Pemuliaan Keadilan
Volume. 2, Nomor. 1, Tahun 2025
e-ISSN : 3063-282X; dan p-ISSN : 3063-2811; Hal. 60-73
DOI: https://doi.org/10.62383/pk.v2i1.402
Available online at: https://ejournal.appihi.or.id/index.php/pk

Pengaturan Hukum Pidana di Indonesia Terhadap Penyalahgunaan Teknologi *Artificial Intelligence Deepfake* Dalam Melakukan Tindak Pidana *Cybercrime*

Patricia Morisa Banfatin[1*], Karolus Kopong Medan[2], Debi F.Ng. Fallo[3]
[1-3]Universitas Nusa Cendana, Indonesia

Alamat Kampus: Jln Adisucipto, Penfui, Kupang, Nusa Tenggara Timur
Korespondensi penulis: patriciamorisabanfatin@gmail.com[*]

Abstract.*The development of artificial intelligence deepfake technology has opened up new opportunities in various fields to help speed up human work. However, on the other hand, this technology can also be misused to commit crimes. This research is a Normative Juridical research with a statutory approach and a conceptual approach, and examines the sources of legal materials according to the main problem, and uses prescriptive analysis techniques.The results of the study show: (1) The activity of using artificial intelligence deepfake technology that can cause cybercrime occurs due to attacks on the system, namely AI botnet attacks that have been infected by malicious software and Generative Adversarial Network attacks that have artificial neural networks that can produce data that is similar to the original data so that it is used as a means of committing crimes, and (2) Criminal law regulations in Indonesia regarding the misuse of artificial intelligence deepfake technology in committing cybercrime have not been regulated comprehensively, so that currently it is necessary to establish clear legal regulations in order to provide legal protection for every community.*

Keywords: *Criminal Law Regulations, Artificial Intelligence, Deepfake, Criminal Acts, Cybercrime.*

Abstrak. Perkembangan teknologi *artificial intelligence deepfake* telah membuka peluang baru dalam berbagai bidang untuk membantu mempercepat pekerjaan manusia. Namun, di sisi lain, teknologi ini juga dapat disalahgunakan untuk melakukan tindak pidana. Penelitian ini merupakan penelitian Yuridis Normatif dengan pendekatan perundang-undangan dan pendekatan konsep, serta menelaah sumber bahan hukum sesuai dengan pokok permasalahan, dan menggunakan teknik analisis preskriptif. Hasil penelitian menunjukan: (1) Aktivitas penggunaan teknologi *artificial intelligence deepfake* yang dapat menyebabkan tindak pidana *cybercrime* terjadi karena adanya serangan pada sistem yakni serangan botnet AI yang telah terinfeksi oleh perangkat lunak berbahaya dan serangan *Generative Adversarial Networks* yang memiliki jaringan syaraf tiruan yang dapat menghasilkan data yang mirip dengan data asli sehingga digunakan sebagai sarana melakukan tindak pidana, dan (2) Pengaturan hukum pidana di Indonesia terhadap penyalahgunaan teknologi *artificial intelligence deepfake* dalam melakukan tindak pidana *cybercrime* belum diatur secara komprehensif, sehingga saat ini perlu untuk ditetapkan pengaturan hukum yang jelas agar dapat memberikan perlindungan hukum bagi setiap masyarakat.

Kata Kunci: Pengaturan Hukum Pidana, *Artificial Intelligence*, *Deepfake*, Tindak Pidana, *Cybercrime*

1. LATAR BELAKANG

Perkembangan kemajuan teknologi saat ini diibaratkan seperti pedang bermata dua, di satu sisi teknologi hadir untuk memberikan pengaruh positif yakni dapat membantu memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan dan membantu mempercepat aktivitas manusia. Namun di sisi lain kehadiran teknologi juga bisa memberikan dampak negatif yang berujung menjadi perbuatan melawan hukum yang tentunya ini sebagai suatu perbuatan yang merugikan berbagai pihak yang terkena dampaknya.

Salah satu hal yang menjadi perhatian dunia saat ini adalah kehadiran teknologi bernama *artificial intelligence* atau di Indonesia dikenal dengan teknologi kecerdasan buatan.

Received: November 16,2024; Revised: November 30,2024; Accepted: Desember 14,2024; Online Available : Desember 16,2024

Sebuah teknologi yang diciptakan dengan berbagai kemampuannya untuk membantu pekerjaan manusia dalam berbagai bidang misalnya dalam sektor pendidikan, kesehatan, transportasi, keamanan, industri dan agrikultur.

