Madani: Jurnal Ilmiah Multidisiplin
Volume 1, Nomor 10, November 2023

E-ISSN: 2986-6340
DOI: https://doi.org/10.5281/zenodo.10201140

Penerapan Hukum Positif Indonesia Terhadap Kasus Kejahatan Dunia Maya *Deepfake*

Shannon Gandrova[1], Ricky Banke[2]
[12] Program Studi Hukum, Fakultas Hukum UPH Kampus Medan
Email: 03051210002@student.uph.edu[1], ricky.banke@lecturer.uph.edu[2]

Abstrak

Perkembangan ilmu teknologi tidak terlepas dari kehidupan manusia modern di abad ke-21 ini. Hampir semua aspek di kehidupan sehari-hari manusia adalah produk dari ilmu teknologi. Teknologi hadir dan diciptakan pertama kali dengan tujuan utama untuk memudahkan kehidupan manusia. Hal ini menjadi suatu hal yang dapat menguntungkan dan juga merugikan secara bersamaan karena ketidakterbatasan internet rawan disalahgunakan. Salah satunya adalah teknologi *deepfake* yang dimanfaatkan untuk melakukan penipuan. *Deepfake* merupakan suatu teknologi canggih yang mampu memanipulasi foto, video, dan suara seseorang. University College London (UCL) menempatkan ancaman olahan *deepfake* sebagai salah satu ancaman terbesar yang dihadapi masyarakat saat ini. Dengan kemampuan meniru suara dan mengubah konten digital, *deepfake* dimanfaatkan untuk menyebarkan konten pornografi, memeras uang, atau menyebarkan misinformasi di khalayak publik. Banyak oknum yang menyalahgunakan teknologi ini untuk mengambil data orang lain secara non-konsensual dan digunakan secara diam-diam untuk melangsungkan tindakan kejahatan. Cerdasnya pelaku kejahatan melahirkan jenis kejahatan baru yang bersifat penipuan sekaligus mampu memanipulasi alat bukti yang dipakai di persidangan. Ditambah dengan fitur anonim yang bisa dimanfaatkan untuk berselancar di dunia internet, kejahatan bisa dilakukan secara lebih gampang dan mempersulit proses investigasi untuk meringkus pelaku. Untuk menghentikan penyebaran misinformasi dari hasil olahan *deepfake*, diperlukan peran tanggap dari petugas polisi dan pemerintah. Oleh karena itu, kemajuan internet perlu diikuti dengan perlindungan *cyber* dan payung hukum yang lebih ketat. Teknologi internet yang melaju tanpa henti melahirkan jenis kejahatan baru yang menuntut pembaharuan hukum yang relevan.
Kata kunci: Penipuan dengan algoritma, Kejahatan dunia maya, Kecerdasan artifisial.

Abstract

The development of yechnology science is unable to be separated from modern human life in this 21st century. Nearly every aspect of human daily life is the product of technology science. Technology was first presented and created with the purpose of making human life easier. It is both beneficial and detrimental at the same time because the limitlessness of the internet is prone to be misused. For instance, deepfake technology is used to commit fraud. Deepfake is a sophisticated technology that has the ability to manipulate a person's photos, videos, and voice. University College London (UCL) ranks the threat of deepfakes as one of the biggest threats facing society today. With the ability to immitate voices and change digital content, deepfake is used to spread pornographic content, extort money, or spread misinformation to the public. Many individuals abuse this technology to take other people's data non-consensually and use it secretly to carry out criminal acts. The intelligance of criminals gives birth to new types of crimes that are fraudulent and are able to manipulate the evidence used in trials. Coupled with the anonymous feature on the internet, crimes can be committed more easily and complicate the investigation process to apprehend the perpetrator. To stop the spread of misinformation from processed deepfakes, a responsive role is required from police and government officials. Therefore, advances of the internet need to be accompanied by cyber protection and stricter legal regulation. The relentless progress of internet technology has given rise to new types of crimes that need relevant legal updates.
***Keyword**: Deepfake, Cyber Crime, Artificial Intelligence.*

