Received: 30-3-2024
Revised: 1-4-2024
Accepted: 11-5-2024
e-ISSN: 2621-4105

Kriminalisasi *Deepfake* Di Indonesia Sebagai Bentuk Pelindungan Negara

Criminalization of Deepfake in Indonesia as a Form of State Protection

Chiquita Thefirstly Noerman, Aji Lukman Ibrahim
Fakultas Hukum, Universitas Pembangunan Nasional "Veteran" Jakarta, Jakarta, Indonesia
2110611111@mahasiswa.upnvj.ac.id

Abstract

This study aims to find out the regulations regarding deepfake crimes in Indonesia and to find out the ideal regulations regarding deepfake crimes in the future. Technology that is growing rapidly in fact can provide convenience in doing anything. But technological developments can cause serious problems, one of which is the misuse of deepfakes which are part of artificial intelligence. Deepfakes certainly harm many people, ranging from victims whose identities are used by fraudsters, to victims who get material losses. With no regulation governing deepfakes, the form of state protection for victims of this crime is still in doubt. This research uses normative legal research methods that use 3 (three) approaches, namely the statutory approach, the comparative approach, and the conceptual approach. This research uses data collection techniques through library research. The author uses descriptive data analysis techniques by presenting data and information as an overview of the subject and object of research that is arranged systematically so that it can be understood. The author also uses the prescriptive analysis method by providing arguments for the research results described. The results of this study explain that Indonesia has not explicitly regulated deepfake crimes. Indonesia only regulates general falsification of personal data in the PDP Law and also electronic falsification in the ITE Law which is a derivative of the 1945 NRI Constitution.
Keywords: *Artificial Intelligence; Data Falsification; Deepfake*

Abstrak

Penelitian ini bertujuan untuk mengetahui peraturan mengenai tindak pidana *deepfake* di Indonesia dan untuk mengetahui idealnya pengaturan mengenai tindak pidana *deepfake* di masa mendatang. Teknologi yang semakin berkembang pesat pada hakikatnya dapat memberikan kemudahan dalam melakukan apapun. Namun perkembangan teknologi dapat menimbulkan permasalahan serius, salah satunya adalah penyalahgunaan *deepfake* yang merupakan bagian dari *artificial intelligence*. *Deepfake* tentunya merugikan banyak orang, mulai dari korban yang identitasnya digunakan oleh penipu, sampai dengan korban yang mendapat kerugian materil. Belum adanya regulasi yang mengatur mengenai *deepfake* mengakibatkan perlindungan negara terhadap korban tindak pidana ini masih diragukan. Penelitian ini menggunakan metode penelitian hukum normatif yang menggunakan 3 (tiga) pendekatan, yakni pendekatan perundang-undangan, pendekatan perbandingan, dan pendekatan konseptual. Penelitian ini menggunakan teknik pengumpulan data melalui penelitian kepustakaan (*library research*). Penelitian ini menggunakan teknik analisis data deskriptif dengan menyajikan data serta informasi sebagai gambaran atas subjek dan objek penelitian yang disusun secara sistematis sehingga dapat dipahami. Penelitian ini juga menggunakan metode analisis preskriptif dengan memberikan argumentasi atas hasil penelitian yang dijabarkan. Hasil dari penelitian ini menjelaskan bahwa di Indonesia belum mengatur secara eksplisit mengenai tindak pidana *deepfake*. Indonesia hanya mengatur mengenai pemalsuan data pribadi secara umum dalam UU PDP dan juga pemalsuan secara elektronik dalam UU ITE yang merupakan turunan dari UUD NRI 1945.
Kata kunci: *Artificial Intelligence*; *Deepfake*; Pemalsuan Data

Received: 30-3-2024
Revised: 1-4-2024
Accepted: 11-5-2024
e-ISSN: 2621-4105

1. PENDAHULUAN

Teknologi seperti *artificial intelligence* yang semakin berkembang pesat pada hakikatnya dapat memberikan kemudahan dalam melakukan apapun. *Artificial intelligence* merupakan suatu teknologi yang berupa sistem komputer yang memiliki kecerdasan layaknya seorang manusia dalam hal melakukan sesuatu.[1] *Artificial intelligence* merupakan sebuah cabang dari teknologi dalam komputer yang berfokus dalam membangun kecerdasan buatan yang berfikir dan bekerja seperti manusia.[2] *Artificial intelligence* dibagi menjadi dua, yakni *autonomous system* dan *autonomous machine*.[3] *Autonomous machine* merupakan suatu bentuk *artificial intelligence* yang dapat bertindak tanpa bantuan manusia. Sedangkan *autonomous system* merupakan bentuk *artificial intelligence* yang diperintah oleh manusia, seperti halnya teknologi *deepfake*. *Deepfake* merupakan sebuah teknologi yang menggunakan *artificial intelligence* untuk memproduksi atau mengedit suara, foto, maupun video yang sebenarnya tidak pernah terjadi.[4]

Deepfake secara etimologi berasal dari bahasa inggris yaitu "*deep learning*" dan kata "*fake*".[5] *Deep learning* merupakan sebuah teknologi yang melahirkan *software* untuk suatu *deepfake*. Sedangkan "*fake*" merujuk pada hasil dari teknologi *deepfake* yang berupa media palsu yang mana bukanlah suatu hal yang original. *Deepfake* dapat memanipulasi fitur wajah seseorang menggunakan teknologi *artificial intelligence*.[6] *Deepfake* dapat berupa video seseorang melakukan sesuatu yang sebenarnya tidak pernah dilakukan dengan cara menggunakan wajah orang tersebut dalam sebuah video yang dilakukan orang lain.[7] Perkembangan teknologi dapat menimbulkan sebuah dampak negatif, yakni munculnya tindak pidana baru.[8] Seperti menjamurnya teknologi *deepfake* yang dapat menimbulkan ancaman epistemik yakni menggiring masyarakat untuk mempercayai hal yang sebenarnya tidak terjadi.[9] Pesatnya perkembangan teknologi *deepfake* menimbulkan ancaman serius dikarenakan dapat digunakan untuk menyebarkan informasi palsu secara global serta berpotensi memengaruhi opini publik.[10] Seperti halnya ketika terdapat video yang mengandung *deepfake* yang menayangkan Presiden Joko Widodo yang fasih berbahasa

---

[1] Ramadhan, Dwi Galih, "'Perlindungan Hukum Atas Invensi Artificial Intelligence Di Era Revolusi Industri 4.0 & Society 5.0'" (Universitas Islam Indonesia, 2022).

[2] Nobert Young, *DeepFake Technology: Complete Guide to Deepfakes, Politics and Social Media* (United States, 2019).

[3] Keith Frankish and William M. Ramsey, eds., *The Cambridge Handbook of Artificial Intelligence* (Cambridge, United Kingdom: Cambridge University Press, 2014).

[4] Young, *DeepFake Technology*.

[5] John Brandon, "Terrifying High-Tech Porn: Creepy 'deepfake' Videos Are on the Rise," *Fox News*, February 20, 2018, https://www.foxnews.com/tech/terrifying-high-tech-porn-creepy-deepfake-videos-are-on-the-rise.

[6] Felix Juefei-Xu et al., "Countering Malicious DeepFakes: Survey, Battleground, and Horizon," *International Journal of Computer Vision* 130, no. 7 (July 2022): 1678–1734, https://doi.org/10.1007/s11263-022-01606-8.

[7] John D. Kelleher, *Deep Learning*, The MIT Press Essential Knowledge Series (Cambridge, Massachusetts: The MIT Press, 2019).

[8] Faiz Emery Muhammad and Beniharmoni Harefa, "Pengaturan Tindak Pidana Bagi Pelaku Penipuan Phisning Berbasis Web," *Jurnal USM Law Review* 6, no. 1 (2023), http://dx.doi.org/10.26623/julr.v6i1.6649.

[9] Don Fallis, "The Epistemic Threat of Deepfakes," *Philosophy & Technology* 34, no. 4 (December 2021): 623–43, https://doi.org/10.1007/s13347-020-00419-2.

[10] John Wojewidka, "The Deepfake Threat to Face Biometrics," *Biometric Technology Today* 2020, no. 2 (February 2020): 5–7, https://doi.org/10.1016/S0969-4765(20)30023-0.

Received: 30-3-2024
Revised: 1-4-2024
Accepted: 11-5-2024
e-ISSN: 2621-4105

Mandarin.[11] Hal tersebut dapat menggiring opini masyarakat terhadap Presiden Joko Widodo yang berkaitan dengan Pemilu 2024.[12]

Deepfake juga memiliki potensi dapat memodifikasi ingatan, membuat ingatan palsu, atau bahkan merubah sifat seseorang.[13] *Deepfake* dapat merugikan banyak orang serta menimbulkan suatu tindak pidana seperti penipuan, pornografi, dan lain sebagainya dengan cara menggunakan identitas seseorang dengan seolah-olah orang tersebut yang melakukan tindak pidana. Meskipun tindak pidana seperti tindak pidana penipuan telah diatur dalam KUHP, namun dampak dari tindak pidana penipuan menggunakan *deepfake* lebih besar dibanding tindak pidana penipuan biasa. Hal ini dikarenakan *deepfake* tidak hanya menggunakan penipuan secara verbal, namun juga secara visual. Secara umum manusia lebih mengandalkan informasi secara visual dibandingkan informasi sensorik lainnya yang disebut sebagai efek dominasi visual colavita.[14] Dengan belum adanya regulasi yang mengatur mengenai *deepfake*, maka bentuk perlindungan negara terhadap korban tindak pidana ini masih diragukan. Indonesia sebagai negara hukum sudah seharusnya memiliki regulasi yang mengatur mengenai *artificiall intelligence* serta tindak pidana yang hadir karena adanya teknologi *artificial intelligence,* khususnya tindak pidana *deepfake.* Dengan adanya kekosongan hukum tersebut, para penegak hukum dapat mengalami kesulitan untuk memberantas mengenai tindak pidana yang hadir karena *artificial intelligence*. Hal ini dikarenakan Indonesia yang menganut asas legalitas, yakni tidak seorangpun dapat dipidana tanpa ada aturan yang mengaturnya.

