Media Hukum Indonesia (MHI)
Published by Yayasan Daarul Huda Krueng Mane
https://ojs.daarulhuda.or.id/index.php/MHI/index

April-June-2024. Vol.2, No.2
e-ISSN: 3032-6591
pp 586-592

Analisis Hukum Terhadap Pencegahan Kasus Deepfake Serta Perlindungan Hukum Terhadap Korban

Adnasohn Aqilla Respati[1], Astri Dewi Setyarini[2], Dodi Parlagutan[3], Muhammad Rafli[4], Rayhan Syahbana Mahendra[5], Andriyanto Adhi Nugroho[6]
[123456]Fakultas Hukum Universitas Pembangunan Nasional "Veteran" Jakarta
Email: 2110611339@mahasiswa.upnvj.ac.id[1], 2110611191@mahasiswa.upnvj.ac.id[2], 2110611011@mahasiswa.upnvj.ac.id[3], 2110611155@mahasiswa.upnvj.ac.id[4], 2110611175@mahasiswa.upnvj.ac.id[5]

Abstract:
This research will examine various legal aspects related to Deepfake Porn, including the role of law in protecting individual privacy, copyright, and cyber security. In addition, this research will also explore the potential for public awareness education as a preventative measure by increasing public understanding of the risks of Deepfakes and how to protect themselves from possible misuse of this technology. The research method that can be used to analyze efforts to prevent deepfake pornography and educate public awareness in the digital environment is the normative juridical research method. The steps in this method include identifying the legal problem to be researched, collecting data through searching regulations and literature related to the problem. Protection of personal data in the use of Artificial Intelligence (AI) technology is very important to avoid threats such as deepfake videos. Personal data, including personal photos, must be legally protected. Privacy is divided into three types: Physical Privacy, Information Privacy, and Organizational Privacy, which includes protection of individual communications, behavior and identity. In Europe, citizens can exercise the "right to be forgotten" (RTBF) right to delete personal information from the internet, as experienced by Mario Costeja Gonzalez in 2010. The EU updated the RTBF rules in the GDPR since May 2018. Indonesia also has a similar concept in the ITE Law Article 26 paragraphs (3) and (4), although the implementation is different and faces challenges in dealing with deepfakes.

Abstrak:
Penelitian ini akan mengkaji berbagai aspek hukum yang berkaitan dengan Deepfake Porn, termasuk peranan hukum dalam melindungi privasi individu, hak cipta, dan keamanan siber. Selain itu, penelitian ini juga akan mengeksplorasi potensi pendidikan kesadaran masyarakat sebagai langkah pencegahan dengan meningkatkan pemahaman masyarakat tentang risiko Deepfake dan cara melindungi diri dari kemungkinan penyalahgunaan teknologi ini. Metode penelitian yang dapat digunakan untuk menganalisis upaya pencegahan deepfake pornografi dan pendidikan kesadaran publik di lingkungan digital adalah metode penelitian yuridis normatif. Langkah-langkah dalam metode ini meliputi identifikasi masalah hukum yang akan diteliti, pengumpulan data melalui penelusuran peraturan dan literatur terkait masalah tersebut. Perlindungan data pribadi dalam penggunaan teknologi Artificial Intelligence (AI) sangat penting untuk menghindari ancaman seperti video deepfake. Data pribadi, termasuk foto diri, harus dilindungi secara hukum. Privasi terbagi menjadi tiga jenis: Physical Privacy, Information Privacy, dan Organizational Privacy, yang mencakup perlindungan terhadap komunikasi, perilaku, dan identitas individu. Di Eropa, warga negara dapat menggunakan hak "right to be forgotten" (RTBF) untuk menghapus informasi pribadi dari internet, seperti yang dialami oleh Mario Costeja Gonzalez pada tahun 2010. EU memperbarui aturan RTBF dalam GDPR sejak Mei 2018. Indonesia juga memiliki konsep serupa dalam UU ITE Pasal 26 ayat (3) dan (4), meskipun implementasinya berbeda dan menghadapi tantangan dalam menangani deepfake.

