Indonesia, *Jurnal Dinamika*, Volume 30 No. 1.
- Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. *International Data Privacy Law*, 7(2), 76-99
- Zenifa Siti Hafsyari, dkk. “Korban Deepfake Pornografi Evaluasi Efektivitas Hukum Positif Dan Kebutuhan akan Reformasi Hukum”

Peraturan Perundang-Undangan

- Kitab Undang-Undang Hukum Pidana Indonesia
- Undang-Undang No. 44 Tahun 2008 Tentang Pornografi
- Undang-Undang No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik
- Undang-Undang No. 1 Tahun 2024 Tentang Informasi dan Transaksi Elektronik
- Undang-Undang No. 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik
- Undang-Undang No 12 Tahun 2022 Tentang Tindak Pidana Kekerasan Seksual