LEX PROSPICIT
Volume 1, Issue 2, July 2023

PERLINDUNGAN HUKUM TERHADAP *ARTIFICIAL INTELLEGENCE* DALAM ASPEK PENYALAHGUNAAN *DEEPFAKE TECHNOLOGY* PADA PERSPEKTIF UU PDP DAN GDPR

Jeremiah Maximillian Laza*, Rizky Karo Karo

Fakultas Hukum Universitas Pelita Harapan, Indonesia

*email: jeremiahlaza@gmail.com

Article Info

Article History:
Submitted: 1 August 2023
Revised: 28 November 2023
Published: 29 November 2023

Keywords:
Articial Intellegence; Deepfake; disinformation

Kata Kunci:
Artificial Intelligence; Deepfake; disinformasi

DOI:
http://dx.doi.org/10.19166/lp.v1i2.7368

Abstract

Deepfake is a hyper-realistic video that applies AI to depict a person saying and doing things that never happened using face-swapping that leaves little trace of evidence that the video was manipulated. Deepfake is a product of AI that combines, stitches, replaces and superimposes images and video clips to make a fake video look like it's real, and the video is said by the person when in reality the person whose face is replaced in the video never said or acted that way. The legal issue that arises from Deepfake is misinformation, disinformation and fraud, so there needs to be a law governing Deepfake, where in the European Union, regulations related to Deepfake are indirectly contained in the General Data Protection Regulation (GDPR), and in Indonesia itself there is Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). The formulation of the problem to be studied is how the legal protection of AI Deepfake in terms of the General Data Protection Regulation (GDPR), Law Number 27 of 2022 concerning Personal Data Protection. The research method used here is normative, where positive law in Indonesia and in the European Union will be used to analyze. In conclusion, Deepfake is not specifically regulated in either the PDP Law or GDPR, but because AI uses data to develop, the PDP Law and GDPR can still be relevant and can regulate to a certain degree regarding AI.

Abstrak

Deepfake merupakan video hiper-realistis yang menerapkan AI untuk menggambarkan seseorang mengatakan dan melakukan hal-hal yang tidak pernah terjadi. Misalnya dengan membuat pertukaran wajah yang meninggalkan sedikit jejak bukti ada manipulasi terhadap video tersebut. *Deepfake* merupakan suatu produk AI yang menggabungkan, mempersatukan, mengganti dan menempatkan gambar maupun klip video palsu tampak seperti video itu asli, dan video tersebut seolah-olah beisi perkataan atau berbuatan orang yang wajahnya muncul dalam video. Namun, kenyataan yang berbicara adalah orang pengganti yang wajahnya tidak muncul dalam video tersebut. Isu hukum yang muncul dari *deepfake* adalah tidak ada pengaturan hukum yang berisi rumusan kaidah yang mengatur larangan melakukan *deepfake* sebagai misinformasi, disinformasi serta penipuan. Oleh sebab itu penulis melakukan penelitian untuk menemukan peraturan dalam undang-undang yang ada rumusan yang dapat dipergunakan untuk meminta pertanggungjawaban hukum dari pelaku *deepfake*. Penulis berpendapat bahwa pengaturan *deepfake* secara tidak langsung tertuang pada *General*

Data Protection Regulation (GDPR), dan di Indonesia sendiri ada Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Oleh karenanya, masalah yang diangkat dalam penelitian ini adalah bagaimana penggunaan pengaturan *deepfake* dalam *General Data Protection Regulation* (GDPR) dan bagaimana UU PDP Indonesia meminta pertanggungjawaban hukum dari pelaku *deepfake* sebagai tindak pidana penipuan atau membuat berita bohong. Metode penelitian yang digunakan adalah metode penelitian hukum normatif. Dikumpulkan dan dibahas aturan hukum positif di Indonesia dan Uni Eropa sebagai sumber bahan hukum primer, serta kepustakaan yang terkait sebagai sumber bahan hukum sekunder. Ditemukan bahwa karena *deepfake* itu adalah AI yang menggunakan data atau informasi elektronik, maka UU PDP dan GDPR relevan digunakan untuk dipelajari pengaturan tentang larangan manipulasi AI untuk misinformasi, disinformasi atau penipuan serta pembuatan berita bohong di *cyberworld*.