Article History
Received May 28, 2024
Revised May 30, 2024
Accepted June 12 2024
Available online 18 June, 2024

Keywords:
Prevention, Deepfakes, Legal Protection, Victims

Keywords :
Pencegahan, Deepfake, Perlindungan Hukum, Korban

https://doi.org/10.5281/zenodo.12508126

PENDAHULUAN

Dalam era yang semakin maju secara digital, kemajuan teknologi informasi telah memberikan dampak positif yang sangat besar pada berbagai sektor kehidupan. Namun, seiring dengan

April-June-2024. Vol.2, No.2
e-ISSN: 3032-6591
pp 586-592

perkembangan teknologi tersebut, muncul pula tantangan baru dalam bentuk penyalahgunaan teknologi yang berpotensi merugikan individu maupun masyarakat secara keseluruhan. Salah satu peristiwa yang mencuat dalam beberapa tahun terakhir adalah fenomena "Deepfake Porn," yang menunjukkan bagaimana teknologi dapat digunakan secara tidak etis dan merugikan.

Salah satu karya Artificial Intelligence (AI) yang menjadi sorotan adalah deepfake. Deepfake merujuk pada penggabungan teknologi deep learning dengan tujuan menciptakan konten palsu. Deep learning, pada dasarnya, adalah teknik yang digunakan untuk melatih AI agar dapat mengeksekusi suatu tugas tertentu. Deepfake adalah istilah yang digunakan untuk algoritma tersebut, yang memungkinkan pengguna untuk mengganti wajah satu aktor dengan wajah aktor lain dalam video dengan tingkat keaslian gambar yang tinggi, meniru objek visual yang nyata. Selain dalam bentuk video, teknologi deepfake juga dapat digunakan untuk merekayasa gambar. Contoh yang paling menonjol adalah deepfake porn, yaitu penggunaan teknologi untuk menciptakan video pornografi palsu dengan menggantikan wajah individu yang sebenarnya dengan wajah orang lain. Permasalahan ini memiliki potensi merusak citra individu, privasi, dan kesejahteraan psikologis pihak yang terlibat.

Pada tahun 2017, istilah "deepfake" mulai dikenal luas setelah seorang pengguna Reddit menggunakan Generative Adversarial Networks (GAN) dan TensorFlow, sebuah perangkat lunak dari Google yang mendukung pembelajaran mesin, untuk membuat video palsu. Kombinasi antara GAN dan TensorFlow memungkinkan penciptaan video deepfake yang menggabungkan tubuh atau wajah tokoh publik atau selebriti ke dalam video porno yang sudah ada. Semakin banyak gambar wajah dan rekaman suara dari subjek sumber yang tersedia, semakin realistis hasilnya. Hal ini membuat identifikasi konten yang dibuat menggunakan teknologi deepfake menjadi semakin sulit karena tingkat realisme yang tinggi. Teknologi ini telah menimbulkan kekhawatiran serius mengenai potensi dan dampak negatif dari deepfake, termasuk kemampuan untuk menipu penglihatan manusia dan masalah serius terkait dengan pemalsuan dan penyebaran konten pornografi palsu yang melibatkan tokoh terkenal.

Penyalahgunaan teknologi deepfake menimbulkan tantangan serius dalam konteks hukum dan etika. Kejahatan semacam ini merujuk pada ketentuan dalam UU ITE dan perubahannya, UU PDP, UU Pornografi, serta UU 1/2023 tentang KUHP baru. Hal ini menimbulkan pertanyaan mengenai batasan hukum dalam menangani kasus-kasus Deepfake Porn dan bagaimana masyarakat serta individu dapat melindungi diri dari potensi penyalahgunaan teknologi ini. Oleh karena itu, studi ini bertujuan untuk menganalisis kerangka hukum yang terkait dengan upaya pencegahan kasus Deepfake Porn serta merumuskan pendekatan pendidikan kesadaran masyarakat dalam lingkungan digital sebagai solusi alternatif untuk mengatasi permasalahan tersebut.