Contoh nyata implementasi AI dalam bidang hukum atau legaltech telah memberikan penyediaan layanan hukum di mana pada tahun 2017 di Hangzhou, Cina telah ada Hakim AI yang mampu menangani sengketa hukum terkait kasus hak cipta dan klaim pertanggungjawaban produk di ranah jual beli online. Kemudian, pada 26 Februari 2018, laman Daily Mail melaporkan kompetensi memahami kontrak antara AI dengan para pengacara terkemuka. Mereka diberikan kesempatan mengidentifikasi permasalahan hukum dari 30 kontrak dalam waktu empat jam. AI ternyata mampu mencapai tingkat akurasi 85 persen. Di Indonesia sendiri, hukumonline.com telah meluncurkan platform LIA (Legal Intelligence Assistant) yang diklaim sebagai chatbot pertama di Indonesia yang dapat membantu masyarakat dalam memperoleh informasi terkait hukum perkawinan, hukum perceraian, dan hukum waris.

Ironisnya, kehadiran teknologi saat ini sudah tidak sesuai lagi dengan tujuan pembuatannya untuk membantu pekerjaan manusia. Artificial intelligence telah disalahgunakan oleh sebagian kalangan sehingga menimbulkan tindak pidana.

Dampak negatif kemajuan teknologi artificial intelligence yang mengancam dan membahayakan saat ini adalah kehadiran salah satu sistem AI bernama *deepfake*. *Deepfake* sendiri dapat diartikan sebagai jenis teknologi kecerdasan buatan atau AI yang digunakan untuk membuat video atau audio yang menampilkan orang yang berkata atau melakukan sesuatu yang mereka tidak pernah katakan atau lakukan. *Deepfake* dibuat dengan menggunakan teknik pembelajaran mesin untuk memanipulasi gambar dan video. Umumnya, penggunaan sebatas untuk hiburan, namun ditangan orang yang tidak bertanggung jawab maka *deepfake* menjadi media hoax yang menyesatkan.

Aplikasi *deepfake* dalam kemajuan teknologi informasi saat ini dapat digunakan sebagai sarana melakukan tindak pidana *cybercrime* di dunia maya yakni melakukan tindak pidana *confidentiality, integrity, dan availability data* atau sistem komputer seperti*: hacking, crecking, phreaking, viruses,* dan lain-lain serta tindak pidana yang dilakukan dengan menggunakan media teknologi informasi dan komunikasi sebagai alat, seperti: *cyberfraud, credit card fraud, cyberpornography, cyberstalking, cyberterrorism*, dan lain-lain.

Di Indonesia sendiri terdapat beberapa contoh kasus penyalahgunaan *deepfake* dalam melakukan tindak pidana *cybercrime* yakni kasus *deepfake* bermuatan konten pornografi yang

menimpa para selebriti, diantaranya adalah kasus tersebarnya video pornografi yang menimpa Nagita Slavina.

Selain itu, kasus rekayasa teknologi *deepfake* juga menimpa Presiden Republik Indonesia, dimana beredar sebuah video pada berbagai *platform* digital yang menampilkan Presiden Joko Widodo sedang menyampaikan pidato kenegaraan menggunakan Bahasa Mandarin dengan fasih, tetapi hal ini telah ditegaskan oleh Direktur Jenderal Aplikasi Informatika Kementerian Komunikasi dan Informatika Republik Indonesia bahwa pidato tersebut merupakan video hasil suntingan yang menyesatkan. Hasil penelusuran Tim AIS Kementerian Komunikasi dan Informatika menemukan kesamaan video yang diunggah oleh kanal YouTube The U.S Indonesia Society (USINDO) pada 13 November 2015 lalu. Secara visual, video tersebut identik, tetapi telah disunting dengan memanfaatkan teknologi *deepfake*.

Contoh-contoh kasus di atas pada intinya merupakan hal yang merugikan dan sangat mengganggu. Kehadiran teknologi *deepfake* ini tidak hanya dapat merubah wajah seseorang saja, tetapi juga bisa merubah audio, gerak gerik, serta rincian visual yang sangat melekat dengan korban. Sehingga manipulasi kejahatan teknologi ini dapat merusak reputasi dan nama baik setiap korban yang terkena dampaknya.

Sebagaimana teori yang dikemukakan oleh Soerjono Soekanto, ada lima faktor yang mempengaruhi penegakan hukum yakni: faktor hukumnya sendiri, faktor penegak hukum, faktor sarana atau fasilitas, faktor masyarakat dan faktor kebudayaan.

Kasus-kasus *deepfake* kian hari terus bertambah dikarenakan adanya kendala dalam pengaturannya yakni ketiadaan norma yang mengatur secara khusus pertanggungjawaban pidana terhadap pelaku kejahatan artificial intelligence *deepfake* dalam melakukan tindak pidana *cybercrime*. Oleh karena itulah calon peneliti ingin mengkaji lebih jauh permasalahan ini.