Article Info
Received date: 2 November 2023 Revised date: 10 November 2023 Accepted date: 19 November 2023

PENDAHULUAN

Kecerdasan artifisial atau *artificial intelligence* (selanjutnya disebut AI) adalah kemampuan komputer tingkat tinggi buatan manusia yang dirancang untuk menyelesaikan kegiatan yang diperintahkan. Cara kerja AI adalah dengan mengumpulkan basis data dari kumpulan informasi yang kemudian diolah sesuai dengan pola yang ditetapkan. Kemampuan AI diterapkan mengikuti karakteristik intelektual manusia, seperti proses penalaran, menemukan jawaban, hingga menciptakan sesuatu (Britannica, 2023).

Teknologi untuk memanipulasi wajah, mengubah audio dari teks, dan menciptakan karya tiga dimensi bukanlah hal yang baru di era modern ini. Sebuah jurnal yang ditulis oleh Christoph Bregler, Michele Covell, dan Malcolm Slaney di tahun 1997 membahas tentang cara mensinkronisasikan suara dan pergerakan mulut yang digunakan dalam film (Song, 2019). Teknik pembelajaran mesin tingkat tinggi memungkinkan untuk menselaraskan suara *dubbing* ke pergerakan mulut sang aktor. Sederhananya, sistem pembelajaran mesin mengamati dan mempelajari, kemudian menggunakan pengetahuannya untuk menduplikasi gerakan aktor pada target. Proses serupa juga dapat digunakan terhadap audio dengan mendengarkan rekaman suara seseorang dan kemudian mereproduksi karakteristik suaranya.

Teknologi ini sangat berguna dalam industri film, salah satunya dalam film Fast and Furious 7. Paul Walker meninggal dunia saat *shooting* filmnya belum usai, namun digantikan oleh adiknya pada adegan selanjutnya. Menggunakan teknologi *face tracking*, Fast and Furious 7 ditayangkan dengan menggantikan Paul Walker dengan Cody Walker. Penderita Alzheimer juga dapat merasakan manfaat dari teknologi ini yang mampu menghasilkan foto wajah saat muda untuk membangkitkan memori penderitanya.

Berkembangnya AI melahirkan teknologi serupa yang kemudian dinamakan sebagai *deepfake*. Menggunakan cara kerja yang sama, *deepfakes* menggunakan teknologi *generative adversarial network* yang mengandalkan jaringan saraf dengan menganalisis kumpulan besar sampel data untuk meniru ekspresi wajah, tingkah laku, suara, dan nada suara manusia. Istilah *deepfake* diambil dari kombinasi kata *deep learning* yang berarti teknologi mesin yang dirancang secara mendalam, dan kata *fake* yang berarti palsu. Penggunaan algoritma pengenalan wajah dan jaringan komputer pembelajaran mendalam disebut sebagai *variational auto-encoder* (Sloan, 2020).

Teknologi ini pertama kali diperkenalkan oleh Ian Godfellow di tahun 2014 dengan tujuan sebagai hiburan belaka. Salah satu implikasi dari teknologi *deepfake* pada masa itu adalah aplikasi Face Swap, di mana pengguna bisa menukar foto wajahnya dengan wajah orang lain.

Gambar 1. Contoh penggunaan teknologi deepfake.

Seiring berkembangnya zaman, teknologi juga berkembang semakin pesat dan dipakai sesuai dengan kemampuannya yang semakin canggih. Objek yang bisa diolah menggunakan teknologi ini adalah foto, video, dan suara. *Deepfake* lalu disalahgunakan untuk menggunakan foto, video, atau suara orang lain di internet tanpa persetujuan yang bersangkutan dan dimanipulasi sedemikian rupa untuk kepentingan suatu pihak. Bukan hanya pihak yang asetnya dipakai saja yang dirugikan, tetapi pihak yang mengkonsumsi media tersebut juga dapat dirugikan dari penyebaran informasi palsu. *Deepfake* mulai populer di

tahun 2017 karena disalahgunakan di platform Reddit, di mana para penggunanya berbagi video porno dengan menggunakan teknologi manipulasi wajah. *Deepfake* sulit dideteksi jika dilihat secara sekilas karena menggunakan rekaman asli sehingga terlihat meyakinkan dan asli (Mika Westerlund, 2019). Setahun kemudian, lahir pula aplikasi FakeApp yang memungkinkan penggunanya untuk menciptakan foto dan video palsu.

