

Implikasi Hukum terhadap Penyalahgunaan Teknologi Deepfake untuk Pemerasan (Sextortion) dalam Perspektif Hukum Teknologi Informasi di Indonesia

Wayan Zenitia Devi¹

Program Studi Ilmu Hukum, Fakultas Hukum dan Ilmu Sosial, Universitas Pendidikan Ganesha, Singaraja

*Penulis korespondensi: zenitia@student.undiksha.ac.id¹

Abstract. *The development of deepfake technology, which utilises artificial intelligence to manipulate images, videos and sounds, has led to a serious threat of sextortion. In the Indonesian context, high internet penetration and low awareness of digital security increase the risk of this crime. This research analyses the legal consequences of the misuse of deepfake technology in sextortion based on the Electronic Information and Transaction Law (UU ITE). Using normative juridical methods and descriptive-qualitative analysis, this research examines the legal challenges faced in enforcing sanctions against this crime and provides recommendations to strengthen the legal framework in Indonesia. The results show that there are gaps in the legal framework that need to be addressed, as well as the importance of education and capacity building of law enforcement in dealing with cybercrime. In addition, the development of more sophisticated deepfake detection technology is expected to be a solution in tackling this abuse in the future.*

Keywords: *Cybercrime; Digital Security; Sextortion Digital; Technology Deepfake; UU ITE*

Abstrak. Perkembangan teknologi deepfake, yang memanfaatkan kecerdasan buatan untuk memanipulasi gambar, video, dan suara, telah memunculkan ancaman serius berupa pemerasan seksual (sextortion). Dalam konteks Indonesia, tingginya penetrasi internet dan rendahnya kesadaran akan keamanan digital memperbesar risiko kejahatan ini. Penelitian ini menganalisis konsekuensi hukum dari penyalahgunaan teknologi deepfake dalam sextortion berdasarkan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Dengan menggunakan metode yuridis normatif dan analisis deskriptif-kualitatif, penelitian ini mengkaji tantangan hukum yang dihadapi dalam penegakan sanksi terhadap kejahatan ini dan memberikan rekomendasi untuk memperkuat kerangka hukum di Indonesia. Hasil penelitian menunjukkan bahwa terdapat celah dalam kerangka hukum yang perlu segera ditangani, serta pentingnya edukasi dan peningkatan kapasitas penegak hukum dalam menghadapi kejahatan siber. Selain itu, pengembangan teknologi deteksi deepfake yang lebih canggih diharapkan dapat menjadi solusi dalam menanggulangi penyalahgunaan ini di masa depan.

Kata kunci: Keamanan Digital; Kejahatan Siber; Sextortion Digital; Teknologi Deepfake; UU ITE

1. LATAR BELAKANG

Kemajuan teknologi informasi dan komunikasi yang cepat dan meluas telah mengubah perilaku manusia dan peradaban global, menyebabkan dunia menjadi saling terhubung dan sangat mempercepat perubahan masyarakat. Pemanfaatan teknologi ini telah meluas ke berbagai aspek kehidupan manusia untuk memenuhi kebutuhan sehari-hari, memberikan banyak dampak positif, seperti mempercepat pertukaran informasi, mendukung penjualan dan pembelian dan beroperasi sebagai platform untuk hiburan. Namun, dampak negatif juga muncul, seperti penyebaran informasi palsu (hoaks), peretasan data (hacking), serta kemudahan akses terhadap konten digital yang mengandung unsur SARA atau asusila. Saat ini manusia hidup melalui revolusi industri keempat dan peradaban telah bertransisi ke revolusi kelima, dimana teknologi kini menjadi komponen integral dari kehidupan sehari-hari. Selain digunakan untuk berbagi informasi, teknologi juga digunakan untuk tugas sehari-hari.

Kecerdasan buatan (AI) adalah salah satu kekuatan utama di balik revolusi industri keempat. Deepfake adalah salah satu dari sekian banyak aplikasi kecerdasan buatan yang kini mendapat banyak perhatian (Faqih & Soerjati Priowirjanto, 2022).