Terdapat beberapa penelitian *artificial intelligence* maupun *deepfake* yang serupa dengan tema penelitian ini, berikut beberapa hasil penelitian tersebut**.** Pertama, penelitian yang ditulis oleh Solichah, dkk.[15] Penelitian tersebut menjelaskan bahwa sampai saat ini belum ada aturan yang mengatur mengenai tindak pidana pornografi yang menggunakan *deepfake* yang mana menimbulkan kekosongan hukum. Namun penelitian tersebut belum membahas bahwa penggunaan *deepfake* merupakan penyalahgunaan data pribadi dikarenakan *deepfake* adalah sebuah data biometrik yang termasuk ke dalam jenis data pribadi. Berbeda dengan penelitian tersebut, penelitian ini akan membahas mengenai penyalahgunaan data pribadi menggunakan *deepfake* serta aturan pidana atas tindak pidana *deepfake* di Indonesia.

---

[11] Gede Arga Adrian, "Deepfake: Bakal Dalang Hoax Jelang Pemilu 2024?," Deepfake: Bakal Dalang Hoax Jelang Pemilu 2024?, accessed May 6, 2024, https://www.ums.ac.id/berita/unggulan/deep-fake-bakal-dalang-hoax-jelang-pemilu-2024.

[12] Gede Arga Adrian.

[13] Cristian Vaccari and Andrew Chadwick, "Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News," *Social Media + Society* 6, no. 1 (January 2020): 205630512090340, https://doi.org/10.1177/2056305120903408.

[14] Camille Koppen and Charles Spence, "Seeing the Light: Exploring the Colavita Visual Dominance Effect," *Experimental Brain Research* 180, no. 4 (June 22, 2007): 737–54, https://doi.org/10.1007/s00221-007-0894-3.

[15] Isnaini Imroatus Solichah, Faizin Sulistio, and Milda Istiqomah, "Protection of Victims of Deep Fake Pornography in a Legal Perspective in Indonesia," *International Journal of Multicultural and Multireligious Understanding* 10, no. 1 (2023), https://ijmmu.com/index.php/ijmmu/article/view/4409/3755. http://dx.doi.org/10.18415/ijmmu.v10i1.4409

Received: 30-3-2024
Revised: 1-4-2024
Accepted: 11-5-2024
e-ISSN: 2621-4105

Kedua, penelitian oleh Kurniawan.[16] Penelitian tersebut menjelaskan bahwa kecerdasan buatan bukanlah subjek hukum, oleh karena perbuatan yang dilakukan oleh kecerdasan buatan hanyalah merupakan perintah dari penggunanya. Padahal *Artificial intelligence* dibagi menjadi dua, yakni *autonomous system* dan *autonomous machine*.[17] *Autonomous machine* merupakan suatu bentuk *artificial intelligence* yang dapat bertindak tanpa bantuan manusia. Sedangkan *autonomous system* merupakan bentuk *artificial intelligence* yang diperintah oleh manusia, seperti halnya teknologi *deepfake*. Selain itu penelitian tersebut hanya membahas *artificial intelligence* sebagai sebuah subjek hukum, tidak merumuskan mengenai pencegahan ataupun penanganan atas *artificial intelligence* yang melakukan tindak pidana. Sedangkan penelitian ini membahas mengenai pencegahan dan penanganan akan penyalahgunaan *deepfake* yang merupakan salah satu bentuk *artificial intelligence* di Indonesia.

Ketiga adalah penelitian Kugler,[18] penelitian tersebut menjelaskan mengenai sikap publik mengenai teknologi *artificial intelligence* khususnya deepfake serta regulasi mengenai tindak pidana *deepfake* di Amerika Serikat. Namun penelitian tersebut hanya menjelaskan kasus *deepfake* berupa pornografi dan penyalahgunaan identitas terkait dengan kepentingan pemilihan umum. Berbeda dengan penelitian tersebut, penelitian ini akan membahas mengenai akan menjelaskan *deepfake* secara umum serta menjelaskan bahwa kasus *deepfake* dapat berupa penipuan yang akan menyebabkan kerugian materil. Penelitian ini bertujuan untuk mengetahui peraturan mengenai tindak pidana *deepfake* di Indonesia dan untuk mengetahui idealnya pengaturan mengenai tindak pidana *deepfake* di masa mendatang.

2. METODE

Penelitian ini menggunakan metode penelitian hukum normatif yang menggunakan 3 (tiga) pendekatan, yakni pendekatan perundang-undangan (*statute approach*), pendekatan perbandingan (*comparative approach*), dan pendekatan konseptual (*conceptual approach*). Penelitian ini menggunakan pendekatan perundang-undangan (*statute approach*) dengan mengkaji penelitian ini dengan menggunakan peraturan perundang-undangan yang berkaitan dengan permasalahan. Penelitian ini juga menggunakan pendekatan perbandingan (*comparative approach*) yang berupa perbandingan peraturan perundang-undangan di negara China, California, serta peraturan di Uni Eropa. Penelitian ini menggunakan prinsip-prinsip hukum serta doktrin hukum untuk menjawab permasalahan terkait tindak pidana *deepfake* di Indonesia dalam bentuk pendekatan konseptual (*conceptual approach*). Penelitian ini menggunakan sumber data sekunder yang memperoleh data secara tidak langsung dari sumber (objek penelitian) melainkan melalui pihak ketiga. Sumber bahan hukum primer pada penelitian ini terdiri dari beberapa peraturan perundang-undangan yang

[16] Itok Kurniawan, "Analisis Terhadap Artificial Intelligence Sebagai Subjek Hukum Pidana," *Mutiara : Jurnal Ilmiah Multidisiplin Indonesia* 1, no. 1 (July 18, 2023): 35–44, https://doi.org/10.61404/jimi.v1i1.4.

[17] Frankish and Ramsey, *The Cambridge Handbook of Artificial Intelligence*.

[18] Matthew B. Kugler and Carly Pace, "Deepfake Privacy: Attitudes and Regulation," *SSRN Electronic Journal*, 2021, https://doi.org/10.2139/ssrn.3781968.

Received: 30-3-2024
Revised: 1-4-2024
Accepted: 11-5-2024
e-ISSN: 2621-4105

terkait dengan tema penelitian. Sedangkan bahan hukum sekunder pada penelitian ini berupa buku-buku, jurnal hukum, dan hasil dari penelitian-penelitian hukum sebelumnya yang relevan sebagai referensi teori peraturan perundang-undangan dalam pembahasan permasalahan penelitian ini. Bahan hukum terakhir yang digunakan dalam penelitian ini adalah bahan hukum tersier yang berupa kamus dan ensiklopedia. Penelitian ini menggunakan teknik pengumpulan data melalui penelitian kepustakaan (*library research*) dengan menggunakan teknik analisis data deskriptif. Penelitian ini juga menggunakan metode analisis preskriptif dengan memberikan argumentasi atas hasil penelitian yang dijabarkan.

3. HASIL DAN PEMBAHASAN

3.1 Pengaturan Mengenai Tindak Pidana *Deepfake* Di Indonesia

Manipulasi atas media (foto, video, dan suara) merupakan sebuah ancaman dikarenakan meliputi atas identitas seseorang. Dengan adanya perkembangan teknologi, media dapat dimanipulasi dengan mudah, yakni dengan hadirnya *deepfake* sebagai bagian dari *artificial intelligence* yang merupakan sebuah alat yang dapat memanipulasikan hal yang berkaitan dengan media seperti foto, video, dan suara.[19] *Deepfake* menghasilkan data palsu yang identik dengan data asli yang mengakibatkan data palsu tersebut terlihat asli.[20] *Deepfake* menggunakan sebuah algoritma *artificial intelligence* yang kemudian memilih data biometrik seperti sebuah video seseorang berbicara yang kemudian merekonstruksi wajah di video tersebut ke dalam wajah orang lain dengan mencocokan pergerakan wajah dan suara orang tersebut.[21] Dengan kata lain, *deepfake* merupakan sebuah media yang sangat realistis dalam bentuk sebuah gambar, video, maupun suara yang dibuat oleh *artificial intelligence.*[22] *Deepfake* pada saat ini dapat diakses oleh semua orang, tanpa batasan apapun. *Deepfake* tidak membutuhkan *skill* professional untuk terlihat nyata, bahkan orang awam sekalipun dapat menggunakan teknologi *deepfake.*[23] Hal ini dikarenakan dengan hadirnya *tools* dan *software* gratis yang dapat diakses oleh banyak orang melalui internet. Pada saat ini, hadirnya dua *platform* terkemuka yang dapat menciptakan suatu *deepfake* adalah *deepfacelab* dan *face swap.*[24] Kedua *platform* ini dijalankan oleh seorang programmer anonim yang menyediakan *deepfake* bagi setiap orang yang ingin membuat media tiruan. Teknologi seperti *deepfake* dapat berkembang lebih cepat yang nantinya akan lebih mudah untuk diakses setiap orang.[25]