Untuk menjawab tantangan-tantangan tersebut, penelitian ini akan mengkaji berbagai aspek hukum yang berkaitan dengan Deepfake Porn, termasuk peranan hukum dalam melindungi privasi individu, hak cipta, dan keamanan siber. Selain itu, penelitian ini juga akan mengeksplorasi potensi pendidikan kesadaran masyarakat sebagai langkah pencegahan dengan meningkatkan pemahaman masyarakat tentang risiko Deepfake dan cara melindungi diri dari kemungkinan penyalahgunaan teknologi ini.

Dengan mengintegrasikan pendekatan yang luas yang meliputi hukum, pendidikan kesadaran masyarakat, kerjasama internasional, etika teknologi, dan mekanisme pelaporan, kita dapat bergerak maju dalam mengatasi tantangan serius yang disajikan oleh Deepfake Porn. Langkah ini sangat penting dalam menjaga integritas, privasi, dan kesejahteraan psikologis individu di era digital yang terus berkembang.

METODE PENELITIAN

Metode penelitian yang dapat digunakan untuk menganalisis upaya pencegahan deepfake pornografi dan pendidikan kesadaran publik di lingkungan digital adalah metode penelitian yuridis normatif. Langkah-langkah dalam metode ini meliputi identifikasi masalah hukum yang akan diteliti, pengumpulan data melalui penelusuran peraturan dan literatur terkait masalah tersebut. Analisis data menggunakan pendekatan normatif yang berfokus pada hukum dan peraturan yang berlaku, serta penarikan kesimpulan berdasarkan analisis tersebut. Peneliti akan menganalisis peraturan dan hukum yang relevan terkait deepfake pornografi dan pendidikan kesadaran publik di lingkungan digital untuk

April-June-2024. Vol.2, No.2
e-ISSN: 3032-6591
pp 586-592

menghasilkan kesimpulan mengenai upaya pencegahan dan penanggulangan masalah ini dalam kerangka hukum yang ada. Data dikumpulkan melalui penelusuran peraturan dan literatur, baik di perpustakaan maupun sumber online seperti jurnal dan situs web pemerintah.

HASIL DAN PEMBAHASAN

Teknologi Deepfake Sebagai Bentuk Kemajuan Teknologi Informasi

Kemajuan teknologi informasi memang memiliki dampak positif terhadap kehidupan manusia yang lebih efisien dan memudahkan dalam segala hal. Namun, kemajuan teknologi tidak hanya memberikan dampak positif, tetapi juga menimbulkan dampak negatif yang dapat merugikan. Salah satu bentuk kemajuan teknologi yang dikenal saat ini yakni Artificial Intelligence (AI), salah satu algoritma Artificial Intelligence (AI) yakni teknologi deepfake.

Menurut Marissa Koopman, Andrea Macarulla Rodriguez, dan Zeno Geradts pada jurnalnya memberikan anggapan bahwa Teknologi Deepfake sebagai algoritma, berupa: *"The Deepfake algorithm allows a user to switch the face of one actor in a video with the face ofa different actor in a photorealistic manner"*[1]. Oleh karena itu, dapat diartikan bahwasannya teknologi deepfake merupakan algorima yang dapat digunakan untuk mengganti wajah ataupun tampilan dalam bentuk foto dan video. Hal tersebut bertujuan untuk menyembunyikan aktor sesungguhnya dalam media tersebut menjadi aktor lain. Semakin canggihnya teknologi deepfake yang tersedia maka hasil dari foto ataupun video yang dimanipulasi semakin sulit untuk dibedakan dari foto dan video aslinya.

Penggunaan teknologi deepfake porn termasuk dalam kekerasan gender berbasis online dengan mayoritas korban perempuan. Hal ini disebabkan karena pada umumnya diciptakan oleh dan untuk para lelaki. Adanya fenomena deepfake pornografi juga diartikan oleh akademi ahli hukum sebagai bentuk invasi privasi seksual. Para ahli juga memasukkan deepfake pornografi ke dalam pornografi tanpa consent dan kekerasan seksual melalui gambar. Pelaku deepfake pornografi mencuri otoritas tubuh korban dengan merekayasa korban melakukan sesuatu yang pelaku inginkan tanpa izin dan bahkan sepengetahuan korban. Pelaku bertindak seolah ia mempunyai kuasa sepenuhnya akan tubuh perempuan yang berada dalam dunia maya. Hal ini termasuk dalam perbuatan kriminal, dimana pelakunya melakukan beberapa kejahatan sekaligus ketika membuat deepfake pornografi, yaitu kekerasan seksual, mencuri data pribadi, menyebarkan informasi palsu, dan juga manipulasi. [2]