Teknologi deepfake adalah bentuk kecerdasan buatan (Artificial Intelligence, AI) yang menggunakan algoritma pembelajaran mendalam (deep learning) untuk membuat atau mengubah konten digital, seperti audio, video, dan gambar, menjadi representasi realistis namun sintetik. Teknologi ini memanfaatkan Generative Adversarial Networks (GANs) untuk menghasilkan media yang terlihat autentik bagi manusia (Admin, 2024). Pada tahun 2017, seorang pengguna Reddit dengan nama akun "Deepfake" mengungkapkan konsep tersebut, sehingga memunculkan Deepfake. Selain memanipulasi atau memalsukan gambar dan video, deepfake juga dapat mengubah suara. Deepfake berpotensi menjadi teknologi yang sangat berguna untuk industri film dimasa depan dan digunakan untuk proses pembuatan film yang sesungguhnya. Sebagai contoh, aktor luar negeri yaitu Paul Walker dapat dihidupkan kembali dan tampil dalam film *Fast & Furious 7* (Faqih & Soerjati Priowirjanto, 2022). Teknologi ini, di satu sisi, memiliki potensi besar dalam bidang industri hiburan, pendidikan, dan komunikasi. Namun, di sisi lain, teknologi deepfake juga menghadirkan risiko besar jika disalahgunakan untuk tujuan kriminal, salah satunya adalah pemerasan seksual (sextortion).

Sextortion adalah bentuk kejahatan di mana pelaku memeras korban dengan ancaman akan menyebarkan materi yang mengandung konten seksual, seringkali berupa video atau foto yang telah dimanipulasi menggunakan teknologi deepfake. Dalam beberapa kasus, korban tidak menyadari bahwa materi tersebut sepenuhnya palsu hingga pelaku memberikan ancaman. Sextortion berbasis deepfake menjadi lebih menakutkan karena kemampuannya untuk menciptakan konten yang sangat realistis, memudahkan pelaku untuk menjebak korban dan menyebabkan tekanan psikologis yang berat. Dalam konteks Indonesia, kejahatan ini semakin memprihatinkan karena perkembangan teknologi seringkali tidak sejalan dengan kemampuan regulasi hukum untuk mengimbangnya (Syauket et al., 2024).

Di Indonesia, fenomena ini menjadi semakin mengkhawatirkan mengingat tingginya penetrasi internet dan penggunaan media sosial di kalangan masyarakat. Pada tahun 2020, Menurut data dari Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), mayoritas dari 196,7 juta pengguna internet di Indonesia menggunakan media sosial. Tingginya aktivitas online ini, ditambah dengan kurangnya kesadaran akan risiko keamanan digital, membuat masyarakat Indonesia rentan terhadap ancaman sextortion berbasis deepfake. Kasus-kasus sextortion menggunakan deepfake mulai bermunculan di berbagai negara, termasuk Indonesia. Meskipun belum ada data statistik resmi yang spesifik tentang prevalensi kasus sextortion

deepfake di Indonesia, beberapa laporan media dan kasus yang terungkap menunjukkan bahwa ancaman ini nyata dan berpotensi meningkat. Korban tidak hanya mengalami kerugian finansial, tetapi juga trauma psikologis yang mendalam, kerusakan reputasi, dan dalam beberapa kasus, bahkan berujung pada tindakan bunuh diri.

UU ITE merupakan bagian utama dari UU yang mengatur kejahatan siber di Indonesia. Tujuan UU No. 11 Tahun 2008 tentang ITE adalah untuk menyelaraskan hukum teknologi informasi nasional dan internasional. Selain itu, UU No. 19 tahun 2016 tentang perubahan atas UU No. 11 tahun 2008 bertujuan untuk memastikan bahwa hak-hak dan kebebasan orang lain diakui dan dihormati, serta untuk memenuhi tuntutan yang wajar dengan tetap memperhatikan ketertiban umum dan masalah keamanan dinegara demokrasi. UU ini juga berusaha untuk memberikan kejelasan hukum, ketertiban umum, dan keadilan (WARSITO, 2016). Namun, meskipun UU ITE dirancang untuk menangani berbagai bentuk kejahatan digital, penyalahgunaan teknologi deepfake sebagai alat pemerasan masih menjadi tantangan yang belum sepenuhnya terakomodasi dalam kerangka regulasi.

Pasal-pasal yang ada dalam UU ITE mungkin dapat diterapkan pada kasus pemerasan secara umum, tetapi teknologi deepfake menghadirkan kompleksitas yang berbeda, baik dari segi pembuktian hukum maupun penerapan sanksi. Penegak hukum juga menghadapi kesulitan dalam mengidentifikasi pelaku, mengumpulkan bukti, dan memastikan bahwa manipulasi digital tersebut memenuhi kriteria kejahatan yang dapat diproses secara hukum. Mengingat potensi dampak yang luas dan serius dari penyalahgunaan teknologi deepfake untuk sextortion, diperlukan kajian mendalam tentang konsekuensi hukum dan tantangan dalam penegakan hukum di Indonesia. Hukum di Indonesia, khususnya yang diatur dalam UU ITE akan dibahas dalam artikel ini khususnya untuk dapat diaplikasikan pada kasus penyalahgunaan teknologi deepfake untuk sextortion. Tantangan yang dihadapi oleh aparat penegak hukum dalam menangani kasus semacam ini, serta memberikan rekomendasi untuk memperkuat kerangka hukum yang ada akan dikaji dalam penelitian ini. Pentingnya pendidikan teknologi dan peningkatan kesadaran publik juga akan dibahas sebagai langkah preventif untuk melindungi masyarakat dari ancaman kejahatan berbasis deepfake di masa depan.