1. PENDAHULUAN

Teknologi *Artificial Intelligence* atau yang disingkat sebagai AI, telah beralih dari yang hanya ada di laboratorium penelitian saja menjadi bagian dari kehidupan sehari-hari dengan kecepatan yang luar biasa. Sebagai contoh konkret dari *autonomous car* yang telah dibuat oleh Elon Musk di mana saat ini sudah diberikan persetujuan untuk beroperasi jalan di empat negara bagian di Amerika Serikat, termasuk District of Columbia,[1] hingga yang sekarang sudah dipakai oleh masyarakat luas yakni ChatGPT dengan rekor *user acquisition* tercepat di dalam sejarah manusia dengan 100 juta pengguna hanya dalam waktu 2 bulan saja. Bisa dikatakan bahwa dengan adanya implementasi AI dalam kehidupan masyarakat sehari-hari, perkembangan teknologi dan dinamika perubahan terhadap kehidupan sosial akan berubah menjadi lebih cepat dari perkembangan sebelum-sebelumnya.[2] Melihat hal tersebut, sudah tidak heran lagi jika dikatakan bahwa era AI sudah resmi dimulai.

Namun, dengan perkembangan yang begitu pesat, tentunya muncul kekhawatiran serta potensi negatif yang turut naik ke permukaan. Isu hukum dalam penyalahgunaan AI yang ada terdapat pada munculnya *deepfake* yang menjadi semakin viral di internet. *Deepfake* merupakan video hiper-realistis yang menerapkan AI untuk menggambarkan seseorang mengatakan dan melakukan hal-hal yang tidak pernah terjadi dengan menggunakan pertukaran wajah yang meninggalkan sedikit jejak bukti bahwa ada manipulasi terhadap video tersebut. *Deepfake* merupakan suatu produk dari AI yang menggabungkan, mempersatukan, mengganti dan menempatkan gambar maupun klip video untuk membuat video palsu bisa tampak seperti video itu asli, dan video tersebut dikatakan oleh orang tersebut padahal secara kenyataan orang yang digantikan wajahnya pada video tersebut tidak pernah berkata atau bertindak seperti itu. Teknologi ini bisa menghasilkan seperti contoh video lucu, pornografi ataupun video politik dari seseorang yang mengatakan sesuatu, tanpa adanya persetujuan dari orang yang ada di gambar dan suaranya terlibat di dalamnya. Ditambah dengan jangkauan dan kecepatan media sosial, *deepfake* yang meyakinkan dapat dengan cepat menjangkau puluhan jutaan orang dan

[1] FL. Yudhi Priyo Amboro and Khusuf Komarhana, "Prospek Kecerdasan Buatan Sebagai Subjek Hukum Perdata Di Indonesia," *Law Review* 21, no. 2 (November 2021): 145, https://doi.org/10.19166/lr.v0i2.3513.

[2] Meirza Aulia Chairani, Angga Pramodya Pradhana, and Taufiq Yuli Purnama, "The Urgency Of Developing Law As A Legal Basis For The Implementation Of Artificial Intelligence In Indonesia," *Law and Justice* 7, no. 1 (2022): 35-45, https://journals2.ums.ac.id/index.php/laj/article/view/760.

berdampak negatif pada masyarakat.[3] Potensi kejahatan yang dimiliki oleh *deepfake* ini sangatlah luas, ia bisa dipakai untuk melakukan penipuan untuk mengambil uang di bank, ia bisa digunakan untuk memeras seseorang, mencuri identitas seseorang, melakukan manipulasi harga saham, merusak reputasi merek yang ada, merusak reputasi seseorang, melakukan perundungan, melakukan intimdasi, dan lain sebagainya.