AI mampu mengumpulkan basis data dari suara seseorang dan memakainya untuk meniru suara orang lain. Di tahun 2019 silam terdapat sebuah kasus di mana seorang CEO sebuah perusahaan menerima telepon dari atasannya yang memerintahkan untuk mentransfer €220.000. Sang CEO merasa janggal karena suara di telepon tidak identik dengan aksen Jerman atasannya. Oleh karena itu, sang CEO menolak untuk melakukan transaksi dan segera melaporkan ke atasannya sekaligus untuk melakukan konfirmasi. Diketahui bahwa telepon tersebut dilakukan oleh seorang penipu yang menyamar dan menggunakan teknologi *deepfake* untuk menyerupai suara sang atasan. Tindakan ini sudah direncanakan sebelumnya dan secara sengaja ditujukan untuk mendapatkan sejumlah uang dari penipuan tersebut.

Menggunakan praktik sejenis, AI bisa mengumpulkan basis data suara para petinggi atau tokoh penting untuk menyebarkan informasi palsu. *Deepfake* banyak digunakan untuk penyalahgunaan politik yang bertujuan untuk menjatuhkan pihak tertentu. AI bisa saja memanipulasi suara dan video Presiden Jokowi untuk menyatakan sesuatu yang tidak pernah diucapkan oleh Presiden Jokowi. Hal ini akan memberikan dampak yang sangat berbahaya hingga berupa konflik global karena masyarakat dapat saja menelan mentah-mentah media yang mereka konsumsi tanpa mengecek validitasnya. Fenomena ini sudah terjadi di tahun 2022, saat Amerika Serikat mengungkapkan rencana Rusia untuk menggunakan video *deepfake* dari Presiden Ukraina, Volodymyr Zelenskyy, untuk melangsungkan invasi. Dalam video tersebut, Presiden Volodymyr Zelenskyy memerintahkan tentara Ukraina untuk menyerah kepada Rusia. (European Union Agency for Law Enforcement Cooperation, 2022).

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

a) Pemalsuan identitas;
b) Konten pornografi non-konsensual dan eksploitasi seksual;
c) Pemerasan (*blackmailing*);
d) Penyebaran informasi palsu dan menggiring opini publik;
e) Menyebarkan teror;
f) Penipuan;
g) Pencemaran nama baik;
h) Dll.

METODE

Penelitian ini dilakukan dengan studi kepustakaan dengan menganalisis secara komprehensif sejumlah artikel internet dan jurnal di laman penyedia jurnal ilmiah terkait dengan fenomena *deepfake* dan landasan hukum pidana yang diberlakukan di Indonesia untuk menanggulangi pokok masalah, dan dikembangkan dengan penalaran deduktif. Penelitian dilakukan dengan metode kualitatif deskriptif dan dipaparkan dengan argumen teoritik.

HASIL DAN PEMBAHASAN

Sebuah perangkat lunak bernama Deeptrace diciptakan oleh dua peneliti Italia pada tahun 2018 dengan maksud untuk mendeteksi foto dan video hasil olahan *deepfake*. Di tahun 2019 silam, tercatat ada lebih dari 14.000 video *deepfake* yang diunggah di internet dan 96% dari video tersebut adalah konten pornografi yang melibatkan perempuan (Sloan, 2020). Manipulasi dilakukan dengan menempelkan wajah korban ke tubuh pemeran konten

pornografi sehingga seakan-akan korban sedang berada dalam aktivitas seksual tersebut. Korban dalam banyak kasus ini adalah artis atau tokoh populer. Terdapat pula sebuah situs yang secara spesifik memproduksi konten pornografi artis yang diciptakan dari olahan *deepfake*. Teror ini tidak semata-mata mengancam artis, orang biasa juga bisa dicelakai secara sengaja dengan tujuan pemerasan ataupun untuk memenuhi hasrat seksual para pelaku.