Perumusan Masalah

Artikel ini akan membahas berbagai permasalahan yang mencakup:

- a. Bagaimana penerapan hukum di Indonesia terhadap kasus penyalahgunaan deepfake dalam sextortion?
- b. Apa saja tantangan hukum yang dihadapi dalam menjerat pelaku sextortion berbasis teknologi deepfake?

- c. Bagaimana peran hukum teknologi informasi dalam menghadapi ancaman deepfake di Indonesia?
- d. Apa langkah-langkah preventif yang bisa diambil untuk melindungi masyarakat dari pemerasan berbasis deepfake?

2. METODE PENELITIAN

Penelitian ini menggunakan metodologi yuridis normatif, yang diterapkan melalui pendekatan perundang-undangan (statute approach), pendekatan kasus (case approach), pendekatan analisis (analytical approach), dan pendekatan perbandingan (comparative approach). Bahan hukum primer, seperti peraturan perundang-undangan yang mengikat seperti UU Nomor 11 Tahun 2008 tentang UU ITE, bahan hukum sekunder, yang merupakan bahan yang menjelaskan atau menafsirkan bahan hukum primer, seperti doktrin, karya ilmiah, jurnal, dan tulisan akademis lainnya, dan bahan hukum tersier, yang merupakan sumber yang memberikan panduan dan penjelasan terhadap bahan hukum primer dan sekunder, termasuk data-data dari internet yang relevan dengan isu yang dibahas dalam penelitian ini. Untuk memberikan gambaran yang lebih baik, pendekatan kualitatif deskriptif digunakan untuk menganalisis data.

3. HASIL DAN PEMBAHASAN

Penerapan Hukum terhadap Kasus Penyalahgunaan Deepfake dalam Sextortion di Indonesia

Saat ini, manipulasi media termasuk gambar, film, dan suara—memiliki risiko yang signifikan karena menyangkut identitas seseorang. Seiring dengan perkembangan teknologi, manipulasi media semakin mudah dilakukan menggunakan teknologi deepfake, yang merupakan bagian dari AI. Deepfake menciptakan data palsu yang meniru data asli agar tampak sah, sehingga memungkinkan manipulasi media secara realistis, termasuk gambar, film, dan suara.

Teknik ini memilih data biometrik, seperti video seseorang yang sedang berbicara, dengan menggunakan algoritma kecerdasan buatan. Kemudian mencocokkan gerakan wajah dan suara untuk membangun kembali wajah video menjadi wajah orang lain. Dengan kata lain, deepfake adalah media yang dihasilkan oleh kecerdasan buatan yang sangat mirip dengan aslinya. Saat ini, teknologi deepfake dapat diakses oleh siapa saja, tanpa memerlukan keahlian profesional, sehingga bahkan orang awam pun dapat menggunakan teknologi ini.

Teknologi ini apabila berada di tangan orang yang salah maka akan menjadi sumber masalah yang sangat signifikan, salah satunya adalah pemerasan seksual (sextortion). Sextortion adalah bentuk kejahatan di mana pelaku memeras korban dengan ancaman akan menyebarkan materi yang mengandung konten seksual, seringkali berupa video atau foto yang telah dimanipulasi menggunakan teknologi deepfake. Dalam beberapa kasus, korban tidak menyadari bahwa materi tersebut sepenuhnya palsu hingga pelaku memberikan ancaman. Sextortion berbasis deepfake menjadi lebih menakutkan karena kemampuannya untuk menciptakan konten yang sangat realistis, memudahkan pelaku untuk menjebak korban dan menyebabkan tekanan psikologis yang berat.

Menurut Weeks, kata “sextortion” pertama kali digunakan dalam media cetak di California pada tahun 1950. Asosiasi Hakim Wanita Internasional kemudian menggunakan kata tersebut sekali lagi pada tahun 2008. Institute for Responsible Online and Cell Phone Communication memuji keutamaan penggunaan situs web mereka setahun kemudian, <http://www.sextortion.org> dan siaran langsung untuk memperingatkan publik tentang epidemi sexting yang semakin meningkat. Lebih mengejutkan lagi, penelitian dari Transparency International pada tahun 2020 menunjukkan bahwa Indonesia menempati posisi pertama dengan kasus sekstorsi tertinggi di Asia, seperti tampak pada infografis di bawah ini.