Menurut Presiden Microsoft yakni Brad Smith, di antara semua potensi bahaya AI, ia paling mengkhawatirkan mengenai perkembangan teknologi dari AI *deepfake* yang memiliki potensi yang tidak ada batasnya, yang jika berada di tangan yang salah, dapat memanipulasi dan memberikan misinformasi dan disinformasi kepada masyarakat sekitar, serta potensi penyalahgunaan data pribadi. Hal ini menimbulkan suatu masalah pada aspek keamanan data konsumen, serta faktor potensi misinformasi yang masif dari efek AI ini. Orang-orang memakai teknologi *deepfake* untuk mengimpersonasi *influencer*, *artist*, *public figure*, ataupun politikus atau presiden, di mana salah satu cara adalah dengan mengambil data pribadi, ataupun dari data yang sudah ada di publik dengan tujuan untuk merusak reputasi orang itu dan memberikan informasi yang tidak benar.[4] Teknologi *Deepfake* ini pertama kali mendapatkan perhatian dunia pada tahun 2017 lalu, di mana Mantan Presiden AS yakni Barrack Obama membuat pernyataan di internet yang ternyata tidak pernah ia lakukan. Hal yang serupa juga terjadi pada Presiden Joko Widodo sendiri mengenai video yang sangat viral di TikTok, di mana Presiden Jokowi bernyanyi lagu Cupid dari girlband asal Korea, Fifty-Fifty, yang merupakan hasil dari teknologi AI ini, yang menggantikan suara penyanyi asli dengan Presiden Jokowi, dan hasilnya akhirnya adalah seperti Presiden Jokowi benar-benar menyanyikan lagu tersebut. Meskipun di Indonesia sendiri kasus terhadap *Deepfake* ini belum ada yang parah, namun bisa dilihat potensi yang begitu besar yang mungkin dapat menyebabkan misinformasi serta disinformasi terutama pada pemilu yang akan datang di 2024.[5]

Dampak negatif yang ditimbulkan dari AI *deepfake* ini tentunya juga akan melanggar Hak atas Privasi yang dimiliki oleh manusia. Landasan filosofis mengenai hak privasi yang ada secara internasional tertera pada *International Covenant on Civil and Political Rights* (ICCPR) *Article 17* yang berisi:

> *"No one shall arbitrarily interfere with his privacy, family, home or correspondence, or attack his honor and reputation. Everyone has the right to legal protection against such interference or attacks." This right guarantees that everyone has the right to, in essence, "hide" or close parts of his life from the public eye as one of the most fundamental Human Rights.*

Sedangkan landasan filosofis yang ada di Indonesia terkait privasi mengacu kepada Pasal 28G ayat (1) Undang-undang Dasar 1945, menyebutkan bahwa:

(1) Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi.

---

[3] Luís Borges, Bruno Martins, and Pável Calado, "Combining Similarity Features and Deep Representation Learning for Stance Detection in the Context of Checking Fake News," *Journal of Data and Information Quality* 11, no. 3 (September 2019): 1–26, https://doi.org/10.1145/3287763.

[4] Benj Edwards, "Among AI dangers, Deepfakes Worry Microsoft President Most," *Ars Technica*, May 26, 2023, https://arstechnica.com/information-technology/2023/05/microsoft-president-declares-deepfakes-biggest-ai-concern.

[5] Nila Chrisna Yulika, "Apa Itu Deepfake, Ancaman yang Membayangi Pemilu 2024," *Liputan6*, March 15, 2023, https://www.liputan6.com/news/read/5233665/apa-itu-deepfake-ancaman-yang-membayangi-pemilu-2024.

Hak untuk mendapatkan perlindungan diri pribadi tidak hanya menyangkut pada dunia fisik saja, namun hak untuk perlindungan diri pribadi juga termasuk pada dunia maya, sehingga hak-hak seseorang terhadap diri pribadinya bisa juga terjaga di dunia maya. Pelanggaran terhadap hak atas privasi ini bisa terjadi ketika ada individu, perusahaan, dan bahkan AI, mengambil data yang dimiliki oleh seseorang tanpa seizin mereka, lalu kemudian data tersebut diolah untuk dijadikan sarana untuk menyebarkan misinformasi dan/atau disinformasi melalui sarana *deepfake.*

Selain itu adapun teori dalam teori hukum yang selaras dengan topik ini ialah Teori Perlindungan Hukum. Konsep negara hukum dan *rule of law* menegaskan pentingnya perlindungan hukum sebagai bagian integral dari sistem hukum yang adil dan berkeadilan. Hal ini melibatkan pengakuan dan perlindungan terhadap hak asasi manusia yang mendasar bagi setiap individu. Perlindungan hukum juga mencerminkan fungsi hukum yang penting, yaitu memberikan keadilan, ketertiban, kepastian, dan kemanfaatan bagi masyarakat. Melalui perlindungan hukum, individu atau kelompok yang merasa terancam atau merasa hak-haknya dilanggar dapat mencari keadilan dan memperoleh pemulihan atau ganti rugi yang pantas. Dengan demikian, perlindungan hukum merupakan prinsip fundamental dalam sistem hukum yang bertujuan untuk menjaga dan memastikan bahwa hak-hak individu dilindungi, aturan hukum ditegakkan, dan keadilan ditegakkan dalam masyarakat.