Di tangan orang yang salah, teknologi *deepfake* dapat menimbulkan ancaman serius. Pertama, *deepfake* dapat menimbulkan ancaman epistemik yang dapat menggiring opini

[19] Nina Schick, *Deepfakes: The Coming Infocalypse* (New York New York: Twelve, 2020).
[20] Tianxiang Shen et al., "'Deep Fakes' Using Generative Adversarial Networks (GAN)," 2018.
[21] Samantha Cole, "This Deepfake of Mark Zuckerberg Tests Facebook's Fake Video Policies," *Motherboard Tech by Vice*, June 12, 2019, https://www.vice.com/en/article/ywyxex/deepfake-of-mark-zuckerberg-facebook-fake-video-policy.
[22] James Vincent, "Why We Need a Better Definition of 'Deepfake' - The Verge," May 23, 2018, https://www.theverge.com/2018/5/22/17380306/deepfake-definition-ai-manipulation-fake-news.
[23] Young, *DeepFake Technology*.
[24] Schick, *Deepfakes*.
[25] Schick.

Received: 30-3-2024
Revised: 1-4-2024
Accepted: 11-5-2024
e-ISSN: 2621-4105

masyarakat terhadap suatu hal yang tidak benar adanya.[26] Salah satunya adalah beredarnya video *deepfake* Presiden Joko Widodo berpidato menggunakan bahasa Mandari yang dapat menggiring opini publik menjelang Pemilu 2024.[27] Kedua, *deepfake* juga dapat menimbulkan rasa ketidakpercayaan masyarakat akan hal yang benar-benar terjadi.[28] Seperti halnya dalam konflik Palestina dan Israel, banyaknya masyarakat yang tidak mempercayai korban anak-anak Palestina dan mempercayai bahwa hal tersbut adalah editan yang dilakukan menggunakan *deepfake*.[29] Ketiga, *deepfake* juga dapat memengaruhi psikologis manusia. *Deepfake* dapat menyebabkan stres dan rasa cemas berlebih terhadap korban yang identitasnya digunakan oleh pelaku.[30] Selain itu, *deepfake* juga dapat menyebabkan adanya ingatan yang terdistorsi antara *deepfake* dan ingatan asli pada otak manusia.[31] Hal tersebut dikarenakan masyarakat yang tidak mengetahui bahwa suatu media merupakan sebuah *deepfake* akan menganggap bahwa hal tersebut merupakan hal asli yang dilakukan oleh korban penyalahgunaan identitas.[32] Keempat, di Indonesia sendiri telah banyak korban dari hasil tindak pidana *deepfake*. Namun sangat disayangkan tidak adanya data statistik yang menjelaskan jumlah korban dari tindak pidana *deepfake* dikarenakan penyalahgunaan *deepfake* belum dianggap sebagai tindak pidana. Hal tersebut dapat dilihat pada kasus panggilan video Baim Wong yang hanya menyatakan penyebaran berita bohong secara elektronik, bukanlah penyalahgunaan identitas seseorang.

Belakangan ini terdapat sebuah kasus yaitu penipuan yang berupa panggilan video yang menampilkan Baim Wong dalam rangka program *giveaway*. Dilansir dari laman Tempo.co, pada tahun 2021 seorang Asisten Rumah Tangga menyatakan bahwa ia mendapat panggilan video dari Baim Wong yang menyatakan bahwa dirinya mendapatkan *giveaway* senilai 100 Juta Rupiah.[33] Penipuan dengan modus panggilan video yang mengatasnamakan Baim Wong nyatanya terus berlanjut meskipun telah banyak korban berjatuhan. Korban selanjutnya adalah Evi, seorang wanita berusia 49 tahun, yang mengalami kerugian yang ditaksir mencapai 149 Juta rupiah.[34] Evi pada tanggal 2 Desember 2022 mendaftarkan diri melalui *link* di media sosial Facebook yang kemudian

[26] Fallis, "The Epistemic Threat of Deepfakes."
[27] Gede Arga Adrian, "Deepfake: Bakal Dalang Hoax Jelang Pemilu 2024?"
[28] Jeffrey T. Hancock and Jeremy N. Bailenson, "The Social Impact of Deepfakes," *Cyberpsychology, Behavior, and Social Networking* 24, no. 3 (March 1, 2021): 149–52, https://doi.org/10.1089/cyber.2021.29208.jth.
[29] David Klepper, "Deepfakes from Gaza War Increase Fears about AI's Power to Mislead | AP News," Fake babies, real horror: Deepfakes from the Gaza war increase fears about AI's power to mislead, accessed May 6, 2024, https://apnews.com/article/artificial-intelligence-hamas-israel-misinformation-ai-gaza-a1bb303b637ffbbb9cbc3aa1e000db47.
[30] Patrick Yung Kang Lee et al., "Speculating on Risks of AI Clones to Selfhood and Relationships: Doppelganger-Phobia, Identity Fragmentation, and Living Memories," *Proceedings of the ACM on Human-Computer Interaction* 7, no. CSCW1 (April 14, 2023): 1–28, https://doi.org/10.1145/3579524.
[31] Lee et al.
[32] Lee et al.
[33] Marvela, "Konten Disalahgunakan Untuk Penipuan, Baim Wong Tak Tinggal Diam," *Tempo*, July 7, 2021, sec. seleb, https://seleb.tempo.co/read/1480763/konten-disalahgunakan-untuk-penipuan-baim-wong-tak-tinggal-diam.
[34] Dewantoto and David Oliver Purpa, "Lagi, Penipuan 'Giveaway' Catut Nama Baim Wong, Bagaimana Pelaku Meyakinkan Korbannya? Halaman All - Kompas.Com," *Kompas.Com*, April 11, 2023, https://medan.kompas.com/read/2023/04/11/105816078/lagi-penipuan-giveaway-catut-nama-baim-wong-bagaimana-pelaku-meyakinkan?page=all#google_vignette.

Received: 30-3-2024
Revised: 1-4-2024
Accepted: 11-5-2024
e-ISSN: 2621-4105

mendapatkan sebuah panggilan video dan panggilan suara dari seseorang yang mana wajah serta suara dari pelaku serupa dengan Baim Wong. Pelaku menyalahgunakan video dan suara dari Baim Wong yang berasal dari kumpulan suara pada program *giveaway* Baim Wong *"Indonesia Giveaway"* pada tahun 2021.[35]

Baim Wong yang digunakan identitasnya juga merupakan korban dari kasus penipuan *giveaway* tersebut. Hal ini dikarenakan kasus penipuan ini menggunakan teknologi *deepfake* yang menggunakan wajah dan juga suara dari Baim Wong sebagai upaya mengelabui korban. Dilansir dari website SIPP Pengadilan Negeri Medan dengan nomor perkara 1295/Pid.Sus/2023/PN Mdn, pelaku atas kasus penipuan yang menimpa Evi telah terbukti secara sah dan bersalah melakukan tindak pidana "Dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik", sebagaimana dalam Pasal 28 ayat (1) *Jo* Pasal 45A ayat (1) Undang-Undang Informasi dan Transaksi Elektronik.[36] Pada hakikatnya terdapat beberapa aturan di Indonesia terkait dengan tindak pidana *deepfake* yang dapat diterapkan, di antaranya dapat dilihat dalam tabel berikut:

Tabel 1. Peraturan Perundang-undangan Terkait *Deepfake* Di Indonesia

No.	Peraturan Perundang-undangan	Pasal
1.	Undang-Undang Dasar Negara Republik Indonesia Tahun 1945	Pasal 28G ayat (1)
2.	Undang-Undang 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.	Undang-Undang 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.	Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi	Pasal 65 ayat (3) Pasal 66 Pasal 67 ayat (3) Pasal 68

sumber: database peraturan JDIH BPK

[35] Dian Nita, "Baim Wong Sebut Pelaku Penipuan Giveaway Pintar Mainkan Suara Dari Potongan Videonya," *Kompas TV*, April 11, 2023, https://www.kompas.tv/entertainment/396955/baim-wong-sebut-pelaku-penipuan-giveaway-pintar-mainkan-suara-dari-potongan-videonya?page=all.

[36] "SIPP Pengadilan," accessed March 28, 2024, https://sipp.pn-medankota.go.id/index.php/list_perkara.