Gambar 1. Penelitian dari Transparency International pada tahun 2020.

Sumber : (Syauket et al., 2024).

Sextortion, yang sering dikenal sebagai pemerasan seksual, di dokumentasikan oleh Transparency International dalam Global Corryotion Barometer Asia 2020. Berdasarkan data tersebut, Indonesia merupakan negara asia yang terbanyak dalam kasus ini. Sebanyak 20.000 orang dari 17 negara asia berpartisipasi dalam jajak pendapat tersebut, sehingga 1.000 orang berasal dari Indonesia. Dibandingkan dengan negara lain, kasus sextortion di Indonesia berada di posisi teratas, di mana 18% responden menyatakan bahwa mereka mengalami atau menyaksikan sextortion, yang umumnya terjadi di sektor layanan publik. Fakta ini bahkan

melampaui India, negara yang sering kita dengar memiliki angka kasus pemerkosaan yang tinggi hingga memicu gerakan protes besar di sana.

Pada tahun 2023, ada lebih dari 95.820 film deepfake yang tersedia di seluruh dunia, menurut data, meningkat 550% dari tahun 2019. Peningkatan ini mengindikasikan bahwa penggunaan teknologi ini semakin meluas dan berpotensi disalahgunakan untuk kejahatan seperti sextortion (CNN Indonesia, 2023).

Epidemi deepfake sextortion di Indonesia pertama kali diperkenalkan sebagian karena gugatan terhadap aktris Nagita Slavina pada awal tahun 2022. Sebuah film porno berdurasi 61 detik yang menampilkan wajah Nagita Slavina sebagai pemeran utama dalam video tersebut mengejutkan para penonton pada saat itu. Namun, penelitian lebih lanjut mengungkapkan bahwa film tersebut merupakan hasil dari manipulasi teknologi deepfake, di sebenarnya, mana pemain Miss Key, wajahnya ditumpangkan secara digital di atas tubuh Nagita Slavina (Nasution et al., 2024).

Untuk contoh kasus kedua adalah kasus deepfake pornografi di Indonesia, terutama yang melibatkan wajah publik figur seperti Jessica Iskandar, menimbulkan kekhawatiran serius terkait penyalahgunaan data pribadi. Dalam kasus ini, wajah mereka dimanipulasi secara digital dan digunakan dalam video bermuatan pornografi tanpa persetujuan. Teknologi deepfake memungkinkan pelaku untuk menciptakan konten yang sangat mirip dengan individu yang sebenarnya, yang tidak terlibat dalam pembuatan video tersebut, sehingga menyesatkan publik dan merusak reputasi korban.

Terlepas dari kenyataan bahwa deepfake belum diatur secara khusus oleh undang-undang, pelaku yang membuat dan menyebarkan konten pornografi menggunakan deepfake dapat dikenai Pasal 27 ayat (1) UU ITE, yang melarang penyebaran konten bermuatan pornografi di internet. Selain itu, Pasal 45 ayat (1) UU ITE dapat digunakan untuk menindak pelaku yang menyebabkan kerugian bagi korban karena penyebaran video tersebut (H., 2020).

Pada prinsipnya, terdapat beberapa aturan di Indonesia yang dapat diterapkan untuk menangani tindak pidana terkait deepfake, sebagaimana dijelaskan dalam tabel berikut:

Tabel 1. Peraturan Perundang-undangan Terkait Deepfake di Indonesia.

No	Perundang-Undangan	Pasal
1	Undang-Undang Dasar Negara Republik Indonesia Tahun 1945	Pasal 28G ayat (1)
2	UU Republik Indonesia Nomor 12 Tahun 2005 Tentang Pengesahan International Covenant On Civil And Political Rights (Kovenan Internasional Tentang Hak-Hak Sipil Dan Politik).	Pasal 17

3	UU Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang Undang Nomor 11 Tahun 2008 tentang Informasi Dan Transaksi Elektronik	Pasal 27A Pasal 28 ayat (1)
4	UU Republik Indonesia Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi	Pasal 65 ayat (3) Pasal 66 Pasal 67 ayat (3) Pasal 68

Hukum dan peraturan yang berkaitan dengan deepfake di Indonesia dapat dilihat pada tabel di atas, yang dimana menunjukkan bahwa aturan-aturan tersebut belum secara eksplisit mengatur tindak pidana deepfake. UU Dasar Negara Republik Indonesia Tahun 1945 menetapkan perlindungan bagi seluruh rakyat Indonesia, termasuk hak privasi sebagai hak asasi manusia yang fundamental dalam Pasal 28G ayat (1).