Oleh sebab itu, peneliti hendak melakukan penelitian lebih lanjut mengenai pencegahan *deepfake* sebagai himpunan bagian dari AI, dengan melakukan studi komparasi antara Uni Eropa dan Indonesia mengenai hukum-hukum yang ada, dan apakah hukum itu sudah cukup saat ini untuk melindungi subjek hukum dari potensial pelanggaran hukum yang dilakukan dengan munculnya *Deepfake*, serta apakah ada urgensi untuk membuat undang-undang baru secara internasional mengenai AI secara keseluruhan. Sehingga, rumusan masalah yang hendak diteliti adalah bagaimana perlindungan hukum terhadap AI *deepfake* yang ditinjau dari *General Data Protection Regulation* (GDPR), Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP).

2. METODE

Jenis penelitian yang digunakan adalah penelitian hukum normatif atau penelitian hukum doktriner. Dinamakan penelitian hukum doktriner dikarenakan penelitian ini hanya ditujukan pada peraturan-peraturan tertulis sehingga penelitian ini sangat erat hubungannya dengan kepustakaan karena akan membutuhkan data-data yang bersifat sekunder yang diperoleh dari perpustakaan. Bahan hukum primer yang akan diambil untuk digunakan pada penelitian ini adalah *General Data Protection Regulation*, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, dan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Bahan hukum sekunder yang akan digunakan pada penelitian ini adalah dari buku, jurnal nasional dan internasional, tesis, disertasi dan skripsi. Bahan hukum tersier yang akan digunakan adalah dari situs-situs seperti EU, White House, dan sebagainya. Penelitian ini menggunakan metode studi komparatif, yakni perbandingan hukum untuk mencari dan mensinyalir perbedaan dan persamaan dari implementasi perlindungan hukum terhadap *deepfake* di negara Indonesia serta Uni Eropa dengan meneliti bagaimana GDPR dan UU PDP mengatur serta melindungi subjek hukum dari *deepfake*, mengingat bahwa saat ini perlindungan hukum Uni Eropa terkait AI baik secara langsung maupun tidak langsung

serta perlindungan terhadap data pribadi, termasuk salah satu yang paling komprehensif di dunia internasional.[6]

3. HASIL DAN PEMBAHASAN

3.1 Kebijakan Hukum di Uni Eropa terkait *Deepfake*

Dalam era teknologi informasi saat ini, data telah menjadi komoditas yang sangat berharga dan dunia semakin berpusat pada data, di mana semua informasi manusia saat ini diolah dan diubah menjadi data. Kemudian data-data tersebut dijadikan satu menjadi *Big Data*. Istilah *big data* mengacu pada data yang sangat besar, cepat atau kompleks, sehingga sulit atau tidak mungkin untuk diproses menggunakan metode tradisional.[7] Berdasarkan riset, volume data yang dihasilkan di dunia berkembang pesat, dari 33 zettabytes pada tahun 2018 menjadi 175 zettabytes yang diharapkan terjadi pada tahun 2025. Data-data ini kemudian yang menjadi "bensin" bagi AI untuk bergerak dan berkembang, mengingat bahwa seluruh pemerosesan pembelajaran yang dilakukan oleh AI, berpusat kepada data, sehingga tanpa data, maka AI tentunya tidak akan bisa beroperasi, layaknya seperti mobil yang tidak bisa berjalan tanpa bensin.