Dalam risetnya Chidera Okolie mengungkapkan beberapa alasan atau motif dari pelaku cyber crime dalam kasus deepfake antara lain kesenangan seksual, melakukan penindasan dengan tujuan untuk menunjukan kekuasaan. Di sini pelaku berulangkali menyebabkan kerugian secara psikologis dan emosional terhadap korban. Teknologi deepfake menimbulkan resiko yang signifikan bagi korban kekerasan dalam rumah tangga, karena pelaku dapat menggunakan deepfake untuk mengancam, memeras dan menganiaya mereka, mengabaikan persetujuan, motif balas dendam, kepuasan maskulinitas pelaku dll[3]

. Dalam mekanismenya, teknologi deepfake melibatkan jaringan yang dikenal dengan Adversarial Network (GAN). Beberapa teknik yang dilakukan dalam teknologi deepfake antara lain:

a. *Source Video Deepfake*
   Teknik ini berhubungan dengan penempatan wajah dan gerakan tubuh dalam video. Prosesnya melibatkan penggunaan algoritma deep learning untuk mendeteksi, memahami dan mereplikasi wajah serta gerakan tubuh dari satu video ke video lainnya;
b. *Audio Deepfake*
   Berfokus pada manipulasi suara menggunakan teknologi deep learning. Dengan memanfaatkan algoritma neural network, suara seseorang dapat direkam dan direplikasi dengan presisi tinggi. Hal ini mencakup pemodelan intonasi, vokal dan nuansa suara yang membuatnya tampak seperti suara asli;
c. *Lip Syncing*

[1] Kasita, I. D. (2022). Deepfake pornografi: Tren kekerasan gender berbasis online (KGBO) di era pandemi COVID-19. *Jurnal Wanita Dan Keluarga*, *3*(1), 16-26.
[2] Ibid hlm 21
[3] Rachmaria, L., & Susanto, A. (2024). Potensi Kekerasan Gender Berbasis Online Pada Penyalahgunaan Teknologi Kecerdasan Buatan Bagi Perempuan Di Media. *Jurnal Netnografi Komunikasi*, *2*(2), 51-63.

April-June-2024. Vol.2, No.2
e-ISSN: 3032-6591
pp 586-592

Merupakan teknik deepfake yang fokus pada keselarasan antara audio dan gerakan bibir dalam video. Tujuannya untuk membuat gerakan bibir dalam rekaman video cocok dengan audio yang dihasilkan secara tepat. Dengan menggunakan model deep learning, seperti *Long Short-Term Memory* (LSTM) atau model berbasis transformator, deepfake dapat menciptakan *lip sync* yang sangat akurat[4].

Bentuk pencegahan kasus deepfake sebagai tantangan kemajuan teknologi informasi

Kemajuan teknologi informasi telah membawa banyak manfaat bagi masyarakat, termasuk peningkatan efisiensi, aksesibilitas informasi, dan komunikasi global. Namun, kemajuan ini juga membawa tantangan baru, salah satunya adalah fenomena deepfake. Deepfake, teknologi yang menggunakan kecerdasan buatan untuk membuat video dan audio yang sangat realistis tetapi palsu, menjadi ancaman serius karena dapat digunakan untuk penipuan, manipulasi informasi, dan berbagai kejahatan lainnya. Pencegahan kasus deepfake memerlukan pendekatan multidimensi yang mencakup edukasi, pengembangan teknologi deteksi, regulasi hukum, dan kerjasama internasional.[5]

Salah satu langkah pertama dan terpenting dalam pencegahan deepfake adalah meningkatkan kesadaran dan edukasi publik. Masyarakat perlu memahami apa itu deepfake, bagaimana cara kerjanya, dan risiko yang terkait. Kampanye literasi digital dapat membantu orang untuk lebih kritis terhadap konten yang mereka lihat dan bagikan di media sosial. Selain itu, pelatihan khusus untuk jurnalis, penegak hukum, dan profesional terkait lainnya penting agar mereka dapat mengenali dan merespons deepfake dengan efektif.[6]