Perlindungan privasi ini diakui dalam Konvenan Internasional tentang Hak-Hak Sipil dan Politik (ICCPR), yang telah diratifikasi oleh Indonesia melalui UU Nomor 12 Tahun 2005 dan menjadi dasar bagi peraturan perlindungan privasi dan data pribadi tambahan di Indonesia. Pasal 17 ICCPR melindungi privasi individu dari gangguan yang sewenang-wenang, menggarisbawahi pentingnya perlindungan hukum terhadap hak privasi dan data pribadi.

UU Nomor 1 Tahun 2024 yang mengubah Undang-Undang Nomor 1 Tahun 2008 tentang UU ITE, yang lebih berfokus pada transaksi elektronik, merupakan salah satu turunan dari Pasal 28G ayat (1). Deepfake, sebagai media palsu, dapat merusak nama baik individu dan diatur dalam Pasal 27A mengenai perbuatan yang merendahkan harga diri orang lain, serta Pasal 28 ayat (1) tentang berita bohong. Selain itu, terkait penggunaan data biometrik dalam tindak pidana, UU No. 27 Tahun 2022 tentang perlindungan data pribadi juga relevan, khususnya Pasal 65, 66, dan 67 ayat (3). Hal ini mengindikasikan bahwa kasus penipuan dengan teknologi deepfake mencakup penyalahgunaan informasi biometrik korban selain penipuan elektronik dan pencemaran nama baik (Noerman & Ibrahim, 2024).

Tantangan Hukum dalam Menjerat Pelaku Sextortion Berbasis Teknologi Deepfake

Menjerat pelaku sextortion berbasis teknologi deepfake di Indonesia menghadapi sejumlah tantangan hukum yang signifikan. Salah satu tantangan utama adalah pembuktian. Deepfake, sebagai manipulasi visual atau audio, sering kali sangat sulit dibedakan dengan yang asli, sehingga identifikasi pelaku dan pembuktian rekaman yang telah dimanipulasi menjadi kompleks. Pada kasus sextortion, pelaku menggunakan teknik manipulasi yang canggih untuk menipu korban, yang membuat pembuktian bahwa rekaman tersebut adalah deepfake menjadi sulit.

Dari sisi hukum yang melindungi, meskipun UU ITE dan UU PDP memberikan beberapa landasan hukum untuk menangani kasus deepfake, peraturan-peraturan tersebut belum secara eksplisit mengatur tentang deepfake (Bullyid, 2024). UU ITE melarang manipulasi data elektronik seolah-olah asli, dan UU PDP melarang penggunaan data pribadi palsu. Namun, aturan ini tidak secara spesifik menyinggung deepfake. Dalam KUHP yang baru, deepfake bermuatan pornografi diatur dengan ancaman hukuman berat, namun regulasi yang lebih spesifik dan menyeluruh masih diperlukan untuk menjerat pelaku (Admin, 2023).

Identifikasi dan pengumpulan bukti juga menjadi tantangan tersendiri, mengingat pelaku sextortion menggunakan teknik manipulasi yang rumit. Video atau audio deepfake dapat digunakan untuk menekan korban agar membayar uang tebusan demi menghindari skandal. Suara dan wajah korban merupakan salah satu data pribadi yang harus dilindungi oleh undang-undang dan penyalahgunaannya dapat menyebabkan kerusakan fisik dan psikologis pada korban yang merupakan alasan lain mengapa melindungi informasi pribadi sangat penting.

Dibutuhkan keterampilan investigasi yang tinggi, termasuk kemampuan forensik digital, agar penegak hukum dapat menganalisis dan memverifikasi keaslian rekaman deepfake dengan lebih baik. Untuk melengkapi upaya penegakan hukum, regulasi yang lebih baik dan spesifik terkait deepfake perlu dirumuskan, terutama dalam konteks kekerasan seksual dan penyalahgunaan teknologi. Masyarakat juga harus lebih sadar akan risiko yang ditimbulkan oleh penyalahgunaan teknologi deepfake ini.