2. METODE PENELITIAN

Penelitian ini merupakan penelitian hukum yuridis normatif. Pendekatan yang dipakai dalam penelitian ini adalah Pendekatan Perundang-Undangan (*Statute Approach*) dan Pendekatan Konsep (*Conceptual Approach*). Penelitian ini menggunakan bahan hukum berupa bahan hukum primer, bahan hukum sekunder dan bahan hukum tersier.

Pengumpulan bahan hukum dalam penelitian ini menggunakan sumber terdiri dari buku-buku, jurnal-jurnal, peraturan perundang-undangan, skripsi, artikel yang berkaitan dengan pembahasan dalam penelitian ini, pendapat para sarjana, kasus-kasus hukum, yurisprudensi, situs-situs lembaga maupun instansi yang berkaitan dengan permasalahan

penyalahgunaan *artificial intelligence deepfake* dalam melakukan tindak pidana *cybercrime.* Teknik analisis yang digunakan dalam penelitian ini menggunakan analisis preskriptif.

3. HASIL DAN PEMBAHASAN

Penggunaan Teknologi *Artificial Intelligence Deepfake* Yang Dapat Dikategorikan Sebagai Tindak Pidana *Cybercrime*

1. Serangan Botnet *Artificial Intelligence*

Botnet merupakan sekumpulan komputer yang sudah terinfeksi oleh perangkat lunak berbahaya (*malware*) yang dijalankan oleh botmaster. Perangkat yang sudah terinfeksi seperti komputer, kamera web, cctv dan perangkat seluler dapat dioperasikan dan dipantau oleh botmaster. Botnet menargetkan sistem operasi window dengan menyebar melalui spam pada *e-mail* dan file unduhan yang sudah terinfeksi. Tujuannya adalah untuk melancarkan serangan pada target atau korban, yang dapat berupa pemerasan.

Kekuatan botnet terletak pada kapasitasnya untuk menghindari sistem keamanan dan melakukan serangan skala besar berkat berbagai taktik seperti penyembunyian data paket dan data paket terenkripsi. Botnet dapat bersembunyi dari sistem perlindungan, kemudian menunggu tahap dan distribusi kelas yang tidak seimbang. Hal ini kemudian dijadikan sarana untuk melakukan tindak pidana.

2. Serangan *Generative Adversarial Networks*

Generative Adversarial Networks (GAN's) diperkenalkan pertama kali oleh Ian J. Goodfellow bersama tujuh orang lainnya pada tahun 2014 melalui Jurnal mereka yang berjudul *Generative Adversarial Nets*. Penggunaan *Generative Adversarial Networks* (GAN's) sangat berbeda dengan Algoritma *Deep Learning* lainnya, dimana algoritma lainnya memanfaatkan penuh terhadap dataset yang ada dimana dataset tersebut dilatih untuk memaksimalkan hasil akurasi dari setiap pengujian yang dilakukan, semakin banyak dataset yang dimiliki maka semakin baik hasil yang didapatkan . *Generative Adversarial Networks* (GAN's) memiliki pendekatan yang berbeda dengan algoritma lainnya, algoritma ini menggunakan dua jaringan syaraf buatan (*neural network*) untuk menyelesaikan permasalahan yang ada. Kedua jaringan syaraf buatan tersebut adalah Generator yang berfungsi untuk mengambil sampel data dari dataset, dan Diskriminator yang berfungsi untuk mengklasifikasikan bahwa sampel data itu bernilai asli atau palsu. Dengan adanya kedua neural network tersebut, maka akan dihasilkan suatu data yang baru yang sangat menyerupai data inputan-nya.

Kehadiran GANs sebagai jaringan saraf tiruan dapat menghasilkan data yang mirip dengan data asli, hal ini kemudian dijadikan alat pembuatan *deepfake* yakni sebagai sarana memanipulasi media untuk menciptakan konten palsu.

Teknik *Deepfake* dengan aplikasi *FakeApp* digunakan untuk menukar wajah seseorang dengan orang lain. *FakeApp* atau aplikasi palsu ini merupakan perangkat lunak yang membutuhkan sejumlah data yang besar untuk menghasilkan data yang baik. Data ini akan disalurkan ke sistem untuk memproses model wajah seseorang yang ditargetkan. Penciptaan wajah palsu ini melibatkan ekstraksi gambar dan video yang nantinya menghasilkan gambar atau video palsu yang sempurna.

Selanjutnya adalah teknik ekspresi dinamis. Teknik merupakan teknik menggunakan waktu dan sistem dengan ketelitian tinggi yang mampu merekonstruksi lebih detail. Generasi *deepfake* selanjutnya adalah teknik pelacakan dengan pendekatan model wajah parametrik. Pelacakan awal adalah dengan memberi pencahayaan ke sekitar area mulut termasuk ke proksi gigi dan ke dalam mulut. Teknik ini menghasilkan gambar yang detail dan menghasilkan gambar yang lebih dekat. Berdasarkan paparan tersebut tentunya perkembangan teknologi informasi dan kecerdasaan buatan atau AI yang sangat pesat memunculkan sebuah tantangan yang sangat besar. Hal ini karena hampir semua institusi baik pemerintahan, perusahaan, dan masyarakat menggunakan serta bergantung pada sistem informasi digital sehingga rentan terhadap ancaman.