Received: 30-3-2024
Revised: 1-4-2024
Accepted: 11-5-2024
e-ISSN: 2621-4105

Mencermati Tabel 1 peraturan perundang-undangan terkait *deepfake* Di Indonesia, beberapa aturan di Indonesia terkait dengan tindak pidana *deepfake* di atas, maka dapat dilihat bahwasanya aturan-aturan tersebut belum mengatur secara eksplisit mengenai tindak pidana *deepfake.* Aturan tertinggi terdapat dalam pembukaan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, yakni melindungi segenap bangsa Indonesia dan seluruh tumpah darah Indonesia. Hal ini diatur lebih lanjut dalam Pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 (UUD NRI 1945) yang menyatakan bahwa hak privasi merupakan hak asasi, yang mana menyatakan bahwa perlindungan data merupakan perlindungan hak asasi manusia yang fundamental. [37] Perlindungan privasi merupakan faktor penting dalam melindungi data pribadi.[38] Aturan dalam UUD NRI 1945 tersebut menjadi turunan aturan-aturan mengenai privasi dan data pribadi lainnya di Indonesia.

Aturan terkait dengan privasi juga terdapat dalam aturan internasional yaitu di dalam *International Covenant On Civil And Political Rights*. Indonesia telah meratifikasi ICCPR dalam Undang-Undang Republik Indonesia Nomor 12 Tahun 2005 tentang Pengesahan *International Covenant On Civil And Political Rights* (Kovenan Internasional Tentang Hak-Hak Sipil Dan Politik). Dengan lahirnya *artificial intelligence* yang melahirkan teknologi lainnya seperti *deepfake,* dapat menimbulkan dampak negatif berupa pelanggaran hak atas privasi yang terdapat dalam Pasal 17 *International Covenant on Civil and Political Rights* (ICCPR).[39] Ketentuan tersebut menyatakan bahwa tidak seorang pun boleh secara sewenang-wenang mengganggu privasi, keluarga, rumah, ataupun menyerang kehormatan dan reputasinya, setiap orang berhak atas perlindungan hukum terhadap gangguan atau serangan semacam itu". Hak tersebut menjamin bahwa setiap orang berhak untuk mendapatkan privasinya, termasuk privasi atas data pribadi.

Salah satu turunan dari Pasal 28G ayat (1) UUD NRI 1945 adalah Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Dan Transaksi Elektronik. UU ITE pada hakikatnya lebih banyak membahas mengenai transaksi elektronik dalam ranah bisnis.[40] *Deepfake* merupakan media palsu yang mana dapat menggunakan identitas orang lain yang dapat merusak nama baik serta harga diri orang lain dapat merujuk ke dalam Pasal 27A yang mengatur mengenai perbuatan yang merendahkan atau merusak nama baik ataupun harga diri orang lain yang dapat merugikan orang tersebut, termasuk juga dengan menista dan/ atau memfitnah. Selanjutnya adalah Pasal 28 ayat (1) yang mengatur mengenai

[37] Husni Kurniawati And Yunanto, "Perlindungan Hukum Terhadap Penyalahgunaan Data Pribadi Debitur Dalam Aktivitas Pinjaman Online" 7, No. 1 (2022). http://dx.doi.org/10.26623/jic.v7i1.4290

[38] Rista Maharani And Andria Luhur Prakoso, "Perlindungan Data Pribadi Konsumen Oleh Penyelenggara Sistem Elektronik Dalam Transaksi Digital," *Jurnal USM Law Review* 7, No. 1 (N.D.). http://dx.doi.org/10.26623/julr.v7i1.8705

[39] Jeremiah Maximillian Laza and Rizky Karo Karo, "Perlindungan Hukum Terhadap Artificial Intellegence Dalam Aspek Penyalahgunaan Deepfake Technology Pada Perspektif UU PDP dan GDPR.," *Lex Prospicit* 1, No. 2 (2023). http://dx.doi.org/10.19166/lp.v1i2.7386

[40] Wahyu Beny Mukti Setiyawa, Erifendi Churniawan, And Femmy Silaswaty Faried, "Upaya Regulasi Teknologi Informasi Dalam Menghadapi Serangan Siber Guna Menjaga Kedaulatan Negara Kesatuan Republik Indonesia" 3, No. 2 (2020). http://dx.doi.org/10.26623/julr.v6i1.6649

Received: 30-3-2024
Revised: 1-4-2024
Accepted: 11-5-2024
e-ISSN: 2621-4105

informasi berita bohong atau yang biasa dikenal dengan "hoax".[41] Aturan ini digunakan dalam kasus di atas dengan nomor perkara 1295/Pid.Sus/2023/PN Mdn untuk menjerat pelaku *deepfake* dalam kasus tersebut.

Aturan turunan Pasal 28G ayat (1) UUD NRI 1945 lainnya yang mengatur mengenai *deepfake* adalah Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi yang berlaku sejak tanggal 27 Oktober 2022. Tepatnya pada Pasal 65 ayat (3), Pasal 66, Pasal 67 ayat (3), dan Pasal 68. Hal tersebut dikarenakan *deepfake* berkaitan dengan digunakannya data biometrik korban sebagai media untuk melakukan tindak pidana. Merujuk pada penjelasan Undang-Undang Perlindungan Data Pribadi Pasal 4 huruf b, Data biometrik merupakan data yang berkaitan dengan fisik, fisiologis, atau karakteristik pelaku individu yang termasuk maupun tidak terbatas pada wajah, suara, sidik jari, retina mata, dan lain sebagainya. Hal ini menggambarkan bahwa kasus penipuan yang menggunakan *deepfake* di atas tidak hanya meliputi penipuan secara elektronik serta pencemaran nama baik saja, namun juga berkaitan dengan digunakannya data biometrik korban sebagai media untuk melakukan tindak pidana. Pasal 65 ayat (3) melarang Setiap Orang untuk menggunakan Data Pribadi yang bukan miliknya yang mana aturan pidananya diatur dalam Pasal 67 ayat (3). Sedangkan Pasal 66 melarang pembuatan Data Pribadi palsu yang dapat merugikan orang lain yang mana aturan pidananya diatur dalam Pasal 88.

Selain kasus dengan nomor perkara 1295/Pid.Sus/2023/PN Mdn, modus penipuan *giveaway* tersebut nyatanya terus berlanjut hingga saat ini. Seperti yang dilaporkan pada hari Senin, 28 Agustus 2023 ke Polres Gowa. Ratnawati, seorang ibu rumah tangga berusia 31 tahun dimintai uang administrasi senilai Rp. 7.450.000 (tujuh juta empat ratus lima puluh ribu rupiah) oleh pelaku sebagai syarat dari pencairan hadiah *giveaway* senilai 50 juta rupiah.[42] Seperti kasus sebelumnya, Kepala Seksi Humas Polres Gowa menyatakan bahwa korban mendapatkan sebuah panggilan sempat dapat panggilan video dengan Baim Wong atau istrinya (Paula).[43] Baim Wong sebagai korban dari pemalsuan data pribadi mengatakan bahwa dirinya bingung untuk mengantisipasi penipuan yang mengatasnamakan dirinya, dikarenakan modus penipuan tersebut tetap berjalan hingga banyaknya korban berjatuhan.[44] Meskipun telah terdapat aturan pidana mengenai pemalsuan data biometrik, namun belum adanya aturan mengenai pertanggungjawaban pidana atas tindak pidana *deepfake* dapat menimbulkan kekosongan hukum. Hal ini dikarenakan tindak pidana *deepfake* tidak hanya dilakukan oleh manusia sebagai orang perorangan, namun juga melibatkan *artificial intelligence* yang dapat berupa *website* maupun aplikasi yang dijalankan oleh programmer.

[41] Hadi Purnomo and Andre Yosua M, "Inkonsistensi Penegakan Hukum Tindak Pidana Hoaks Di Indonesia Pasca Reformasi," *Jurnal Ius Constituendum* 6, no. 2 (2021), http://dx.doi.org/10.26623/jic.v6i1.3176.

[42] Nur Afni Aripin, "Tertipu 'Video Call Baim Wong', IRT di Gowa Kehilangan Uang Rp 7 Juta," *detikjatim*, August 31, 2023, https://www.detik.com/jatim/hukum-dan-kriminal/d-6905688/tertipu-video-call-baim-wong-irt-di-gowa-kehilangan-uang-rp-7-juta.

[43] Aripin.

[44] Dewantoto and David Oliver Purpa, "Lagi, Penipuan 'Giveaway' Catut Nama Baim Wong, Bagaimana Pelaku Meyakinkan Korbannya? Halaman All - Kompas.Com."

Received: 30-3-2024
Revised: 1-4-2024
Accepted: 11-5-2024
e-ISSN: 2621-4105

Kekosongan hukum ini dapat mengakibatkan timbulnya korban-korban baru dikarenakan kurangnya upaya pencegahan melalui hukum.