Peran Hukum Teknologi Informasi dalam menghadapi ancaman Deepfake di Indonesia

Teknologi deepfake merupakan bentuk kecerdasan buatan (Artificial Intelligence, AI) yang menggunakan algoritma pembelajaran mendalam (deep learning) untuk membuat atau memodifikasi konten digital, seperti audio, video, dan gambar, sehingga tampak realistis meski bersifat sintetik. Teknologi ini memanfaatkan Generative Adversarial Networks (GANs) untuk menciptakan media yang tampak autentik di mata manusia. Beberapa jenis deepfake yang umum termasuk pertukaran wajah (Face Swapping), sinkronisasi bibir (Lipsyncing), kloning suara (Voice Cloning), dan pembuatan manusia sintetik (Synthetic Humans) (Admin, 2024).

Walaupun deepfake berpotensi dimanfaatkan dalam bidang seperti hiburan dan pendidikan, penggunaannya juga menimbulkan masalah serius, seperti disinformasi, penipuan, dan pelanggaran privasi. Oleh karena itu, regulasi yang tepat sangat diperlukan agar teknologi ini digunakan secara etis tanpa merugikan masyarakat. Di Indonesia, meskipun regulasi mengenai deepfake masih dalam tahap perkembangan, beberapa undang-undang sudah memberikan dasar hukum yang dapat digunakan.

Ada beberapa UU yang dapat digunakan untuk menangani ancaman yang muncul dari teknologi deepfake di Indonesia. Beberapa di antaranya adalah:

- a. UU No. 11 Tahun 2008 tentang UU ITE: Undang-Undang ini mengontrol tentang penyebaran informasi elektronik, termasuk konten yang bersifat menipu, fitnah, atau berpotensi menyebabkan kerugian bagi masyarakat. Artikel 27 ayat 3, misalnya, mengontrol larangan penyebaran hoaks, termasuk deepfake dan informasi yang memfitnah.
- b. UU No. 19 Tahun 2016 sebagai perubahan Undang-Undang Informasi dan Transaksi Elektronik: Perubahan ini memperbarui beberapa pasal yang menyangkut pencemaran nama baik, penyebaran hoaks, dan perlindungan data pribadi, yang sangat relevan dalam kasus deepfake. Deepfake yang digunakan untuk mendiskreditkan individu, lembaga, atau pemerintah dapat ditindak berdasarkan undang-undang ini.
- c. UU No. 44 Tahun 2008 tentang Pornografi: Dalam kasus deepfake yang digunakan untuk membuat konten pornografi palsu, undang-undang ini menjadi dasar hukum untuk melindungi korban. Konten deepfake yang menampilkan manipulasi wajah seseorang ke dalam video atau gambar pornografi dapat diatur di bawah UU ini, terutama pada pasal-pasal yang mengatur distribusi dan produksi konten pornografi.
- d. UU No. 14 Tahun 2008 tentang Keterbukaan Informasi Publik : Terlepas dari itu, UU ini lebih terkait dengan hak publik atas informasi, penting bagi pemerintah untuk menjaga integritas informasi yang tersedia bagi publik. Deepfake dapat mengaburkan batas antara informasi yang benar dan palsu, sehingga undang-undang ini juga memiliki relevansi dalam memerangi disinformasi yang dihasilkan oleh deepfake.
- e. Rencana Perlindungan Data Pribadi: Indonesia sedang mengembangkan undang-undang tentang perlindungan data pribadi yang diharapkan akan mencakup perlindungan terhadap penyalahgunaan data untuk membuat konten deepfake. Data biometrik, seperti wajah dan suara, yang sering digunakan dalam pembuatan deepfake, dapat dimasukkan ke dalam kategori data yang dilindungi oleh undang-undang ini.

Jika konten deepfake merugikan individu atau kelompok, pelaku dapat dikenakan tuntutan berdasarkan hukum yang berlaku di Indonesia. Beberapa tindakan hukum yang dapat diterapkan antara lain tindak pidana pencemaran nama baik, jika deepfake digunakan untuk mendiskreditkan atau merusak reputasi seseorang, di mana pelaku dapat dijerat dengan pasal pencemaran nama baik sesuai UU ITE atau KUHP. Selain itu, dalam kasus pemerasan (sextortion), di mana deepfake digunakan untuk membuat video pornografi palsu dan memeras korban, pelaku dapat diadili berdasarkan hukum pidana terkait pemerasan dan pornografi.

Deepfake juga dapat digunakan untuk menyebarkan disinformasi, seperti penipuan dalam konteks politik, keuangan, atau keamanan. Dalam hal ini, pelaku bisa dijerat dengan pasal penipuan dan penyebaran berita palsu sesuai dengan UU ITE.