Penggunaan teknologi *artificial intelligence deepfake* yang menimbulkan masalah keamanan siber terjadi karena adanya serangan *malware*, yang mana dapat mempermudah para *hacker* untuk mengidentifikasi dan menganalisis kelemahan berbagai variasi *software* secara efisien. Aktivitas para *hacker* inilah yang kemudian menyebabkan terjadinya tindak pidana siber.

Ada dua metode untuk membuat *deepfake*, pertama yaitu menggunakan algoritma AI bernama *encoder*. Pertama-tama, kita harus mengumpulkan ribuan foto dari dua orang yang berbeda. Lalu, *encoder* akan memprosesnya untuk menemukan kemiripan dan memancarkan wajah A ke wajah B di video lain. Selain *encoder*, *deepfake* juga bisa dibuat menggunakan *Generative Adversarial Network* atau GAN yang menggunakan komponen *generator* dan *discriminator* untuk menghasilkan data sintesis.

Pengaturan Hukum Pidana Di Indonesia Terhadap Penyalahgunaan Teknologi *Artificial Intelligence Deepfake* Dalam Melakukan Tindak Pidana *Cybercrime*

Saat ini pengaturan hukum pidana di Indonesia terhadap penyalahgunaan teknologi *artificial intelligence deepfake* dalam melakukan tindak pidana *cybercrime* belum diatur secara khusus. Namun dalam pelaksanaan menindak pelaku yang melakukan tindak pidana terdapat pengaturan hukum yang dapat dijadikan acuan yakni:

1. **Undang-Undang Republik Indonesia Nomor 1 Tahun 2023 Tentang Kitab Undang-Undang Hukum Pidana**
   a. **Pasal 243 Undang-Undang Republik Indonesia Nomor 1 Tahun 2023 Tentang Kitab Undang-Undang Hukum Pidana**

      Pasal ini dapat menjadi dasar untuk mengatur penyalahgunaan AI *deepfake* yang tidak sesuai dengan ketentuan perundang-undangan yang berlaku, namun demikian masih terdapat hambatan dalam proses penegakkan hukum karena sulit untuk mendeteksi pembuat konten *deepfake*.

   b. **Pasal 407 Undang-Undang Republik Indonesia Nomor 1 Tahun 2023 Tentang Kitab Undang-Undang Hukum Pidana**

      Ketentuan dalam pasal ini hadir untuk melindungi martabat dan hak asasi manusia. Teknologi *deepfake* memungkinkan siapa saja untuk membuat konten palsu khususnya bermuatan pornografi yang melibatkan orang lain tanpa adanya persetujuan. Pasal ini juga menegaskan bahwa pembuatan konten pornografi untuk kepentingan pribadi tidak dapat dipidana, artinya bahwa jika kedua belah pihak saling bersepakat maka tidak dapat dijatuhi hukuman. Untuk mempertegas ketentuan ini maka perlu untuk membenahi aturan hukum di Indonesia yang lebih spesifik mengatur tindakan penyalahgunaan teknologi AI *deepfake*.

   c. **Pasal 433 Undang-Undang Republik Indonesia Nomor 1 Tahun 2023 Tentang Kitab Undang-Undang Hukum Pidana**

      Ketentuan penjelasan dalam pasal ini lebih lanjut menegaskan bahwa perbuatan pencemaran adalah jika perbuatan penghinaan yang dilakukan dengan cara menuduh, baik secara lisan, tulisan, maupun dengan gambar, yang menyerang kehormatan dan nama baik seseorang, sehingga merugikan orang tersebut. Perbuatan yang dituduhkan tidak perlu harus suatu Tindak Pidana. Sifat melawan hukum dari perbuatan tersebut ditiadakan karena adanya alasan pemaaf yaitu jika perbuatan tersebut dilakukan untuk kepentingan umum atau karena terpaksa membela diri.

d. Pasal 492 Undang-Undang Republik Indonesia Nomor 1 Tahun 2023 Tentang Kitab Undang-Undang Hukum Pidana

Pasal ini yang mengatur tentang Tindak Pidana penipuan. Perbuatan materiel dari penipuan adalah membujuk seseorang dengan berbagai cara yang disebut dalam ketentuan ini, untuk memberikan sesuatu Barang, membuat utang atau menghapus piutang. Dengan demikian, perbuatan yang langsung merugikan itu tidak dilakukan oleh pelaku Tindak Pidana, tetapi oleh pihak yang dirugikan sendiri. Perbuatan penipuan baru selesai dengan terjadinya perbuatan dari pihak yang dirugikan sebagaimana dikehendaki pelaku. Barang yang diberikan, tidak harus secara langsung kepada pelaku Tindak Pidana tetapi dapat juga dilakukan kepada orang lain yang disuruh pelaku untuk menerima penyerahan itu.