Teknologi *deepfake* sering digunakan untuk tujuan menseksualisasi korban. Melalui bantuan AI, *deepfake* dimonetisasi oleh oknum tidak bertanggungjawab yang menyediakan layanan *editing* berbayar dengan sistem isi ulang kredit. Pelanggan hanya perlu mengirimkan foto korban yang hendak disunting. Jasa pembuatan video *deepfake* juga memiliki angka permintaan yang tinggi. Biayanya berkisar dari $300 hingga US$20.000 per menit tergantung tingkat kesulitannya (Herman, 2023). Tidak berhenti sampai di sana, media yang telah dimanipulasi biasanya disertai dengan ancaman untuk disebarkan. Motivasi dari intimidasi ini adalah untuk memberikan rasa teror dan memeras korban agar memberikan sejumlah uang sebagai syarat agar tidak disebarkan. Banyak oknum yang menikmati konten hasil olahan *deepfake* meskipun mereka tau bahwa media tersebut merupakan bentuk pelecehan seksual dan melanggar hukum. Sebuah subreddit bernama r/deepfakes yang kini telah dihapus dilaporkan memiliki hampir 90.000 pengguna. Aktivitas utama anggota grup tersebut adalah saling berbagi konten pornografi dari hasil olahan *deepfake*.

Internet menjadi platform utama yang dimanfaatkan untuk konten eksplisit. Seiring bertambahnya zaman, konten pornografi juga menjadi sangat bervariasi. Hal ini tentu menguntungkan siapa saja untuk mengakses maupun mengunggah hal tidak senonoh. Preferensi dan fantasi seksual yang tidak terbatas juga dengan gampang mendapatkan tempat di situs web porno yang bisa diakses dengan gratis. Permasalahan ini mengindikasikan krisis moral dan akses pornografi yang gampang ini telah memberikan dampak negatif yang besar karena pihak yang dirugikan sangat banyak dan tidak tertutup untuk siapapun. Artinya, ini menjadi suatu ironi bahwa keamanan terhadap laman pornografi cenderung minim. Korban dari konten pornografi yang dirugikan juga seringkali menderita kerugian fisik dan psikologis yang berkepanjangan, termasuk predasi seksual, trauma emosional, *cyberbullying*, dan bahkan tendensi untuk bunuh diri. Menyebarkan konten pornografi sering disepelekan, namun memperbaiki nama baik dan menghapus jejak digital adalah sesuatu yang sulit.

Anak-anak dapat mengakses internet secara mudah karena tidak adanya batasan usia yang ketat dari penyedia laman internet. Internet menyediakan informasi yang teramat sangat banyak dan memfasilitasi rasa penasaran anak-anak yang besar sehingga ini menjadi sebuah *butterfly effect* karena anak-anak dapat terpapar hal yang tidak seharusnya. Dilansir dari survey Pew Research Center, hampir 95% remaja memiliki akses ke internet. Kementerian Pemberdayaan Perempuan dan Perlindungan Anak (Kemen PPPA) mengungkapkan 66,6% anak laki-laki dan 62,3% anak perempuan di Indonesia terekspos konten pornografi di internet (Qommarria Rostanti, 2021). Peneliti berpendapat bahwa semakin banyak remaja dan anak-anak menghabiskan waktu di internet, semakin besar kemungkinan mereka secara tidak sengaja terpapar konten eksplisit, seperti yang ada di iklan saat menjelajah internet (Pisker et al.). Pelaku *deepfake* bukan hanya menargetkan orang dewasa, namun anak-anak dan remaja di bawah umur juga turut menjadi sasaran empuk, terutama bagi pengidap kelainan pedofilia.