Langkah-Langkah Preventif untuk melindungi masyarakat dari pemerasan berbasis Deepfake

Langkah preventif menjadi aspek penting dalam melindungi masyarakat dari kejahatan berbasis deepfake. Meningkatkan tingkat literasi digital di kalangan masyarakat Indonesia adalah salah satu upaya yang dapat dilakukan. Kesadaran akan bahaya penyalahgunaan teknologi deepfake perlu ditingkatkan melalui inisiatif melibatkan pendidikan sejumlah yang pemangku kepentingan, seperti pemerintah, institusi akademis, dan platform online.

Ditambah lagi, perusahaan teknologi serta media sosial juga harus mengambil langkah-langkah untuk memperkuat keamanan digital di platform mereka. Misalnya, dengan mengembangkan teknologi deteksi deepfake yang lebih canggih dan melarang penyebaran konten deepfake yang bersifat merugikan.

Dari sisi hukum, diperlukan adanya pembaruan regulasi yang mengatur secara spesifik tentang penyalahgunaan deepfake. Pembaruan ini bisa berupa penambahan pasal dalam UU ITE yang secara khusus mengontrol tentang deepfake dan konsekuensinya. Presiden Joko Widodo pernah menjadi korban penyalahgunaan teknologi deepfake ketika sebuah video palsu yang menampilkan dirinya berpidato dalam bahasa Mandarin beredar di media sosial (Damar Iradat, 2023). Kominfo mengonfirmasi untuk video tersebut adalah hasil manipulasi menggunakan teknologi artificial intelligence (AI) deepfake, yang menyesatkan publik dan merusak reputasi presiden.

Kasus ini menunjukkan konsekuensi serius dari teknologi canggih seperti deepfake dan fakta bahwa pelanggar dapat menghadapi tuntutan berdasarkan ayat pertama dari Pasal 27 UU ITE mengontrol penyebaran materi elektronik yang melanggar kesusilaan. Hukuman maksimum bagi pelanggar adalah hukuman 6 tahun penjara atau denda sebanyak 1 miliar. Peristiwa ini juga menekankan betapa pentingnya meningkatkan kemampuan penegak hukum untuk menangani kasus yang berkaitan dengan teknologi seperti deepfake.

4. KESIMPULAN DAN REKOMENDASI

Kesimpulan

Penyalahgunaan teknologi deepfake untuk pemerasan (sextortion) merupakan salah satu tantangan serius dalam era digital saat ini. Perkembangan teknologi informasi telah membuka peluang bagi kejahatan siber yang semakin kompleks, termasuk penggunaan deepfake dalam

manipulasi visual yang sangat realistis. Meskipun teknologi ini awalnya diciptakan untuk kepentingan hiburan dan inovasi, penyalahgunaannya dalam kegiatan kriminal mengancam privasi, keamanan, dan kehormatan individu.

Regulasi hukum di Indonesia saat ini masih menghadapi tantangan dalam menangani kasus penyalahgunaan deepfake karena kerangka hukum yang ada belum sepenuhnya mencakup fenomena baru ini. Selain itu, keterbatasan kapasitas aparat penegak hukum dalam memahami dan menangani kejahatan teknologi menambah kompleksitas masalah ini.

Untuk mengatasi tantangan tersebut, diperlukan upaya kolaboratif yang melibatkan peningkatan regulasi, pelatihan bagi penegak hukum, edukasi masyarakat, serta kerja sama internasional yang kuat. Pengembangan teknologi deteksi deepfake juga menjadi solusi penting untuk menanggulangi ancaman ini, guna melindungi individu dan masyarakat dari dampak negatif teknologi yang disalahgunakan.

Rekomendasi

Peningkatan Kerangka Hukum: Pemerintah perlu memperbarui dan memperjelas regulasi yang berkaitan dengan kejahatan berbasis teknologi, seperti penyalahgunaan deepfake untuk pemerasan (sextortion), agar lebih relevan dengan perkembangan teknologi saat ini. Revisi terhadap Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) serta undang-undang terkait lainnya diperlukan untuk mengakomodasi kompleksitas kejahatan digital yang terus berkembang.

Peningkatan Kapasitas Penegak Hukum: Pelatihan dan pembekalan aparat penegak hukum mengenai teknologi kecerdasan buatan, deepfake, dan metode investigasi digital perlu ditingkatkan. Hal ini untuk memastikan bahwa kasus kejahatan berbasis teknologi dapat diselidiki secara menyeluruh dan pelaku dapat diidentifikasi dan ditangkap dengan tepat.

Edukasi Masyarakat: Edukasi publik terkait keamanan digital, dampak negatif teknologi deepfake, serta cara melindungi diri dari ancaman kejahatan siber perlu diperluas. Program kesadaran digital harus diperkenalkan di berbagai lapisan masyarakat untuk meminimalisir kerentanan individu terhadap ancaman seperti sextortion.