Dalam kaitannya dengan penyalahgunaan AI *deepfake*, pelaku dapat memanfaatkan teknologi ini untuk melakukan tindakan penipuan, baik menggunakan audio, video maupun foto. Tindakan ini telah terjadi dan beberapa kasus sempat dipercayai oleh masyarakat, tetapi dengan adanya tindakan lebih lanjut oleh aparat hukum maka dapat dibuktikan bahwa hal tersebut adalah bentuk penipuan yang menyesatkan publik.

Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor I1 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik

Ketentuan-ketentuan yang mengatur kriminalisasi perbuatan yang termasuk dalam tindak pidana *cybercrime* atas penyalahgunaan teknologi *artificial intelligence deepfake* adalah sebagai berikut.

a. Pasal 27 Undang-Undang Informasi dan Transaksi Elektronik

Ketentuan Pasal 27 menegaskan bahwa perbuatan yang dikriminalisasi adalah perbuatan menyiarkan, mempertunjukkan, mendistribusikan, mentransmisikan atau membuat dapat diaksesnya informasi elektronik atau dokumen elektronik yang memiliki muatan yang melanggar beberapa tindak pidana dalam KUHP, yakni tindak pidana kesusilaan dan perjudian yang mana hal tersebut dilakukan “dengan sengaja” dan “tanpa hak”.

Berkaitan dengan tindak pidana *cybercrime* pelaku dapat dijerat dengan pasal ini apabila menggunakan teknologi *artificial intelligence deepfake* sebagai sarana untuk melakukan kejahatan siber dalam menyiarkan, mempertunjukkan, mendistribusikan, mentransmisikan atau membuat dapat diaksesnya informasi elektronik atau dokumen elektronik yang memiliki muatan yang melanggar kesusilaan dan perjudian. Namun pasal ini

masih memiliki kekurangan karena tidak mengatur mengenai pelaku pembuatan foto atau video AI *deepfake*, sehingga dapat dipakai pelaku sebagai celah untuk terus melakukan aksi kejahatannya.

b. Pasal 27A Undang-Undang Informasi dan Transaksi Elektronik

Ketentuan Pasal 27 A pada intinya menegaskan bahwa adanya jaminan hukum untuk melindungi hak asasi setiap orang, dimana setiap individu memiliki hak untuk menjaga kehormatan dan nama baiknya. Dalam penyalahgunaan *artificial intelligence deepfake* seringkali pelaku menggunakan teknologi ini untuk menyebarkan berita bohong dan menyesatkan masyarakat sehingga dengan adanya pengaturan ini maka dapat mencegah penyebaran berita bohong yang dapat merusak reputasi seseorang atau kelompok, serta menciptakan ruang digital yang sehat dan bebas dari ujaran kebencian, fitnah, dan informasi yang tidak benar.

Namun kendati masih terdapat tantangan dalam penerapan pasal ini meskipun telah mengalami perbaikan yang mana seringkali sulit untuk membedakan antara kritik yang membangun dengan tindakan yang bersifat pencemaran nama baik sehingga pasal ini masih berpotensi disalahgunakan untuk membungkam kritik atau kepentingan pribadi.

c. Pasal 27 B Undang-Undang Informasi dan Transaksi Elektronik

Kehadiran *deepfake* dapat dijadikan sarana melakukan kejahatan oleh pelaku. Sistem yang ada dapat dirancang sedemikian rupa untuk menciptakan sebuah konten yang terlihat asli namun sebenarnya palsu. Pasal ini tidak membahas secara spesifik perlindungan identitas digital dan mekanisme pengaduan untuk korban *deepfake.* Hal ini tentu berbahaya mengingat kecanggihan *deepfake* yang dapat meniru gerak gerik dan suara seseorang dan bisa di pakai oleh pelaku untuk melakukan penipuan.

d. Pasal 28 Undang-Undang Informasi dan Transaksi Elektronik

Ketentuan Pasal 28 Ayat (1) mengatur tentang pemberitahuan bohong atau informasi menyesatkan yang mengakibatkan kerugian material bagi konsumen. Pada dasarnya tindak pidana ini merupakan pelanggaran hukum karena perbuatannya menyebarkan berita bohong dan menyesatkan. Namun dalam rumusan tindak pidana tersebut disyaratkan adanya akibat yaitu kerugian konsumen dalam transaksi elektronik. Pasal 28 Ayat (1) tersebut dimaksudkan untuk memberikan perlindungan pada konsumen dalam transaksi elektronik.