Selain edukasi, pengembangan teknologi deteksi deepfake adalah langkah kunci dalam pencegahan. Para peneliti dan perusahaan teknologi harus terus mengembangkan alat dan algoritma yang dapat mendeteksi deepfake dengan akurasi tinggi. Misalnya, penggunaan analisis forensik digital, pembelajaran mesin, dan kecerdasan buatan untuk mengenali anomali yang tidak biasa dalam video dan audio. Deteksi otomatis ini dapat diintegrasikan ke dalam platform media sosial dan penyedia layanan internet untuk memantau dan menghapus konten deepfake sebelum menyebar luas.

Regulasi dan kerangka hukum yang jelas juga sangat penting dalam menghadapi deepfake. Pemerintah perlu mengembangkan undang-undang yang spesifik mengatur penggunaan dan penyebaran teknologi deepfake. Ini termasuk sanksi bagi pelaku yang dengan sengaja membuat dan menyebarkan deepfake untuk tujuan jahat. Selain itu, regulasi harus mengatur tanggung jawab platform media sosial dalam mendeteksi dan menghapus konten deepfake, serta memberikan perlindungan hukum bagi korban deepfake.[7]

Deepfake adalah masalah global yang memerlukan kerjasama internasional untuk mengatasinya. Negara-negara perlu bekerja sama dalam berbagi informasi, teknologi, dan sumber daya untuk mendeteksi dan menangani deepfake. Organisasi internasional dapat berperan dalam mengkoordinasikan upaya ini, serta menetapkan standar dan pedoman untuk pencegahan deepfake. Selain itu, kerjasama antara sektor publik dan swasta juga penting untuk mengembangkan solusi yang efektif dan inovatif.

Pencegahan kasus deepfake sebagai tantangan kemajuan teknologi informasi memerlukan pendekatan yang komprehensif dan kolaboratif. Edukasi dan kesadaran publik, pengembangan teknologi deteksi, regulasi yang jelas, dan kerjasama internasional adalah elemen-elemen kunci dalam upaya ini. Dengan menggabungkan langkah-langkah ini, kita dapat meminimalkan dampak negatif dari deepfake dan memastikan bahwa kemajuan teknologi informasi terus memberikan manfaat yang lebih besar bagi masyarakat.

[4]AstraDigital,https://astradigital.id/article/detail/apa-itu-deepfake-dan-bagaimana-cara-mendeteksinya diakses pada tanggal 2 Juni 2024

[5] Wibowo, A., Wangsajaya, Y., & Surahmat, A. (2023). Pemolisian Digital dengan Artificial Intelligence. PT. RajaGrafindo Persada-Rajawali Pers.

[6] Utama, A. N., Kesuma, P. T., & Hidayat, R. M. (2023). Analisis Hukum terhadap Upaya Pencegahan Kasus Deepfake Porn dan Pendidikan Kesadaran Publik di Lingkungan Digital. Jurnal Pendidikan Tambusai, 7(3), 26179-26188.

[7] Mutmainnah, A., Suhandi, A. M., & Herlambang, Y. T. (2024). Problematika Teknologi Deepfake sebagai Masa Depan Hoax yang Semakin Meningkat: Solusi Strategis Ditinjau dari Literasi Digital. UPGRADE: Jurnal Pendidikan Teknologi Informasi, 1(2), 67-72.

April-June-2024. Vol.2, No.2
e-ISSN: 3032-6591
pp 586-592

Bentuk Perlindungan kasus deepfake sebagai tantangan kemajuan teknologi informasi ?

Dalam penggunaan teknologi Artificial Intelligence perlindungan data pribadi haruslah sangat dijunjung erat oleh berbagai pihak, Masalah akan muncul apabila permohonan penghapusan data tersebut ditolak, sehingga berpotensi untuk mengancam seseorang menjadi korban video deepfake. Foto diri seseorang sesungguhnya termasuk dalam kategori data pribadi yang secara hukum seharusnya dilindungi. Pada umumnya privasi dapat dikategorikan dalam 3 (tiga) tipe dasar yaitu
1) *Physical Privacy*;
2) *Information Privacy;*
3) *Organizational Privacy*.