3.2 Pengaturan Yang Ideal Mengenai Tindak Pidana *Deepfake* Di Masa Mendatang

Hukum pidana dianggap mengalami kegagalan dalam menangani tindak pidana yang dilakukan oleh *artificial intelligence.*[45] Hal ini dikarenakan minimnya aturan pidana terkait dengan *artificial intelligence*, meskipun bahaya dari *artificial intelligence* telah dirasakan oleh masyarakat dunia. Sekretaris Jenderal PBB Antonio Guterres bahkan mengatakan bahwa *artificial intelligence* menimbulkan ancaman bagi umat manusia setara dengan "perang nuklir".[46] Sudah sepatutnya hukum hadir untuk melindungi masyarakat, khususnya masyarakat Indonesia. Tindak pidana yang timbul atas *artificial intelligence* seperti penyalahgunaan *deepfake* pada hakikatnya merupakan tindak pidana yang telah ada namun terpengaruh perkembangan teknologi. Seperti tindak pidana penipuan yang telah terdapat dalam KUHP, namun dengan hadirnya teknologi *deepfake* yang menggunakan identitas orang lain menjadikannya tindak pidana baru. Hal ini dikarenakan penyalahgunaan *deepfake* memiliki dampak yang lebih besar dari penipuan biasa.[47] Penyalahgunaan *deepfake* tidak hanya menggunakan aspek verbal dalam penipuan, namun juga aspek visual yang menggunakan identitas orang lain.[48] Aspek visual memiliki efek yang lebih besar dikarenakan secara umum manusia lebih mengandalkan informasi secara visual dibandingkan informasi sensorik lainnya yang disebut sebagai efek dominasi visual colavita.[49] Efek dominasi visual colavita menjelaskan bahwa masyarakat lebih cenderung mengingat pesan visual daripada pesan verbal, yang menyebabkan informasi visual palsu lebih banyak dipercaya dibandingkan dengan informasi verbal.

Hadirnya tindak pidana atas penyalahgunaan *deepfake* seharusnya dapat diatasi dengan penerapan hukum. Namun dengan tidak adanya aturan di Indonesia yang mengatur mengenai *deepfake* secara eksplisit dapat menyebabkan kekosongan hukum yang menimbulkan ketidakpastian hukum. Hal ini dikarenakan ketidakjelasan mengenai apa yang harus dilakukan untuk mencegah maupun menanggulangi tindak pidana *deepfake* maupun tindak pidana yang akan datang dari sebuah *artificial intelligence.* Kekosongan hukum ini dengan jelas menggambarkan adagium *het recht hinkt achter de faiten aan* yang menyatakan bahwa hukum diibaratkan berjalan tertatih-tatih yang mana tertinggal dari perkembangan manusia.[50] Padahal sejatinya hukum bersifat dinamis, yakni dapat bergerak mengikuti perkembangan manusia. Perubahan-perubahan baik dalam masyarakat maupun dalam suatu teknologi menuntut hukum agar berkembang sebagaimana mestinya.

---

[45] Ryan Abbott, *The Reasonable Robot: Artificial Intelligence and the Law* (Cambridge, United Kingdom ; New York, NY, USA: Cambridge University Press, 2020).

[46] Adla Massoud, "UN Chief Warns AI Threat on Par with 'Nuclear War,'" *The National*, June 12, 2023, sec. World, https://www.thenationalnews.com/world/2023/06/12/un-chief-warns-ai-threat-on-par-with-nuclear-war/.

[47] Hancock and Bailenson, "The Social Impact of Deepfakes."

[48] Hancock and Bailenson.

[49] Markus Prior, "Visual Political Knowledge: A Different Road to Competence?," *The Journal of Politics* 76, no. 1 (January 2014): 41–57, https://doi.org/10.1017/S0022381613001096.

[50] Raharjo, "Reformasi Menuju Hukum Progresif."

Received: 30-3-2024
Revised: 1-4-2024
Accepted: 11-5-2024
e-ISSN: 2621-4105

Sebagaimana teori hukum progresif yang digagas oleh Satjipto Rahardjo yang menyatakan bahwa hukum dibentuk untuk manusia bukan manusia untuk hukum.[51] Hukum sudah sepatutnya melindungi kepentingan manusia dengan aturan-aturannya. Satjipto Rahardjo berpendapat bahwa hukum merupakan suatu alat untuk mewujudkan kepentingan manusia.[52] Hukum pada saat ini bergerak statis berbanding terbalik dengan perkembangan masyarakat yang bergerak dinamis.[53]

Indonesia pada hakikatnya merupakan negara yang menganut sistem hukum *civil law* yang mana tidak dapat mengadili perkara apabila tidak terdapat suatu aturan hukum yang mengaturnya. Pembaharuan hukum mengenai tindak pidana *deepfake* harus dilakukan dalam memenuhi asas legalitas hukum pidana untuk sebuah kepastian hukum. Terdapat pokok-pokok pikiran yang wajib dicermati terkait dengan pembaharuan hukum mengenai tindak pidana *deepfake*, adapun pokok-pokok pikiran sebagai berikut: Pertama, telah terdapat aturan mengenai *deepfake* sejak tahun 2019 di negara lain yang dapat menjadi acuan dalam pembuatan regulasi *deepfake* di Indonesia. Di Amerika serikat, tepatnya di California telah terdapat dua aturan yang disahkan sebagai bentuk pencegahan atas efek *deepfake* terhadap distribusi materi seksual eksplisit dan pemilihan umum tanpa persetujuan.[54] Aturan pertama adalah *Assembly Bill Number* 602 yang ditambahkan ke dalam hukum perdata negara bagian California yang menentukan pembuatan *deepfake* mengenai pornografi harus mendapatkan suatu persetujuan, apabila hal tidak dengan persetujuan individu terkait, maka dapat dikenakan ganti rugi hingga $ 150.000.[55] Aturan kedua mengenai *deepfake* di California terdapat dalam *Assembly Bill Number* 730 yang telah disahkan menjadi *Chapter 493, Statutes of 2019* California yang melarang produksi, distribusi *deepfake* seorang kandidat, komite kampanye politik, partai politik, atau entitas lain dalam waktu 60 hari setelah pemilu.[56] Larangan ini tidak berlaku jika audio atau video *deepfake* tersebut memuat pengungkapan yang menyatakan bahwa media tersebut telah dimanipulasi atau diberi tanda *(AI-Generated)*.

Kedua, China sebagai negara yang menganut sistem hukum *civil law* dapat menjadi contoh bagi Indonesia yang menganut sistem hukum yang sama dalam hal pembuatan aturan mengenai *deepfake*. Pada 18 November 2019, Kementerian Kebudayaan dan Pariwisata, Administrasi Cyberspace Tiongkok, dan Administrasi Radio dan Televisi Nasional mengeluarkan Provisi Administratif tentang Layanan Informasi Audio-visual

[51] Satjipto Rahardjo, *Hukum Progresif* (Yogyakarta: Genta Press, 2009).
[52] Herol Hansen Samin, "Perlindungan Hukum Terhadap Kebocoran Data Pribadi Oleh Pengendali Data Melalui Pendekatan Hukum Progresif.," *Ampus Akademik Publishing Jurnal Sains Student Research* 1, No. 2 (2023), https://doi.org/10.15294/ciils.v3i1.78690.
[53] M. Zulfa Aulia, "Ulasan Tokoh Dan Pemikiran Hukum Hukum Progresif Dari Satjipto Rahardjo: Riwayat, Urgensi, Dan Relevansi.," *Undang: Jurnal Hukum* 1, no. 1 (June 1, 2018): 159–85, https://doi.org/10.22437/ujh.1.1.159-185.
[54] Juan Felipe Rodrigo López, "Tragic Realism: How to regulate Deepfakes in Colombia?," *Latin American Law Review*, no. 8 (February 2022): 125–45, https://doi.org/10.29263/lar08.2022.08.
[55] Rodrigo López.
[56] Rodrigo López.

Received: 30-3-2024
Revised: 1-4-2024
Accepted: 11-5-2024
e-ISSN: 2621-4105

Online.[57] Aturan ini juga mengatur yang berhubungan dengan produksi, distribusi, dan publikasi terkait dengan *deepfake.* Aturan ini mengatur mengenai dilarangnya memproduksi, menerbitkan, atau menyebarkan informasi yang membahayakan keamanan politik dan stabilitas sosial serta rumor internet, pencabulan, dan pelanggaran hak orang lain atas reputasi. *Internet Provider* juga diatur untuk melakukan penilaian keamanan apabila menawarkan fungsi dan layanan yang menggunakan *deepfake*. Pasal 11 peraturan ini juga mengatur mengenai ketentuan di mana penyedia layanan diwajibkan untuk melakukan penandaan pada *deepfake* yang diproduksi, dipublikasikan, dan disebarluaskan di *website* maupun aplikasi tersebut.