Penggunaan teknologi yang tidak tepat sasaran dapat menyebabkan kerusuhan. Dengan kehadiran pasal ini sebagai bentuk upaya mencegah dan menjaga keamanan di ruang digital maupun dalam masyarakat agar tidak terjadinya penyebaran informasi yang merugikan khususnya informasi dengan menggunakan teknologi AI *deepfake.*

e. Pasal 29 Undang-Undang Informasi dan Transaksi Elektronik

Pasal ini mengatur tentang ancaman kekerasan dan/ atau menakut-nakuti dengan mengirim ancaman secara langsung kepada korban. Tindakan ancaman kekerasan yang dimaksud menimbulkan rasa takut baik yang dilakukan dengan kata-kata atau yang dilakukan melalui teknologi. Pengaturan ini penting mengingat kehadiran teknologi *artificial intelligence deepfake* saat ini digunakan pelaku kejahatan untuk melakukan ancaman baik seksual atau keamanan terhadap seseorang sehingga menimbulkan ketakutan pada korban.

f. Pasal 31 Undang-Undang Informasi dan Transaksi Elektronik

Ketentuan dalam Pasal 31 mengatur perbuatan *illegal interception* yaitu intersepsi atau penyadapan informasi dan/ atau dokumen elektronik milik orang lain dan intersepsi transmisi informasi dan/ atau dokumen elektronik milik orang lain. Intersepsi atau penyadapan yang dikriminalisasi dan diancam dengan pidana dikecualikan untuk intersepsi yang dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan atau institusi penegak hukum lainnya, namun harus dilakukan sesuai dengan ketentuan dalam perundang-undangan untuk menghindari penyalahgunaan kewenangan oleh aparat penegak hukum.

g. Pasal 32 Undang-Undang Informasi dan Transaksi Elektronik

Ketentuan ini hadir dengan tujuan untuk melindungi privasi dan menjamin keamanan data seseorang dari akses ilegal, termasuk akses ilegal karena penyalahgunaan teknologi AI *deepfake*. Namun, dalam implementasinya masih terdapat banyak kasus penyalahgunaan teknologi AI *deepfake* sehingga pasal ini masih belum dapat mencegah pergerakan pelaku karena keterbatasan sistem elektronik yang belum memadai.

h. Pasal 33 Undang-Undang Republik Informasi dan Transaksi Elektronik

Pasal ini termasuk dalam *system interference*, yaitu melakukan tindakan apapun yang mengakibatkan terganggunya sistem elektronik dan/atau sistem elektronik tidak bekerja sebagaimana mestinya. Dalam pasal ini juga dirumuskan secara umum untuk semua jenis

tindakan *system interference*, yang tampak pada penggunaan kata-kata "melakukan tindakan apapun".

i. Pasal 34 Undang-Undang Tentang Informasi dan Transaksi Elektronik

Ketentuan dalam pasal ini yang dilarang adalah memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki perangkat keras atau perangkat lunak komputer yang dirancang atau secara khusus dikembangkan untuk memfasilitasi dilakukannya tindak pidana siber, sandi, kode akses atau sejenisnya tetapi perbuatan ini dikecualikan apabila digunakan dalam hal penelitian, pengujian sistem elektronik dan perlindungan sistem komputer. Perbuatan yang menyebabkan terjadinya tindak pidana termasuk juga dalam penyalahgunaan AI *deepfake* , sehingga pelaku yang melanggar unsur-unsur tindak pidana sebagaimana yang tercantum dalam pasal ini dapat dijerat sesuai ketentuan yang berlaku.

j. Pasal 35 Undang-Undang Tentang Informasi dan Transaksi Elektronik

Ketentuan Pasal 35 termasuk dalam perbuatan pemalsuan dengan menggunakan sistem komputer. Perbuatan yang dikriminalisasi adalah manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar dianggap seolah-olah data otentik. Perbuatan pemalsuan dalam tindak pidana siber biasanya dilakukan menggunakan aplikasi palsu dalam menjalankan aksi kejahatan yang dilakukan oleh pelaku, salah satunya juga dapat dilakukan dengan AI *deepfake* dengan memanipulasi data yang ada sehingga dapat dipakai untuk melakukan penipuan.