Lebih lanjut, dalam hal memastikan data privasi yang sering kali berbenturan dengan data publik, dapat dilihat dalam beberapa point diantaranya terkait dengan : 1) *Privacy of our Communications*, 2) *Privacy of our behavior*, 3) *Privacy of our person* [8]. Pembagian tersebut pada dasarnya menempatkan foto dan video seseorang sebagai bagian dari data pribadi yang perlu dilindungi secara khusus, sebagaimana beberapa negara telah memiliki aturan khusus terkait data pribadi Indonesia sendir yang pada saat ini sudah berlaku di Indonesia.

Di Negara Eropa, perlindungan data pribadi telah berjalan dengan baik. Warga negara Eropa dapat mengajukan permohonan untuk dipenuhinya apa yang dikenal dengan istilah *right to be forgotten* (RTBF). RTBF dikenal banyak pihak setelah pada tahun 2010, setelah seseorang warga negara Spanyol Mario Costeja Gonzalez mengajukan penghapusan informasi dirinya tentang pelelangan rumah guna melunasi hutang jaminan sosial yang dialaminya pada tahun 1998 kepada mesin pencarian Google. Informasi pelelangan rumah tersebut dapat ditemui pada hasil teratas mesin pencarian Google apabila dituliskan nama dirinya. Pemberitaan Gonzalez tersebut dapat ditelusuri akibat langkah digitalisasi yang dilakukan oleh surat kabar Spanyol, *La Vanguardia* terhadap arsip-arsip beritanya- termasuk didalamnya berita tentang Gonzales . Perjuangan Gonzalez, berakhir dengan diputuskannya perusahaan Google untuk *de-index* artikel pemberitaan tentang pelelangan rumahnya. Selain, karena peristiwa tersebut telah lama terselesaikan oleh Gonzales, putusan tersebut didasarkan terkait ketentuan yang berlaku di European Union (EU) [9].

Putusan RTBF pada kasus Gonzales tersebut didasarkan ketentuan yang terkandung dalam Directive 95/46/EC, yang memberikan perlindungan kepada warga negaranya atas penggunaan data pribadi yang tidak sesuai. Setelah kasus Gonzalez tersebut marak dibicarakan, EU segera merumuskan ketentuan baru dan sejak Mei 2018 ketentuan mengenai RTBF diatur dalam Art.17 General Data Protection Regulation (GDPR) dengan judul "*Right to erasur*e ('*right to be forgotten*') yang memiliki sedikit perbedaan dengan RTBF sebelumnya.

Instrumen hukum serupa RTBF atau Right to Erasure sesungguhnya telah diadopsi dalam sistem hukum Indonesia, dengan istilah "hak untuk dilupakan" yang terdapat dalam Pasal 26 ayat (3) dan (4) UU ITE. Secara lengkap ketentuan tersebut yaitu :

(3) Setiap Penyelenggara Sistem Elektronik wajib menghapus Informasi dan Elektronik yang tidak relevan yang berada di bawah kendalinya atas permintaan orang yang bersangkutan berdasarkan penetapan pengadilan ;

(4) Setiap Penyelenggara Sistem Elektronik wajib menyediakan mekanisme penghapusan Informasi Elektronik yang sudah tidak relevan.

Hak untuk dilupakan tidak sepenuhnya serupa dengan konsep RTBF, perbedaan mendasar yang membedakan keduanya berada hasil pemenuhan hak tersebut. Pada RTBF, informasi tersebut akan hilang dari hasil mesin pencarian namun tetap dapat ditemukan pada tautan asli informasi data tersebut berada, sehingga RTBF kerap disebut sebagai langkah untuk menyulitkan seseorang untuk mengakses informasi tentang seseorang pada hasil situs mesin pencarian. Konsep Hak untuk dilupakan mengambil langkah yang berbeda dengan menghapus data tersebut sehingga tidak hanya dilakukan penghapusan dari hasil situs mesin pencari namun turut dilakukan pada tautan asli sumber data tersebut. Namun, terdapat kendala yang dapat dihadapi oleh seseorang yang hendak menghindari

[8] Terence Craig dan Marr E. Ludloff, "Privacy and Big Data : The Player, Regulators and Stakeholders, O'Reilly Media, Sebastopol, pp.14-15, 2011.
[9] Chelsea E. Carbone, "To be or not to be Forgotten : Balancing the right to know with the right to privacy in the digital age", Virginia Journal of Social Policy & the Law, Vol. 22:3,pp. 533-535, 2015.