Ketiga, pada saat ini telah terdapat aturan mengenai *Artificial Intelligence* yang juga mengatur mengenai *deepfake* di Eropa. Uni Eropa telah mengatur tindak pidana *deepfake* dalam *Artificial Intelligence Act* yang merupakan ketentuan hukum mengenai *Artificial Intelligence* komprehensif pertama di dunia sebagai wujud dari kepastian hukum.[58] Hal ini menggambarkan bahwa pembaharuan hukum mengenai aturan *deepfake* bukanlah sebuah kemustahilan. Dalam rangka meminimalisir akibat dari tindak pidana *deepfake*, *Artificial Intelligence Act* mengatur beberapa hal, salah satunya adalah keterbukaan atas konten *deepfake.* Pasal 52 ayat (3) *Artificial Intelligence Act* yang menyatakan bahwa setiap orang yang menciptakan ataupun menyebarkan *deepfake* harus mengungkapkan bahwa hal tersebut adalah sebuah media tiruan (bukan media asli) dengan tujuan untuk meminimalisir penyalahgunaan media palsu tersebut.[59] Meskipun aturan mengenai *deepfake* tersebut masih tergolong baru, namun hal tersebut menjadi dasar perlindungan masyarakat Uni Eropa akan bahaya *deepfake. Artificial Intelligence Act* Uni Eropa dapat menjadi acuan untuk membuat aturan terkait *deepfake* di Indonesia. Indonesia dapat membuat aturan yaitu dengan membuat regulasi agar suatu *deepfake* yang dibuat oleh aplikasi maupun website terdapat tanda yang menyatakan bahwa media tersebut adalah palsu atau dibuat oleh *Artificial Intelligence (AI-Generated).* Penanda *deepfake* seperti ini sangat penting untuk mengatasi dampak buruk yang ditimbulkan oleh *deepfake*, yakni untuk meminimalisir penyalahgunaan data pribadi atas teknologi *deepfake*.[60]

Keempat, pembuatan aturan mengenai pembatasan teknologi bukanlah hal yang asing di Indonesia, sebelumnya terdapat Peraturan Menteri Perdagangan Nomor 31 Tahun 2023 yang mengatur mengenai larangan untuk berjualan di *platform* media sosial seperti Tiktok shop, yang mana sejatinya fungsi media sosial hanyalah sebagai media promosi.[61] Peraturan

[57] "Pemberitahuan tentang penerbitan "Ketentuan tentang Administrasi Layanan Informasi Audio Visual Online"_ Kantor Komisi Keamanan Cyber dan Teknologi Informasi," 2019, https://www.cac.gov.cn/2019-11/29/c_1576561820967678.htm.

[58] Shiona McCallum, Liv McMahon, and Tom Singleton, "MEPs Approve World's First Comprehensive AI Law," *BBC*, March 13, 2024, https://www.bbc.com/news/technology-68546450.

[59] "Artificial Intelligence Act" (2024), https://data.consilium.europa.eu/doc/document/ST-5662-2024-INIT/en/pdf.

[60] Jack Langa, "Deepfakes, Real Consequences: Crafting Legislation To Combat Threats Posed By Deepfakes," *Boston University Law Review* 101, no. 2 (2021), https://www.bu.edu/bulawreview/files/2021/04/LANGA.pdf.

[61] Tim CNN Indonesia, "Poin-poin Permendag soal Larangan Social Ecommerce Seperti TikTok Shop," *ekonomi*, September 27, 2023, https://www.cnnindonesia.com/ekonomi/20230927172615-92-1004544/poin-poin-permendag-soal-larangan-social-ecommerce-seperti-tiktok-shop.

Received: 30-3-2024
Revised: 1-4-2024
Accepted: 11-5-2024
e-ISSN: 2621-4105

ini dibuat sebagai upaya pemerintah melindungi usaha mikro kecil dan menengah (UMKM) di dalam negeri serta mengedepankan kesetaraan dalam persaingan usaha. Hal tersebut menggambarkan bahwa bukanlah hal yang mustahil untuk diadakannya aturan pembatasan penggunaan mengenai teknologi *deepfake*. Pembatasan mengenai penggunaan suatu aplikasi ataupun website juga telah diatur dalam Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik Lingkup Privat. Namun aturan tersebut belum mengakomodasi terkait penggunaan *deepfake.* Aturan pembatasan *deepfake* dapat diterbitkan oleh kementerian yang berwenang, seperti Kementrian Komunikasi dan Informatika yang berbunyi "Pembuatan media tiruan menggunakan kecerdasan buatan hanya diperbolehkan jika berdasarkan persetujuan pihak terkait dan diberi tanda bahwa media tersebut merupakan media tiruan". Hal tersebut menyatakan bahwa penggunaan *deepfake* diperbolehkan namun dengan pemberian tanda bahwa media tersebut merupakan media palsu dan dengan persetujuan orang terkait.

Sanksi administratif pada tindak pidana *deepfake* dapat diterapkan terhadap *provider/developer* sebuah *website* ataupun aplikasi yang mengandung *artificial intelligence* dengan mengacu kepada penegakan hukum suatu korporasi. Dalam sebuah korporasi, meskipun yang melakukan suatu tindak pidana adalah direksi, namun korporasi tersebut dapat dikenakan sanksi administratif seperti pembubaran korporasi.[62] Hal tersebut diatur dalam *lex generali* hukum pidana yaitu Kitab Undang-Undang Hukum Pidana 2023 yang menjadikan korporasi sebagai suatu badan hukum. Persamaan penegakan hukum terhadap website ataupun aplikasi teknologi *deepfake* dengan suatu korporasi dapat dilakukan dikarenakan *developer/provider* dalam suatu aplikasi atau website yang menjalankan program aplikasi ataupun website tersebut sama seperti direksi menjalankan suatu korporasi. Namun suatu korporasi hanya dapat dijalankan minimal oleh 2 (dua) orang, sedangkan sebuah website ataupun aplikasi dapat dijalankan oleh minimal seorang *programmer* saja. *Website* ataupun aplikasi *deepfake* dapat diberikan sanksi administratif apabila pengguna maupun pengembang/penyedia aplikasi atau website tersebut terlibat dalam suatu tindak pidana *deepfake* yang berupa pemutusan akses di wilayah Indonesia. Selain itu, penelitian ini menyarankan adanya perubahan pada Pasal 70 ayat (1) UU PDP yang berbunyi "Dalam hal tindak pidana sebagaimana dimaksud dalam Pasal 67 dan Pasal 68 dilakukan oleh korporasi, pidana dapat dijatuhkan kepada pengurus, pemegang kendali, pemberi perintah, pemilik manfaat, dan/ atau Korporasi" menjadi "Dalam hal tindak pidana sebagaimana dimaksud dalam Pasal 67, Pasal 68, *dan Pasal 68A* dilakukan oleh korporasi, pidana dapat dijatuhkan kepada pengurus, pemegang kendali, pemberi perintah, pemilik manfaat, dan/ atau korporasi".

Kelima, terdapat kemungkinan adanya konten *deepfake* yang tidak diberi penanda bahwa hal tersebut dihasilkan oleh *artificial intelligence* yang diproduksi di negara lain namun dibagikan di Indonesia. Selain adanya aturan mengenai *deepfake*, diperlukan lebih

[62] Alya Sani Pratiwi et al., "Pelaksanaan Pemberian Sanksi Bagi Perusahaan Yang Tidak Mempekerjakan Tenaga Kerja Penyandang Disabilitas," *Jurnal USM Law Review* 6, no. 1 (n.d.), http://dx.doi.org/10.26623/julr.v6i1.6817herol.

Received: 30-3-2024
Revised: 1-4-2024
Accepted: 11-5-2024
e-ISSN: 2621-4105

banyak kerja sama internasional antara pemerintah dan jaringan sosial untuk mengatasi akibat dari tindak pidana *deepfake*.[63] Penelitian ini menyarankan untuk menambahkan aturan kerjasama dengan menyisipkan Pasal 62A di antara Pasal 62 dan Pasal 63 yang mana terdapat dalam Bab X UU PDP mengenai kerjasama internasional. Pasal 62A yang disarankan penelitian ini dapat berbunyi "Kerja sama internasional dilakukan terkait dengan penggunaan data pribadi menggunakan kecerdasan buatan". Kerja sama penggunaan data pribadi menggunakan kecerdasan buatan berbeda dengan kerja sama internasional pada umumnya dikarenakan kerja sama penggunaan data pribadi menggunakan kecerdasan buatan tidak hanya mencakup kerja sama negara saja, namun juga kerja sama terhadap provider kecerdasan buatan. Kemudian dalam penjelasan pasal tersebut dapat dijelaskan dengan penjelasan yang berbunyi "yang dimaksud dengan kerja sama internasional dalam penggunaan data pribadi menggunakan kecerdasan buatan adalah kerja sama terkait aturan penggunaan penanda akan media tiruan yang dibuat oleh kecerdasan buatan, hal ini mencakup dengan kerja sama dengan *platform* kecerdasan buatan dan/atau negara asal pembuatan media tiruan".

Keenam, kebijakan hukum pidana dapat menjadi sebuah solusi untuk mengatasi tindak pidana baru seperti tindak pidana *deepfake*. Hal ini dikarenakan kebijakan hukum pidana digunakan untuk menilai suatu efektivitas hukum pidana dalam rangka pembaharuan hukum pidana, atau yang biasa dikenal dengan *penal reform*.[64] Melakukan tindak pidana memalsukan data pribadi menggunakan kecerdasan buatan dapat disamakan dengan menyuruh binatang melakukan suatu tindak pidana dikarenakan dapat melakukan suatu tindakan sendiri, namun tidak memiliki kemampuan berpikir layaknya seorang manusia. Jacob Turner, seorang pengacara internasional yang juga merupakan seorang penulis, mengatakan bahwa persamaan tersebut dapat dilihat dari *self-driving car* yang mana dijalankan oleh *artificial intelligence* dan kereta kuda yang dijalankan oleh kuda yang mana keduanya diperintah oleh manusia.[65] Namun penerapan pidana terkait menyuruh binatang dan menyuruh *artificial intelligence* dianggap lebih berat hukumannya apabila menyuruh *artificial intelligence* melakukan tindak pidana. Marvin Minsky, pelopor *artificial intelligence*, dalam sebuah diskusi tentang sejauh mana kecerdasan seperti yang ditunjukkan oleh manusia dan entitas buatan berbeda dari apa yang disebut "kecerdasan" pada hewan mengatakan bahwa hewan mampu untuk belajar dan mengembangkan keterampilan sendiri seperti halnya mencari mangsa, namun hal tersebut memanglah yang seharusnya dilakukan oleh hewan.[66] Sebaliknya, *artificial intelligence* dapat berfungsi tidak hanya berdasarkan apa yang telah diprogram untuk dilakukan tetapi dapat belajar dan memakukan sesuatu sendiri.