Frederick S. Lane, penulis Obscene Profits: The Enterpreneurs of Pornography in the Cyber Age (2000) mengatakan bahwa industri pornografi adalah salah satu industri yang sangat bersahabat dengan internet dan cerdas memanfaatkan teknologi internet. Riset di tahun 2022 silam membuktikan bahwa industri pornografi mendapatkan profit sebesar $15 miliar, di mana angka tersebut melebihi penghasilan industri Hollywood (Faisal Irfani and Windu Jusuf, 2019).

Pornografi merupakan kejahatan yang diatur secara jelas secara hukum. Di Indonesia sendiri, Pasal 4 Undang-Undang Nomor 44 Tahun 2008 tentang Pornografi mengatur bahwa

tindakan memproduksi, membuat, memperbanyak, menggandakan, menyebarluaskan, menyiarkan, mengimpor, mengekspor, menawarkan, memperjualbelikan, menyewakan, atau menyediakan pornografi dapat dijerat hukuman pidana. Ancaman pidana terhadap pelaku diatur dalam Pasal 45 Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang berbunyi "Setiap Orang yang 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 sebagaimana dimaksud dalam Pasal 27 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah)."

Hukuman pidana yang diberikan bertujuan untuk memberikan efek jera bagi pelaku dan memberikan keadilan bagi korban. Pada faktanya, jauh lebih banyak orang-orang yang berupaya mengembangkan teknologi *deepfake* dibandingkan teknologi untuk mendeteksi dan menghapusnya.

Deepfake belum diatur secara spesifik dalam undang-undang perdata atau pidana, namun konstitusi telah mengadaptasi undang-undang untuk mencakup pencemaran nama baik, penipuan identitas, atau meniru identitas yang diolah dengan *deepfake.* Indonesia memiliki beberapa dasar hukum yang dapat dipakai untuk menjerat pelaku *deepfake*. Dasar hukum yang bisa dipakai adalah Pasal 48 ayat (1) yang berbunyi "Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (1) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp2.000.000.000,00 (dua miliar rupiah)." Pasal 32 ayat (1) mengatur bahwa tindakan mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik merupakan perbuatan melawan hukum.

Pasal lain yang dapat dipakai adalah Pasal 68 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi yang berbunyi "Setiap Orang yang dengan sengaja membuat Data Pribadi palsu atau memalsukan Data Pribadi dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian bagi orang lain sebagaimana dimaksud dalam Pasal 66 dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau pidana denda paling banyak Rp6.000.000.000,00 (enam miliar rupiah)."

Kerangka hukum memiliki peran yang sangat vital dalam mengatur pembuatan dan penyebaran konten *deepfake* (Kumar, 2023). Meningkatnya jumlah misinformasi dan *deepfake* juga berdampak pada menurunnya kepercayaan masyarakat terhadap pihak berwenang. Ketidakpercayaan masyarakat terhadap pihak berwenang berimplikasi pada olahan *deepfake* yang semakin mudah tersebar luas dan dikonsumsi oleh masyarakat. Diperlukan kemajuan teknologi dari pihak keamanan *cyber* untuk mengembangkan alat pendeteksi yang lebih canggih dan mampu bersanding untuk mengidentifikasi konten *deepfake.* Adalah sebuah tantangan bagi pihak keamanan *cyber* untuk bisa menanggulangi permasalahan ini. Tantangan ini ditambah lagi dengan masyarakat yang masih kurang sadar dengan proteksi data pribadi dan relatif mudah mengkonsumsi berita hoaks karena enggan mengecek validitas suatu media. Peningkatan kesadaran dan transparansi terhadap masyarakat juga menjadi komponen penting.