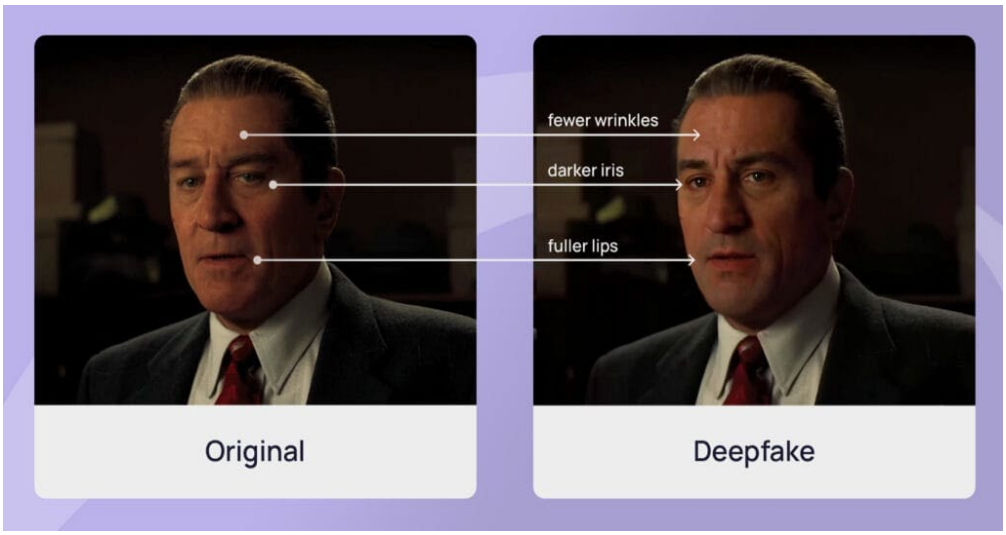
Sehingga dalam hal ini, diperlukan peran GDPR untuk menjadi filter dari data yang akan menjadi objek pemrosesan. GDPR berlaku untuk semua 27 negara anggota Uni Eropa (UE). Tidak hanya itu, namun ia juga berlaku untuk semua negara di *European Economic Area* (EEA, yang mencakup negara-negara seperti Islandia, Norwegia, dan Liechtenstein. Meskipun GDPR tidak secara langsung mengatur mengenai AI di dalamnya, namun tentu saja secara tidak langsung GDPR mengatur juga mengenai AI, karena AI harus menggunakan data untuk bisa tetap "hidup", sehingga jika bisa dikontrol pasokannya, maka kita akan bisa mengontrol cara AI berkembang. Hal ini juga sama dengan *deepfake*. Pembentukan *deepfake* biasanya melibatkan penggunaan data pribadi. Data pribadi ini merupakan data yang biasanya bisa dilacak kembali kepada suatu individu, atau di mana individu tersebut bisa diidentifikasi dari pengambilan data tersebut, seperti contohnya potongan-potongan suara yang dicuplik, foto ataupun video yang menggambarkan suatu individu. *Deepfake* yang menggambarkan subjek hukum perorangan atau *naturlijk persoon*, bisa dikategorikan sebagai data pribadi, karena hal tersebut berkorelasi dengan *identified or identifiable natural person*.[8]

---

6 Agus Budianto, "Legal Research Methodology Reposition in Research on Social," *International Journal of Criminology and Sociology* 9, (2020): 1339–1346, https://doi.org/10.6000/1929-4409.2020.09.154.

7 FL. Yudhi Priyo Amboro and Khusuf Komarhana, *Op. Cit.,* 147.

8 Article 4 section (1) *General Data Protection Regulation.*



Gambar 1. *De-aging Robert Deniro in The Irishman [Deepfake]*[9]
Sumber: Shamook, 2020.

Pada gambar yang di atas, dapat dilihat perbedaan antara gambar yang asli, dan gambar yang dibuat menggunakan *deepfake*. Hasil dari gambar tersebut sangatlah mirip, sehingga menjadi sulit untuk dibedakan. Namun tidak hanya itu, kian hari, *Deepfake* yang ada yang dibuat oleh AI semaking canggih, sehingga kedepannya akan semakin sulit dan bahkan hampir mustahil untuk bisa dibedakan yang mana yang asli dan yang mana yang palsu, sehingga perlunya ada regulasi yang mengatur terkait hal tersebut.[10]

Ada banyak cara *deepfake* dapat digunakan, mulai dari sindiran, seni, atau hiburan yang tidak berbahaya, hingga disinformasi, konten dewasa, skandal politik, berita palsu, dan bahkan perang modern. Membuat *deepfake* itu sendiri bukanlah tindakan ilegal. Namun, jika mereka melanggar hak pribadi subjek atau digunakan untuk keuntungan jahat atau kriminal, mempunyai akibat hukum tersendiri. Jika dilihat dari ketentuan dari GDPR mengenai *deepfake*, data pribadi hanya bisa diproses pada kondisi-kondisi tertentu saja, karena setiap individu mempunyai hak atas privasi dan perlindungan terhadap data pribadi mereka.