[63] Rodrigo López, "Tragic Realism."
[64] Nandang Sambas and Ade Mahmud, *Perkembangan Hukum Pidana* (Bandung: PT. Refika Aditama, 2019).
[65] Jacob Turner, *Robot Rules: Regulating Artificial Intelligence* (Cham: Springer International Publishing, 2019), https://doi.org/10.1007/978-3-319-96235-1.
[66] Marvin Minsky, *The Society of Mind* (New York: Simon and Schuster, 1986).

Received: 30-3-2024
Revised: 1-4-2024
Accepted: 11-5-2024
e-ISSN: 2621-4105

Ketentuan mengenai larangan penggunaan *deepfake* dapat diatur dalam UU PDP dengan menyisipkan Pasal 66A di antara Pasal 66 dan Pasal 67. Pasal tersebut dapat berbunyi "Setiap Orang dilarang membuat Data Pribadi palsu atau memalsukan Data Pribadi orang lain dengan menggunakan kecerdasan buatan dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian bagi orang lain". Pasal tersebut dirumuskan berbeda dengan Pasal 66 yang mengatur mengenai larangan pemalsuan data pribadi secara umum dikarenakan dengan menggunakan bantuan seperti *artificial intelligence* (kecerdasan buatan), maka pelaku tidak secara langsung melakukan hal tersebut, namun melalui perantara seperti aplikasi atau *website* yang menggunakan *artificial intelligence*.

Dengan ditambahkannya sisipan Pasal 66A di antara Pasal 66 dan Pasal 67 UU PDP, maka pada hakikatnya terdapat penambahan pasal dalam Bab XIV Ketentuan Pidana. Ketentuan pidana dapat diatur dengan menyisipkan Pasal 68A di antara Pasal 68 dan Pasal 69 UU PDP. Pasal tersebut dapat berbunyi "Setiap Orang dilarang membuat Data Pribadi palsu atau memalsukan Data Pribadi orang lain dengan menggunakan kecerdasan buatan dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian bagi orang lain sebagaimana dimaksud pada Pasal 66A dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau pidana denda paling banyak Rp 8.000.000.000,00 (delapan miliar rupiah)". Lama pidana penjara dan banyaknya denda tersebut merujuk pada Pasal 68 yang mengatur mengenai pidana atas pembuatan data pribadi palsu dan juga merujuk pada Pasal 490 KUHP ayat (1) mengenai memerintahkan hewan. Pasal 490 KUHP ayat (1) berbunyi "barang siapa mengacuhkan binatang kepada manusia atau kepada binatang yang ditunggangi, dipasang di kereta atau di gerobak atau yang dimuati barang". R. Soesilo berpendapat bahwa yang dimaksud dengan mengacuhkan binatang adalah menyuruh binatang melakukan sesuatu, seperti memerintahkan anjing untuk mengejar orang lain.[67]

4. PENUTUP

Deepfake yang merupakan sebuah media yang sangat realistis dalam bentuk sebuah gambar, video, maupun suara yang dibuat oleh *artificial intelligence* dapat diakses oleh semua orang, tanpa batasan apapun. Indonesia hanya mengatur mengenai pemalsuan data pribadi secara umum dalam UU PDP dan juga pemalsuan secara elektronik dalam UU ITE yang merupakan turunan dari UUD NRI 1945. Aturan mengenai pemalsuan data pribadi menggunakan kecerdasan di Indonesia belum mengatur secara eksplisit mengenai tindak pidana *deepfake.* Kekosongan hukum atas teknologi *deepfake* dapat menimbulkan ketidakpastian hukum yang disebabkan oleh ketidakjelasan mengenai apa yang harus dilakukan untuk mencegah maupun menanggulangi tindak pidana *deepfake* maupun tindak pidana di masa yang akan datang yang diakibatkan oleh penyalahgunaan *artificial intelligence*. Penelitian ini menyarankan agar adanya pembuatan aturan *deepfake* yang

[67] R. Soesilo, *Kitab Undang-Undang Hukum Pidana (KUHP) Serta Komentar-Komentarnya Lengkap Pasal Demi Pasal.* (Bogor: Politeia, 1991).

Received: 30-3-2024
Revised: 1-4-2024
Accepted: 11-5-2024
e-ISSN: 2621-4105

diterbitkan Kementerian Komunikasi dan Informatika mengenai pembatasan penggunaan *deepfake* untuk diberikan penanda bahwa media tersebut telah dimanipulasi. Selain itu penelitian ini menyarankan untuk kriminalisasi terhadap perbuatan *deepfake* yang dapat merugikan orang lain yang dapat disisipkan dalam UU PDP.

DAFTAR PUSTAKA

Abbott, Ryan. *The Reasonable Robot: Artificial Intelligence and the Law*. Cambridge, United Kingdom ; New York, NY, USA: Cambridge University Press, 2020.

Alya Sani Pratiwi, Sonhaji, Suhartoyo, and Endah Pujiastuti. "Pelaksanaan Pemberian Sanksi Bagi Perusahaan Yang Tidak Mempekerjakan Tenaga Kerja Penyandang Disabilitas." *Jurnal USM Law Review* 6, no. 1 (n.d.). http://dx.doi.org/10.26623/julr.v6i1.6817herol.

Andang Furqon. *Pengantar Hukum Indonesia*. Bandung: fakultas hukum unisba, 2005.

Aripin, Nur Afni. "Tertipu 'Video Call Baim Wong', IRT di Gowa Kehilangan Uang Rp 7 Juta." *detikjatim*, August 31, 2023. https://www.detik.com/jatim/hukum-dan-kriminal/d-6905688/tertipu-video-call-baim-wong-irt-di-gowa-kehilangan-uang-rp-7-juta.

Artificial Intelligence Act (2024). https://data.consilium.europa.eu/doc/document/ST-5662-2024-INIT/en/pdf.

Aulia, M. Zulfa. "Ulasan Tokoh Dan Pemikiran Hukum Hukum Progresif Dari Satjipto Rahardjo: Riwayat, Urgensi, Dan Relevansi." *Undang: Jurnal Hukum* 1, no. 1 (June 1, 2018): 159–85. https://doi.org/10.22437/ujh.1.1.159-185.

David Klepper. "Deepfakes from Gaza War Increase Fears about AI's Power to Mislead AP News." Fake babies, real horror: Deepfakes from the Gaza war increase fears about AI's power to mislead. Accessed May 6, 2024. https://apnews.com/article/artificial-intelligence-hamas-israel-misinformation-ai-gaza-a1bb303b637ffbbb9cbc3aa1e000db47.

Dewantoto and David Oliver Purpa. "Lagi, Penipuan 'Giveaway' Catut Nama Baim Wong, Bagaimana Pelaku Meyakinkan Korbannya? Halaman All - Kompas.Com." *Kompas.Com*, April 11, 2023. https://medan.kompas.com/read/2023/04/11/105816078/lagi-penipuan-giveaway-catut-nama-baim-wong-bagaimana-pelaku-meyakinkan?page=all#google_vignette.

Dian Nita. "Baim Wong Sebut Pelaku Penipuan Giveaway Pintar Mainkan Suara Dari Potongan Videonya." *Kompas TV*, April 11, 2023. https://www.kompas.tv/entertainment/396955/baim-wong-sebut-pelaku-penipuan-giveaway-pintar-mainkan-suara-dari-potongan-videonya?page=all.

Faiz Emery Muhammad and Beniharmoni Harefa. "Pengaturan Tindak Pidana Bagi Pelaku Penipuan Phisning Berbasis Web." *Jurnal USM Law Review* 6, no. 1 (2023). http://dx.doi.org/10.26623/julr.v6i1.6649.

Fallis, Don. "The Epistemic Threat of Deepfakes." *Philosophy & Technology* 34, no. 4 (December 2021): 623–43. https://doi.org/10.1007/s13347-020-00419-2.

Frankish, Keith, and William M. Ramsey, eds. *The Cambridge Handbook of Artificial Intelligence*. Cambridge, United Kingdom: Cambridge University Press, 2014.

Gede Arga Adrian. "Deepfake: Bakal Dalang Hoax Jelang Pemilu 2024?" Deepfake: Bakal Dalang Hoax Jelang Pemilu 2024? Accessed May 6, 2024.

Received: 30-3-2024
Revised: 1-4-2024
Accepted: 11-5-2024
e-ISSN: 2621-4105

https://www.ums.ac.id/berita/unggulan/deep-fake-bakal-dalang-hoax-jelang-pemilu-2024.

Hadi Purnomo and Andre Yosua M. "Inkonsistensi Penegakan Hukum Tindak Pidana Hoaks Di Indonesia Pasca Reformasi." *Jurnal Ius Constituendum* 6, no. 2 (2021). http://dx.doi.org/10.26623/jic.v6i1.3176.