Pembuktian merupakan tahap yang sangat krusial dalam hukum pidana yang secara langsung mempengaruhi berjalannya proses persidangan. Tanpa adanya proses pembuktian dan barang bukti, maka peristiwa pidana tidak bisa dianggap sah. Putusan hakim sangat dipengaruhi oleh barang bukti yang mendukung suatu tindak kejahatan. Pasal 6 ayat (2) Undang-Undang Nomor 48 Tahun 2009 tentang Kekuasaan Kehakiman menyatakan "tidak seorangpun dapat dijatuhi pidana kecuali apabila pengadilan, karena alat pembuktian yang

sah menurut undang-undang, mendapat keyakinan bahwa seorang yang dianggap dapat bertanggung jawab, telah bersalah atas perbuatan yang didakwakan atas dirinya." Diperkuat dengan Pasal 1 Angka 13 Undang-Undang Nomor 2 Tahun 2002 tentang Kepolisian yang berbunyi "penyidikan ialah serangkaian tindakan penyidik dalam hal dan menurut cara yang diatur dalam undang-undang ini untuk mencari serta mengumpulkan bukti yang dengan bukti itu membuat terang tentang tindak pidana yang terjadi dan guna menemukan tersangkanya."

Foto, video, dan rekaman suara bisa dijadikan sebagai alat bukti penting yang dibutuhkan dalam proses penyidikan. Dengan *deepfake*, media-media tersebut bisa saja dipalsukan dan sengaja diciptakan untuk merekayasa peristiwa yang tidak pernah terjadi untuk memutarbalikkan fakta. Dampak dari bukti yang tidak benar adalah semakin sulit untuk mengetahui mana yang harus dipercaya, alhasil memperlambat proses persidangan dan bahkan hingga memengaruhi putusan hakim yang akan merugikan pihak yang berperkara. Maraknya penggunaan *deepfake* membuat petugas polisi dituntut untuk meneliti barang bukti secara lebih mendalam dan memverifikasi apakah barang bukti tersebut bersifat otentik keasliannya atau tidak.

Proses persidangan kasus kejahatan *cyber* dimulai dengan aparat kepolisian membuat laporan polisi dan memanggil saksi dari pemilik *provider* internet yang digunakan pelaku, memeriksa tempat kejadian perkara untuk mengumpulkan barang bukti yang dipakai pelaku dalam menjalankan aksinya terutama di dalam perangkat komputer, melakukan pemeriksaan terhadap saksi dan meminta keterangan ahli, menangkap dan menahan pelaku untuk melakukan investigasi secara langsung, dan akhirnya menetapkan pasal yang dapat dijatuhkan untuk melanjutkan ke proses persidangan. Jaksa penuntut umum perlu membuat surat dakwaan yang diikuti dengan alat bukti yang sah dan sesuai dengan Pasal 183 KUHAP minimal berjumlah dua alat bukti dan disertai dengan keyakinan hakim (Kunci & Yustia, n.d.). Tentu yang sulit dalam proses ini adalah menemukan pelaku kejahatan yang keberadaan dan identitasnya sulit terlacak.

Fenomena ini menuntut penegak hukum untuk mengembangkan keterampilan dan proses hukum yang semakin kompleks. Teknologi yang begitu canggih memudahkan pelaku untuk menutupi identitas dan jejak digital dan mempersulit aparat penegak hukum untuk melakukan proses pelacakan. Pelaku bisa mengakses internet dari perangkat apa saja, di mana saja, dengan identitas yang disembunyikan, sehingga proses pengumpulan bukti dan alat bukti membutuhkan upaya ekstra. Virtual Private Network (VPN) turut membantu pelaku dalam melangsungkan kejahatan karena VPN dirancang untuk menyembunyikan identitas IP Address penggunanya. Sebagaimana pepatah mengatakan "tidak ada kejahatan yang sempurna", kejahatan konvensional selalu meninggalkan jejak. Kemudahan akses internet di zaman ini telah membuat kejahatan *cyber* dapat saja dilakukan tanpa jejak dan tidak terlihat oleh satu orang pun saksi. Oleh karena itu, aparat penegak hukum tidak hanya perlu meningkatkan keterampilan untuk mendeteksi *deepfake*, namun juga berinvestasi pada kemampuan mengatasi tantangan teknologi yang akan datang (European Union Agency for Law Enforcement Cooperation, 2022).