Harus digarisbawahi bahwa kata '*processing*' merupakan kata yang mempunyai arti secara luas, yang mencakup semua kemungkinan terkait penggunaan data pribadi dalam siklus hidup *deepfake*. Cakupan yang luas ini mempunyai relevansi terhadap implikasi untuk pengembang teknologi dan pencipta *deepfake* itu sendiri, karena data pribadi tidak hanya digunakan untuk membuat *deepfake* tertentu, namun juga melatih perangkat lunak yang digunakan untuk pembuatan *deepfake*, agar perangkat tersebut bisa semakin canggih. Akibatnya, pengoperasian layanan aplikasi yang memungkinkan untuk membuat video *deepfake*, membutuhkan *Data Protection Impact Assessment* (DPIA), dari pihak yang berwenang, di mana pengendali pribadi itu sendiri yang harus secara aktif mencari pihak yang berwenang, dan bersama-sama menggunakan evaluasi yang sistematis dan ekstensif untuk memastikan bahwa pemrosesan yang menggunakan teknologi baru tidak mempunyai risiko besar untuk melanggar hak dan kebebasan subjek hukum perorangan.[11] Dengan demikian, bisa dikatakan bahwa GDPR berlaku dan memberikan perlindungan

---

9 "How to Spot a Deepfake," Sosafe, last modified August 18, 2022, https://sosafe-awareness.com/blog/how-to-spot-a-deepfake.

10 Mika Westerlund, "The Emergence of Deepfake Technology: A Review," *Technology Innovation Management Review* 9, no. 11 (November 2019): 39–52, https://doi.org/10.22215/timreview/1282.

11 Article 35 *General Data Protection Regulation.*

yang substantif untuk pengembangan *software* dan aplikasi *deepfake*, serta untuk pembuatan dan penyebaran *deepfake* itu sendiri.[12]

GDPR memberikan landasan bahwa untuk memproses data pribadi, selalu membutuhkan dasar hukum sebelum melakukan pemrosesan tersebut. Dasar hukum yang ada di GDPR terdapat 6,[13] namun dalam korelasinya dengan *deepfake*, hanya '*informed consent*' dan '*legitimate interest*' yang mempunyai kualifikasi dalam konteks yang sama.[14] Ketika pencipta *deepfake*, atau *deepfake creator* melakukan klaim bahwa mereka mempunyai *legitimate interest* untuk melakukan pemrosesan terhadap data pribadi seseorang, *legitimate interest* tersebut yang dikejar oleh *deepfake creator* tidak boleh timpang tindih dengan kepentingan atau hak fundamental dan kebebasan dari orang yang ada di *deepfake* tersebut.[15] Misalnya, dengan penggambaran *deepfake*, *deepfake creator* dapat mengunggah video yang ironis menggambarkan suatu tokoh yang terkenal. Dalam kasus seperti itu, *deepfake creator* dapat mengklaim hak atas kebebasan berbicara untuk tujuan sindiran atau komentar politik.[16]

Namun jika *legitimate interest* ini tidak tercapai, dan tidak dapat diaplikasikan, maka penggunaan selanjutnya terhadap data pribadi untuk penggunaan dan penyebaran *deepfake* harus tunduk pada *informed consent* dari orang-orang yang digambarkan dalam video tersebut. Penting untuk digarisbawahi, bahwa *consent* harus diperoleh dari orang yang ada di video orisinalnya, dan orang yang akan muncul pada video yang sudah diedit oleh *deepfake*nya, karena data pribadi dari kedua orang tersebut akan diproses. Jika *deepfake creator* gagal untuk mendapatkan *consent* dari kedua belah pihak sebelum ia melakukan *deepfake*, maka mereka akan berisiko melanggar GDPR.