4. KESIMPULAN DAN SARAN

Kesimpulan

1. Keberadaan teknologi *artificial intelligence deepfake* saat ini merupakan bukti bahwa dunia telah mengalami perkembangan yang pesat. Teknologi AI *deepfake* terus berkembang dengan cepat, menghadirkan tantangan baru dalam upaya pencegahan dan penindakan terhadap tindak pidana *cybercrime* yang memanfaatkan teknologi ini. Penyalahgunaan AI *deepfake* tidak hanya mengancam privasi individu, tetapi juga dapat merusak reputasi, memanipulasi opini publik, dan mengganggu stabilitas ekonomi. Penggunaan teknologi AI *deepfake* yang dapat dikategorikan sebagai tindak pidana *cybercrime* terjadi karena adanya serangan pada perangkat yang telah terinfeksi oleh virus-

virus berbahaya yakni serangan botnet dan serangan GAN's yang dapat merugikan berbagai pihak. Kasus-kasus penyalahgunaan teknologi AI *deepfake* adalah bukti ketidak bijaksana dalam menggunakan teknologi.

2. Pengaturan hukum yang mengatur tentang penggunaan teknologi AI *deepfake* belum diatur secara spesifik dalam perundang-undangan di Indonesia. Hal ini yang kemudian menjadi hambatan dalam proses penegakan hukum sehingga menciptakan celah yang dapat dimanfaatkan oleh pelaku kejahatan siber. Penyalahgunaan AI *deepfake* adalah ancaman nyata terhadap keamanan digital. Sejatinya keberadaan AI *deepfake* yang awalnya digunakan sebagai sarana hiburan telah berubah menjadi alat yang ampuh untuk memanipulasi serta melakukan penipuan dengan dukungan algoritma yang terdapat pada AI.

Saran

1. Pemerintah perlu untuk membangun sistem deteksi yang lebih canggih untuk mengetahui serangan siber yang memanfaatkan teknologi *artificial intelligence deepfake.*
2. Maraknya kasus *artificial intelligence deepfake* menuntut adanya kerangka hukum yang komprehensif untuk melindungi masyarakat dari dampak negatif penyalahgunaan teknologi ini. Dengan melakukan modernisasi dalam penegakan hukum merupakan hal penting, karena seiring dengan berjalannya waktu kejahatan pun terus berkembang. Oleh karena itu, DPR sebagai lembaga pembuat undang-undang perlu untuk membahas dan membuat kebijakan khusus yang mengatur permasalahan teknologi AI *deepfake.* Aparat penegak hukum juga perlu dibekali dengan pengetahuan dan teknologi khusus yang digunakan untuk mendeteksi kasus-kasus AI *deepfake*, sehingga setiap pelaku yang melakukan tindak pidana penyalahgunaan teknologi AI *deepfake* diproses sesuai ketentuan hukum yang berlaku.

DAFTAR REFERENSI

Abdul, R. (2019). Artificial intelligence untuk pemula. UNIPMA Press.

Afni, N. (2022). Implikasi hukum penggunaan artificial intelligence dalam tindak pidana cyber crime. Artikel Jurnal Skripsi Repository, Fakultas Hukum Universitas Pancasakti Tegal.

Ahmad, S. (2020). Teknologi dan media pembelajaran. CV Jejak.

Alya, A. (2024). Legal regulations on criminal acts against misuse of AI technology in voice phishing fraud via mobile phones. Jurnal Hukum De Rechtsstaat, 10(2).

Amalia, A. H. (2022). Perlindungan hukum penyalahgunaan artificial intelligence deepfake pada layanan pinjaman online. Artikel Ilmiah, Fakultas Hukum Universitas Muhammadiyah Surakarta.

Amir, I. (2012). Asas-asas hukum pidana: Memahami tindak pidana dan pertanggungjawaban pidana sebagai syarat pemidanaan. Mahakarya Rangkang Offset.

Anti, M., Suhandi, A. M., & Herlambang, Y. T. (2024). Problematika teknologi deepfake sebagai masa depan hoax yang semakin meningkat: Solusi strategis ditinjau dari literasi digital. Jurnal Pendidikan Teknologi Informasi, 1(2).

Antika, R. (2020). Deepfake pornografi: Ketika kekerasan seksual bertransformasi tanpa kendali. Jurnal.

Ariman, H. M. R., & Raghib, F. (2016). Hukum pidana. Setara Press.

Asman. (2019). Tindak pidana penipuan berbasis transaksi elektronik. Guepedia.

Chandra, T. Y. (2022). Hukum pidana. PT. Sangir Multi Usaha.

Chazawi, A. (2002). Pelajaran hukum pidana bagian 1. RajaGrafindo Persada.

Eriana, E. S., & Zein, A. (2023). Artificial intelligence (AI). CV Eureka Media Aksara.

Faqih, F. 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).

Fatmawati, et al. (2023). Analisis yuridis terhadap artificial intelligence pada tindak pidana penyebaran malware di Indonesia. Journal of Social Research, 3(2).

Frisky, A. Y., Kaimuddin, A., & Ashsyarofi, H. L. (2024). Pertanggungjawaban pidana pelaku terhadap korban penyalahgunaan artificial intelligence deepfake menurut hukum positif Indonesia. Jurnal Dinamika Ilmiah Ilmu Hukum, 30(1).