April-June-2024. Vol.2, No.2
e-ISSN: 3032-6591
pp 586-592

ancaman teknik deepfake terhadap dirinya, mengingat RTBF dan Hak untuk dilupakan memiliki syarat yang harus dipenuhi agar informasi tersebut dihapuskan. RTBF merujuk pada putusan *Court of Justice of the European Union* (CJEU) pada kasus Gonzalez masyarakat informasi tersebut inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes[10]. Sementara Hak untuk dilupakan mensyaratkan informasi tersebut "tidak relevan". Tidak mudah tentunya untuk dalam mendasarkan ketidakrelevanan suatu informasi ketika informasi tersebut belum diproses dalam bentuk video porno atau manipulasi video lainnya sehingga ketakutan akan hadirnya ancaman terhadap diri seseorang terhadap potensi penggunaan informasi yang tidak sesuai sebaiknya menjadi pertimbangan dalam menerapkan pemberlakuan hak untuk dilupakan, dengan mendasarkan perlindungan hukum serta pengakuan terhadap hak atas data pribadi yang dimiliki oleh setiap individu. Masalah lainnya yang harus dihadapi oleh masyarakat Indonesia, karena hingga saat ini Peraturan Menteri terkait Hak Untuk Dilupakan belum terbit.

Selain adanya hak untuk dilupakan, ada beberapa langkah yang dapat dilakukan untuk perlindungan diri dari kejahatan deepfake, diantaranya adalah perlunya pemahaman yang mendalam terhadap deepfake dan bagaimana deepfake tersebut dapat disalahgunakan. Kemudian selain itu tindakan pencegahan juga dapat dilakukan dengan membatasi penggunaan media sosial dengan tidak mengirimkan gambar pribadi yang terlalu berlebihan, pergunakan watermark terhadap foto pribadi atau data pribadi yang dimiliki agar dapat membantu mencari tahu sumber kebocoran data yang berasal darimana. Kemudian perlunya penggunaan keamanan tingkat lanjut terhadap media sosial yang digunakan , hal tersebut bertujuan untuk melindungi data pribadi dari orang lain dan upaya penipuan akan menjadi lebih canggih. Penjahat dunia maya semakin mahir dalam hal-hal seperti mencuri dan mengkloning cuplikan suara untuk digunakan dalam upaya deepfake atau bypass biometrik. Untuk menggagalkan kemajuan yang tidak diinginkan ini, pemadaman kebakaran dengan api mungkin perlu dilakukan dan memanfaatkan solusi perlindungan berbasis AI .

SIMPULAN

Perlindungan data pribadi dalam penggunaan teknologi Artificial Intelligence (AI) sangat penting untuk menghindari ancaman seperti video deepfake. Data pribadi, termasuk foto diri, harus dilindungi secara hukum. Privasi terbagi menjadi tiga jenis: Physical Privacy, Information Privacy, dan Organizational Privacy, yang mencakup perlindungan terhadap komunikasi, perilaku, dan identitas individu. Di Eropa, warga negara dapat menggunakan hak "right to be forgotten" (RTBF) untuk menghapus informasi pribadi dari internet, seperti yang dialami oleh Mario Costeja Gonzalez pada tahun 2010. EU memperbarui aturan RTBF dalam GDPR sejak Mei 2018. Indonesia juga memiliki konsep serupa dalam UU ITE Pasal 26 ayat (3) dan (4), meskipun implementasinya berbeda dan menghadapi tantangan dalam menangani deepfake. Selain RTBF, langkah-langkah lain untuk melindungi diri dari deepfake termasuk memahami risiko, membatasi penggunaan media sosial, menggunakan watermark pada foto, dan mengadopsi keamanan tingkat lanjut. Solusi berbasis AI juga dapat digunakan untuk melindungi data pribadi dari kejahatan siber yang semakin canggih.