Hancock, Jeffrey T., and Jeremy N. Bailenson. "The Social Impact of Deepfakes." *Cyberpsychology, Behavior, and Social Networking* 24, no. 3 (March 1, 2021): 149–52. https://doi.org/10.1089/cyber.2021.29208.jth.

Herol Hansen Samin. "Perlindungan Hukum Terhadap Kebocoran Data Pribadi Oleh Pengendali Data Melalui Pendekatan Hukum Progresif." *Ampus Akademik Publishing Jurnal Sains Student Research* 1, no. 2 (2023). https://doi.org/10.15294/ciils.v3i1.78690.

Husni Kurniawati and Yunanto. "Perlindungan Hukum Terhadap Penyalahgunaan Data Pribadi Debitur Dalam Aktivitas Pinjaman Online." *Jurnal Ius Constituendum* 7, no. 1 (2022). http://dx.doi.org/10.26623/jic.v7i1.4290.

Isnaini Imroatus Solichah, Faizin Sulistio, and Milda Istiqomah. "Protection of Victims of Deep Fake Pornography in a Legal Perspective in Indonesia." *International Journal of Multicultural and Multireligious Understanding* 10, no. 1 (2023). https://ijmmu.com/index.php/ijmmu/article/view/4409/3755.

Jack Langa. "Deepfakes, Real Consequences: Crafting Legislation To Combat Threats Posed By Deepfakes." *Boston University Law Review* 101, No. 2 (2021). https://www.bu.edu/bulawreview/files/2021/04/LANGA.pdf.

James Vincent. "Why We Need a Better Definition of 'Deepfake' - The Verge," May 23, 2018. https://www.theverge.com/2018/5/22/17380306/deepfake-definition-ai-manipulation-fake-news.

Jeremiah Maximillian Laza and Rizky Karo Karo. "Perlindungan Hukum Terhadap Artificial Intellegence Dalam Aspek Penyalahgunaan Deepfake Technology Pada Perspektif Uu Pdp Dan Gdpr." *Lex Prospicit* 1, no. 2 (2023). http://dx.doi.org/10.19166/lp.v1i2.7386.

John Brandon. "Terrifying High-Tech Porn: Creepy 'deepfake' Videos Are on the Rise." *Fox News*, February 20, 2018. https://www.foxnews.com/tech/terrifying-high-tech-porn-creepy-deepfake-videos-are-on-the-rise.

Juefei-Xu, Felix, Run Wang, Yihao Huang, Qing Guo, Lei Ma, and Yang Liu. "Countering Malicious DeepFakes: Survey, Battleground, and Horizon." *International Journal of Computer Vision* 130, no. 7 (July 2022): 1678–1734. https://doi.org/10.1007/s11263-022-01606-8.

Kelleher, John D. *Deep Learning*. The MIT Press Essential Knowledge Series. Cambridge, Massachusetts: The MIT Press, 2019.

Koppen, Camille, and Charles Spence. "Seeing the Light: Exploring the Colavita Visual Dominance Effect." *Experimental Brain Research* 180, no. 4 (June 22, 2007): 737–54. https://doi.org/10.1007/s00221-007-0894-3.

Kugler, Matthew B., and Carly Pace. "Deepfake Privacy: Attitudes and Regulation." *SSRN Electronic Journal*, 2021. https://doi.org/10.2139/ssrn.3781968.

Kurniawan, Itok. "Analisis Terhadap Artificial Intelligence Sebagai Subjek Hukum Pidana." *Mutiara : Jurnal Ilmiah Multidisiplin Indonesia* 1, no. 1 (July 18, 2023): 35–44. https://doi.org/10.61404/jimi.v1i1.4.

Received: 30-3-2024
Revised: 1-4-2024
Accepted: 11-5-2024
e-ISSN: 2621-4105

Lee, Patrick Yung Kang, Ning F. Ma, Ig-Jae Kim, and Dongwook Yoon. "Speculating on Risks of AI Clones to Selfhood and Relationships: Doppelganger-Phobia, Identity Fragmentation, and Living Memories." *Proceedings of the ACM on Human-Computer Interaction* 7, no. CSCW1 (April 14, 2023): 1–28. https://doi.org/10.1145/3579524.

Marvela. "Konten Disalahgunakan Untuk Penipuan, Baim Wong Tak Tinggal Diam." *Tempo*, July 7, 2021, sec. seleb. https://seleb.tempo.co/read/1480763/konten-disalahgunakan-untuk-penipuan-baim-wong-tak-tinggal-diam.

Massoud, Adla. "UN Chief Warns AI Threat on Par with 'Nuclear War.'" *The National*, June 12, 2023, sec. World. https://www.thenationalnews.com/world/2023/06/12/un-chief-warns-ai-threat-on-par-with-nuclear-war/.

Michael Water. "The Great Lengths Taken to Make Abraham Lincoln Look Good in Portraits." *Atlas Obscura*, July 12, 2017. https://www.atlasobscura.com/articles/abraham-lincoln-photos-edited.

Minsky, Marvin. *The Society of Mind*. New York: Simon and Schuster, 1986.

Nandang Sambas and Ade Mahmud. *Perkembangan Hukum Pidana*. Bandung: PT. Refika Aditama, 2019.

Prior, Markus. "Visual Political Knowledge: A Different Road to Competence?" *The Journal of Politics* 76, no. 1 (January 2014): 41–57. https://doi.org/10.1017/S0022381613001096.

R. Soesilo. *Kitab Undang-Undang Hukum Pidana (KUHP) Serta Komentar-Komentarnya Lengkap Pasal Demi Pasal*. Bogor: Politeia, 1991.

Raharjo, Satjipo. "Reformasi Menuju Hukum Progresif." *Unisia* 27, no. 53 (September 20, 2004): 238–41. https://doi.org/10.20885/unisia.vol27.iss53.art3.

Ramadhan, Dwi Galih. "'Perlindungan Hukum Atas Invensi Artificial Intelligence Di Era Revolusi Industri 4.0 & Society 5.0.'" Universitas Islam Indonesia, 2022.

Rista Maharani and Andria Luhur Prakoso. "Perlindungan Data Pribadi Konsumen Oleh Penyelenggara Sistem Elektronik Dalam Transaksi Digital." *Jurnal USM Law Review* 7, no. 1 (2024). http://dx.doi.org/10.26623/julr.v7i1.8705.

Rodrigo López, Juan Felipe. "Tragic Realism: How to regulate Deepfakes in Colombia?" *Latin American Law Review*, no. 8 (February 2022): 125–45. https://doi.org/10.29263/lar08.2022.08.

Samantha Cole. "This Deepfake of Mark Zuckerberg Tests Facebook's Fake Video Policies." *Motherboard Tech by Vice*, June 12, 2019. https://www.vice.com/en/article/ywyxex/deepfake-of-mark-zuckerberg-facebook-fake-video-policy.

Satjipto Rahardjo. *Hukum Progresif*. Yogyakarta: Genta Press, 2009.

Schick, Nina. *Deepfakes: The Coming Infocalypse*. New York New York: Twelve, 2020.

Shen, Tianxiang, Ruixian Liu, Ju Bai, and Zheng Li. "'Deep Fakes' Using Generative Adversarial Networks (GAN)," 2018.

Shiona McCallum, Liv McMahon, and Tom Singleton. "MEPs Approve World's First Comprehensive AI Law." *BBC*, March 13, 2024. https://www.bbc.com/news/technology-68546450.

"SIPP Pengadilan." Accessed March 28, 2024. https://sipp.pn-medankota.go.id/index.php/list_perkara.

Tim CNN Indonesia. "Poin-poin Permendag soal Larangan Social Ecommerce Seperti TikTok Shop." *ekonomi*, September 27, 2023.

Received: 30-3-2024
Revised: 1-4-2024
Accepted: 11-5-2024
e-ISSN: 2621-4105

https://www.cnnindonesia.com/ekonomi/20230927172615-92-1004544/poin-poin-permendag-soal-larangan-social-ecommerce-seperti-tiktok-shop.

Turner, Jacob. *Robot Rules: Regulating Artificial Intelligence*. Cham: Springer International Publishing, 2019. https://doi.org/10.1007/978-3-319-96235-1.

Vaccari, Cristian, and Andrew Chadwick. "Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News." *Social Media + Society* 6, no. 1 (January 2020): 205630512090340. https://doi.org/10.1177/2056305120903408.

Wahyu Beny Mukti Setiyawa, Erifendi Churniawan, and Femmy Silaswaty Faried. "Upaya Regulasi Teknologi Informasi Dalam Menghadapi Serangan Siber Guna Menjaga Kedaulatan Negara Kesatuan Republik Indonesia." *Jurnal USM Law Review* 3, no. 2 (2020). http://dx.doi.org/10.26623/julr.v6i1.6649.

Wojewidka, John. "The Deepfake Threat to Face Biometrics." *Biometric Technology Today* 2020, no. 2 (February 2020): 5–7. https://doi.org/10.1016/S0969-4765(20)30023-0.

Young, Nobert. *DeepFake Technology: Complete Guide to Deepfakes, Politics and Social Media*. United States? Nobert Young, 2019.

"关于印发《网络音视频信息服务管理规定》的通知_中央网络安全和信息化委员会办公室," 2019. https://www.cac.gov.cn/2019-11/29/c_1576561820967678.htm.