Analisa digital dan forensik digital lahir sebagai disiplin ilmu yang bertujuan untuk bersanding dalam menanggulangi kejahatan *cyber*. Ancaman teknologi AI dan internet membutuhkan peningkatan akan alat komputasi yang efisien untuk mendeteksi dan memblokir konten pornografi (Cifuentes, Lucila and Javier, 2021). Reddit dan Pornhub telah melarang pornografi dari hasil olahan *deepfake* dan berupaya menindaklanjuti setiap laporan dari pengguna atas konten tersebut.

Amerika Serikat telah mengambil upaya hukum dengan mengesahkan National Defense Authorization Act (NDAA). Undang-undang tersebut mengatur bahwa Direktur Intelijen Nasional Amerika Serikat diwajibkan untuk melaporkan penggunaan *deepfake* oleh pemerintah internasional. Kendati demikian, kebijakan ini dinilai belum sepenuhnya cukup

untuk mengatasi masalah yang ditimbulkan oleh *deepfake*, karena kemajuan teknologi terus melaju cepat dan memiliki inovasi yang belum tentu bisa dijangkau secara yuridis.

Sejak pembentukannya, baru lima negara bagian di Amerika Serikat yang turut mengesahkan undang-undang mengenai teknologi *deepfake*. Mulai tahun 2019, negara bagian Texas dan California melarang penggunaan *deepfake* untuk mempengaruhi pemilu mendatang. Undang-undang negara bagian California dan Virginia juga disahkan di tahun yang sama untuk melarang pembuatan dan penyebaran konten pornografi *deepfake* non-konsensual. Setahun kemudian, New York mengesahkan undang-undang yang menetapkan hak untuk mengambil tindakan hukum terhadap publikasi *deepfake* yang melanggar hukum. Rancangan undang-undang untuk mengatur AI juga telah diusulkan dan disahkan di beberapa negara bagian pada tahun 2022 (deansr, 2023).

KESIMPULAN

Minimnya regulasi dan luasnya penyebaran kejahatan tidak hanya mengancam tokoh populer, namun berpotensi membahayakan siapapun. Media yang telah diunggah di internet dapat diakses oleh siapa saja, sehingga foto, video, dan suara siapapun yang tersebar di internet dapat dijadikan sebagai target *deepfake*. Dampaknya terhadap privasi dan keamanan pribadi pasti menjadi efek kejahatan *cyber* yang harus diawasi. Apabila tidak ditanggulangi dengan tegas, kejahatan *deepfake* dengan perkembangannya yang pesat bisa menghancurkan kehidupan seseorang melalui penyebaran informasi yang tidak benar. Hukum bersifat dinamis, namun tidak cukup dinamis untuk menyaingi kecepatan kejahatan dunia maya yang terlampau inovatif. Proses hukum terkait kasus ini menjadi tugas yang tidak gampang karena berhadapan langsung dengan teknologi yang kecerdasannya melampaui kecerdasan manusia. Teknologi internet juga tidak dilengkapi kompas moral, hanya manusia saja yang mampu memasukkan sistem ke dalam teknologi internet.

Oleh karena itu, teknologi internet pada hematnya dikendalikan oleh manusia dan tidak bisa ditetapkan sebagai subjek hukum. Pelanggaran yang dilakukan oleh AI menjadi tanggung jawab sepenuhnya orang yang mengoperasikannya. Pengguna internet harus kritis dalam menggunakan teknologi agar tidak menjadi korban dari penyalahgunaan *deepfake*. Dengan manfaat yang begitu besar, pengguna internet dihimbau untuk tidak menelan informasi secara cuma-cuma dan mencari validitas atas informasi yang dikonsumsi. Di samping itu, penegakan payung hukum terkait penggunaan AI tentunya harus ditegakkan secara ekstra untuk meminimalisir resiko dari oknum yang tidak bertanggungjawab. Aparat penegak hukum perlu melihat kondisi ini sebagai urgensi untuk menindak serius permasalahan *deepfake* dan mencari langkah untuk mencapai upaya preventif dan represif. Aparat penegak hukum dan pihak keamanan *cyber* perlu meningkatkan kompetensi dalam melakukan penyelidikan dan mengumpulkan bukti yang sah untuk dilanjutkan di persidangan. Apabila hal ini tidak ditindak, maka pelaku kejahatan *deepfake* akan terus menjalankan aksinya dan merugikan siapa saja, bahkan orang yang tidak dikenal sekalipun.