SARAN

Menurut pandangan kelompok kami, menggarisbawahi pentingnya memiliki peraturan yang jelas untuk menangani masalah deepfake, kita sebagai pengguna media sosial juga perlu meningkatkan kesadaran akan risiko yang terlibat. Hal ini termasuk menyadari bahwa dengan mengekspos diri atau identitas secara berlebihan di platform-platform tersebut, kita bisa menjadi lebih rentan terhadap penyalahgunaan oleh pihak yang tidak bertanggung jawab. Terlebih lagi, kita harus memahami bahwa dunia maya seringkali tidak dapat diprediksi, dan perilaku atau sikap orang lain terhadap kita dapat sangat bervariasi. Oleh karena itu, sebagai langkah pencegahan, bijaksanalah dalam berbagi informasi pribadi atau mengekspos diri secara berlebihan di dunia maya.

[10] McKay Cunningham, "Privacy Law That Does Not Protect Privacy, Forgetting the Right to be Forgotten, Bufallo Law Review,Vol.65, pp.496. 2017.

April-June-2024. Vol.2, No.2
e-ISSN: 3032-6591
pp 586-592

REFERENSI

Pasal 35, Undang-Undang No. 11 Tahun 2008 Tentang Informasi Dan Transaksi ElektroniK

Pasal 51, Undang-Undang No. 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik

Peraturan Pemerintah Pengganti Undang-Undang No. 18 Tahun 1960 tentang Informasi dan Transaksi Elektronik (Indonesia). diakses 31 Oktober 2023, dari http://peraturan.bpk.go.id/Details/53472/perpu-no-18-tahun-1960

Undang-Undang No. 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (Indonesia). diakses 31 Oktober 2023, dari http://peraturan.bpk.go.id/Details/37582/uu-no-19-tahun-2016

Undang-Undang No. 36 Tahun 1999 tentang Perubahan Jumlah Hukuman Denda Dalam Kitab Undang-Undang Hukum Pidana Dan Dalam Ketentuan-Ketentuan Pidana Lainnya Yang Dikeluarkan Sebelum Tanggal 17 Agustus 1945 (Indonesia). diakses 31 Oktober 2023, dari http://peraturan.bpk.go.id/Details/45357/uu-no-36-tahun-1999

Kasita, I. D. (2022). Deepfake pornografi: Tren kekerasan gender berbasis online (KGBO) di era pandemi COVID-19. *Jurnal Wanita Dan Keluarga*, *3*(1), 16-26

Rachmaria, L., & Susanto, A. (2024). Potensi Kekerasan Gender Berbasis Online Pada Penyalahgunaan Teknologi Kecerdasan Buatan Bagi Perempuan Di Media. *Jurnal Netnografi Komunikasi*, *2*(2), 51-63.

Mutmainnah, A., Suhandi, A. M., & Herlambang, Y. T. (2024). Problematika Teknologi Deepfake sebagai Masa Depan Hoax yang Semakin Meningkat: Solusi Strategis Ditinjau dari Literasi Digital. UPGRADE: Jurnal Pendidikan Teknologi Informasi, 1(2), 67-72.

Terence Craig dan Marr E. Ludloff, "Privacy and Big Data : The Player, Regulators and Stakeholders, O'Reilly Media, Sebastopol, pp.14-15, 2011.

Chelsea E. Carbone, "To be or not to be Forgotten : Balancing the right to know with the right to privacy in the digital age", Virginia Journal of Social Policy & the Law, Vol. 22:3,pp. 533-535, 2015.

McKay Cunningham, "Privacy Law That Does Not Protect Privacy, Forgetting the Right to be Forgotten, Bufallo Law Review,Vol.65, pp.496. 2017.

AstraDigital,https://astradigital.id/article/detail/apa-itu-deepfake-dan-bagaimana-cara-mendeteksinya