Kerja Sama Internasional: Mengingat kejahatan berbasis teknologi tidak terbatas pada wilayah negara, diperlukan kerja sama internasional yang lebih erat dalam hal pengaturan hukum, pertukaran informasi, dan penegakan hukum terhadap pelaku kejahatan lintas negara.

Pengembangan Teknologi Deteksi: Pemerintah dan lembaga penelitian perlu mendukung pengembangan teknologi yang dapat mendeteksi deepfake secara lebih akurat dan efisien. Teknologi ini akan sangat bermanfaat untuk melawan penyalahgunaan deepfake dan membantu proses pembuktian dalam kasus-kasus hukum.

DAFTAR REFERENSI

- Admin. (2023). Deepfake, AI-crime, UU PDP, dan KUHP baru. *CSIRT KemenPANRB*. <https://csirt.menpan.go.id/posts/deepfake-ai-crime-uu-pdp-dan-kuhp-baru>
- Admin. (2024). Pengaturan hukum teknologi deepfake di Indonesia. *Alchemist Group*. <https://alchemistgroup.co/pengaturan-hukum-teknologi-deepfake-di-indonesia/>
- Bullyid. (2024). Menggunakan AI untuk deepfake: Definisi, dasar hukum, dan cara mengatasinya. *Bullyid*. <https://bullyid.org/edukasi-hukum/tindakan-deepfake/>
- Chesney, R., & Citron, D. K. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review*, 107(6), 1753–1820.
- Citron, D. K., & Chesney, R. (2024). *Deep fakes and the law*. Oxford University Press.
- CNN Indonesia. (2023, November 20). Kominfo beri peringatan, perempuan jadi target penyalahgunaan AI. *CNN Indonesia*. <https://www.cnnindonesia.com/teknologi/20231120105820-192-1026470/kominfo-beri-peringatan-perempuan-jadi-target-penyalahgunaan-ai>
- European Union. (2024). *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*. *Official Journal of the European Union*.
- Faqih, M., & Priowirjanto, E. S. (2022). Pengaturan pertanggungjawaban pelaku penyalahgunaan deepfakes dalam teknologi kecerdasan buatan pada konten pornografi berdasarkan hukum positif Indonesia. *Jurnal Indonesia Sosial Teknologi*, 3(11), 1156–1168. <https://doi.org/10.36418/jist.v3i11.528>
- H., C. M. T. D. (2020, November 10). Polda Metro akan gelar perkara penyebaran video viral mirip Jessica Iskandar. *Tempo*. <https://metro.tempo.co/read/1404620/polda-metro-akan-gelar-perkara-penyebaran-video-viral-mirip-jessica-iskandar>
- Iradat, D. (2023). Apa itu deepfake yang bikin “Jokowi” jago ngomong Mandarin? *CNN Indonesia*.
- Kietzmann, J., Lee, L. W., McCarthy, I. P., & Kietzmann, T. C. (2020). Deepfakes: Trick or treat? *Business Horizons*, 63(2), 135–146. <https://doi.org/10.1016/j.bushor.2019.11.006>
- Nasution, A. V. A., Suteki, S., & Lumbanraja, A. D. (2024). Prospek pemenuhan *right to be forgotten* bagi korban deepfake pornography akibat penyalahgunaan artificial intelligence di Indonesia. *Diponegoro Law Journal*, 13(2). <https://doi.org/10.14710/dlj.2024.43617>
- Nguyen, T. T., Nguyen, C. M., Nguyen, D. T., Nguyen, D. T., & Nahavandi, S. (2019). Deep learning for deepfakes creation and detection: A survey. *arXiv*. <https://arxiv.org/abs/1909.11573>
- Noerman, C. T., & Ibrahim, A. L. (2024). Kriminalisasi deepfake di Indonesia sebagai bentuk perlindungan negara. *Jurnal USM Law Review*, 7(2), 603. <https://doi.org/10.26623/julr.v7i2.8995>

- Syauket, A., Saimima, I. D. S., Simarmata, R. P., Aidy, W. R., Zainab, N., Prayitno, R. B., & Cabui, C. E. (2024). Sextortion fenomena pemerasan seksual di lingkungan pendidikan. *Jurnal Kajian Ilmiah*, 22(3), 219–230. <https://doi.org/10.31599/sqgp1z49>
- Warsito, B. (2016). Tinjauan KUHP dan Undang-Undang ITE terhadap cyber crime di Indonesia. *Jurnal Teknologi*, 85(1), 6.