Heny, N., & Astuti, P. (2021). Jerat hukum penyalahgunaan aplikasi deepfake ditinjau dari hukum pidana. Artikel Jurnal Hukum Vonum, Fakultas Ilmu Sosial dan Hukum Universitas Negeri Surabaya, 9(4).

Hidayat, M. D. Y., Taufik, H. W., & Ilyas, S. (2022). Tinjauan hukum terhadap cyber pornografi di Indonesia. Jurnal Pendidikan Dan Konseling, Fakultas Hukum Universitas Lancang Kuning Riau, 4(6).

Ibrahim, J. (2007). Teori & metodologi penelitian hukum normatif. Bayumedia Publishing.

Intan, L., et al. (2023). Etika dalam era deepfake: Bagaimana menjaga integritas komunikasi. Jurnal Visi Komunikasi, 22(2).

Kade Budhi, I. G. (2022). Artificial intelligence: Konsep, potensi, masalah, hingga pertanggungjawaban pidana. PT Raja Grafindo Persada.

Komnas Perempuan. (2023). Lembar Fakta Catatan Tahunan: Kekerasan terhadap perempuan di ranah publik dan negara minimnya perlindungan dan pemulihan. Komnas Perempuan.

Lamintang, P. A. F. (1984). Dasar-dasar hukum pidana Indonesia. Sinar Baru.

Marzuki, P. M. (2005). Penelitian hukum. Kencana.

Nugraha, U. A., Kesuma, P. T., & Hidayat, R. M. (2023). Analisis hukum terhadap upaya pencegahan kasus deepfake porn dan pendidikan kesadaran publik di lingkungan digital. Artikel Jurnal Pendidikan Tambusai, 7(3).

Nurhidayah, I. W., et al. (2022). Botnet detection using independent component analysis. Artikel Jurnal Ilmu Engineering, Universitas Teknologi Malaysia, 23(1).

Pasaribu, M., & Widjaja, A. (2022). Artificial intelligence: Perspektif manajemen strategis. PT Gramedia.

Renuat, F., et al. (2023). Pengantar hukum pidana. CV. Gita Lentera.

Rifki, S. M. (2019). Perlindungan hukum terhadap korban penyalahgunaan data pribadi: Penggunaan teknik deepfake. Artikel Prosiding Seminar Nasional Hasil Penelitian & Pengabdian Kepada Masyarakat, Fakultas Hukum Universitas Islam Nusantara Bandung, 4(1).

Rohman, M. M., et al. (2023). Asas-asas hukum pidana. PT Global Eksekutif Teknologi.

Rustam, et al. (2015). Pembelajaran berbasis teknologi informasi dan komunikasi: Mengembangkan profesionalitas guru. Rajawali Pers.

Setia, D. A., & Setiawan, D. A. (2024). Penegakan hukum terhadap pelaku tindak pidana video deepfake porn dihubungkan hukum pidana positif di Indonesia. Jurnal Bandung Conference: Law Studies, 4(1).

Soekanto, S. (2006). Pengantar penelitian hukum. Universitas Indonesia (UI-Pers).

Soekanto, S. (2022). Faktor-faktor yang mempengaruhi penegakan hukum. PT RajaGrafindo Persada.

Soekanto, S. (2022). Penelitian hukum normatif: Suatu tinjauan singkat. PT RajaGrafindo Persada.

Sulaiman, R., et al. (2021). Hukum di era artificial intelligence. RSP Forensic Legal Auditor Specialist.

Suseno, S. (2012). Yurisdiksi tindak pidana siber. PT Refika Aditama.

Suyanto. (2018). Pengantar hukum pidana. Deepublish.

Syahrani, L. N. (2024). Kebijakan formulasi hukum pidana atas praktik deepfake dilihat dari perspektif kejahatan siber dan pornografi. Artikel Jurnal Skripsi, Fakultas Hukum Universitas Sriwijaya.

Taufik, I. (2021). Pengantar teknologi informasi: Konsep, teori, dan praktik. Yayasan Prima Agus Teknik.

Undang-Undang Republik Indonesia Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana.

Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Utawi, E. I., & Rohaeni, N. (2023). Penegakan hukum terhadap tindak pidana pornografi menurut peraturan perundang-undangan tentang pornografi melalui media sosial. Jurnal Bandung Conference Series: Law Studies, 3(1).

Wenggedes, F. (2022). Kelemahan pelaksanaan kebijakan kriminal terhadap cyberbullying anak di Indonesia. Jurnal Indonesia Criminal Law Review, 1(2).

Widnyana, I. M. (2010). Asas-asas hukum pidana. PT. Fikahati Aneska.