Referensi

Cifuentes, J., Lucila, A., & Javier, L. (2021). A survey of artificial intelligence strategies for automatic detection of sexually explicit videos. *Multimedia Tools and Applications*, *81*(3), 3205–3222. https://doi.org/10.1007/s11042-021-10628-2

Europol. (2022). *Facing reality? - Publications Office of the EU*. Publications Office of the EU. https://op.europa.eu/en/publication-detail/-/publication/b844aa2b-dbd4-11ec-a534-01aa75ed71a1/language-en

Kunci, K., & Yustia, M. (n.d.). *Pembuktian dalam Hukum Pidana Indonesia terhadap Cyber Crime*.

Liu, M., & Zhang, X. (2023). Deepfake Technology and Current Legal Status of It. *Proceedings of the 2022 3rd International Conference on Artificial Intelligence and Education (IC-ICAIE 2022)*, 1308–1314. https://doi.org/10.2991/978-94-6463-040-4_194

Pahajow, A. A. J. (2016). *Pembuktian terhadap Kejahatan Dunia Maya dan Upaya Mengatasinya Menurut Hukum Positif di Indonesia*.

Pisker, B., Dokic, K., & Martinovic, M. (n.d.). *Measuring Search Engine Bias in European Women's Image Results using Machine Learning Algorithms*.

Unpad, P. F. (2023, August 24). *Perlindungan Hukum bagi Korban Deepfake Pornografi: Evaluasi Efektivitas Hukum Positif dan Kebutuhan akan Reformasi Hukum*. Medium. https://pleads-fhunpad.medium.com/perlindungan-hukum-bagi-korban-deepfake-pornografi-evaluasi-efektivitas-hukum-positif-dan-1fb2bb20da35

Artificial intelligence (AI) | Definition, Examples, Types, Applications, Companies, & Facts | Britannica. (2023). In *Encyclopædia Britannica*. https://www.britannica.com/technology/artificial-intelligence

deansr. (2023, June 20). *The High Stakes of Deepfakes: The Growing Necessity of Federal Legislation to Regulate This Rapidly Evolving Technology - Princeton Legal Journal*. Princeton Legal Journal. https://legaljournal.princeton.edu/the-high-stakes-of-deepfakes-the-growing-necessity-of-federal-legislation-to-regulate-this-rapidly-evolving-technology/

Faisal Irfani, & Windu Jusuf. (2019, July 2). *Berapa Besar Pendapatan Industri Porno?* Tirto.id; Tirto.id. https://tirto.id/berapa-besar-pendapatan-industri-porno-edqa Sloan, M. (2020).

Herman. (2023, June 12). *Makin Meresahkan, Foto di Medsos Dijadikan Deepfake Porno untuk Pemerasan*. Beritasatu.com; BeritaSatu.com. https://www.beritasatu.com/ototekno/1050805/makin-meresahkan-foto-di-medsos-dijadikan-deepfake-porno-untuk-pemerasan/2

Kumar, N. (2023, June 25). *What is Deepfake Technology? Origin and Impact*. Analytics Insight. https://www.analyticsinsight.net/what-is-deepfake-technology-origin-and-impact/#:~:text=Origin%20of%20Deepfake%20Technology%3A,and%20his%20team%20in%202014

Qommarria Rostanti. (2021, November 30). *66,6 Persen Anak Tonton Pornografi di Media Daring*. Republika Online; Republika Online. https://news.republika.co.id/berita/r3dtc3425/666-persen-anak-tonton-pornografi-di-media-daring

Sloan, M. (2020, July 21). *Deepfakes, explained | MIT Sloan*. MIT Sloan. https://mitsloan.mit.edu/ideas-made-to-matter/deepfakes-explained

Song, D. (2019, September 24). *A Short History of Deepfakes - David Song - Medium*. Medium; Medium. https://medium.com/@songda/a-short-history-of-deepfakes-604ac7be6016