Sehingga, GDPR memberikan penanganan yang substansial terhadap *deepfake* konten yang tidak sesuai dengan regulasi, dan memberikan korban hak untuk membenarkan informasi data yang tidak benar, atau bahkan memintanya untuk menghapus video tersebut. Di setiap negara anggota, setidaknya ada satu otoritas pengawasan independen yang bertanggung jawab untuk memastikan serta menegakkan aturan dan peraturan yang ada. Namun, dalam konteks *deepfake* sendiri, secara implementasinya, jalur hukum bagi para korban bisa lebih menantang. Dalam banyak kasus, tidak mungkin bagi korban untuk bisa mengidentifikasi pelaku yang sering beroperasi secara anonim. Selain itu korban mungkin juga kekurangan sumber daya yang diperlukan untuk memulai prosedur peradilan, sehingga sering kali membuat mereka rentan terhadap *deepfake*.[17]

3.2 Kebijakan Hukum di Indonesia terkait *Deepfake*

Setelah sekian lama ditunggu-tunggu, Indonesia akhirnya mengeluarkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). UU PDP ini diambil dari GDPR, yakni salah satu regulasi yang paling komprehensif terkait perlindungan data pribadi. Dalam konteks *deepfake*, pengaturan yang diaturkan dalam UU PDP yang ada di Indonesia, sama halnya dengan yang ada di GDPR. UU PDP tidak mengatur secara langsung mengenai AI ataupun *deepfake* sebagai himpunan bagian dari AI. Namun karena AI menggunakan data, maka UU PDP secara tidak langsung juga

[12] European Parliament, *Tackling Deepfakes in European Policy* (LU: Publications Office, 2021), https://data.europa.eu/doi/10.2861/325063.
[13] Article 6 Section (1) *General Data Protection Regulation.*
[14] European Parliament, *Op.Cit.*
[15] Preamble 47 *General Data Protection Regulation.*
[16] European Parliament, *Op.Cit.,* 39.
[17] *Ibid.*, 39.

memberikan perlindungan hukum terhadap *deepfake* yang dilakukan secara ilegal terhadap pencipta yang mengambil data pribadi orang tanpa adanya persetujuan terlebih dahulu atau tanpa adanya.

Dalam hal ini secara umumnya data pribadi yang diambil oleh *deepfake creator* adalah data yang bersifat spesifik yakni data biometrik yang dimiliki oleh subjek data pribadi itu sendiri,[18] yang biasanya mencakup wajah dan suara yang ada pada seseorang, yang kemudian diambil dan dipasang ke gambar atau video lain untuk tujuan tertentu. Secara umum, sama seperti di GDPR, agar seseorang bisa terhindar dari adanya kemungkinan untuk melanggar undang-undang yang ada dalam hal ini adalah UU PDP, maka *deepfake creator* tersebut harus bisa memenuhi kriteria antara kepentingan yang sah dan/atau adanya persetujuan terlebih dahulu dari orang yang digambarkan pada *deepfake* tersebut.[19] Perlu diingat bahwa persetujuan yang sah ini harus secara eksplisit dari subjek data pribadi itu sendiri dan tidak boleh adanya unsur paksaan yang terjadi antara pengendali data pribadi dan subjek data pribadi itu sendiri, agar tidak ada terjadinya pelanggaran terhadap UU PDP.

Dalam UU PDP, pada Pasal 65 ayat (1) terdapat larangan yang mengatakan bahwa "Setiap Orang dilarang secara melawan hukum memperoleh atau mengumpulkan Data Pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian Subjek Data Pribadi." Sehingga, setiap orang yang ada, dilarang untuk melakukan pengumpulan data pribadi yang bukan miliknya yang dilakukan secara melawan hukum yang berarti ia tidak melakukan pengumpulan data tersebut secara legal, sehingga mengakibatkan kerugian terhadap subjek data pribadi itu sendiri. Hal tersebut dilarang oleh undang-undang, sehingga setiap orang yang melanggar hal tersebut, akan dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah).[20]

Selain UU PDP itu sendiri, di Indonesia Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE)[21] mengatur adanya pertanggungjawaban hukum yang bisa dikenakan juga terhadap penciptanya, yakni orang yang menggunakan *deepfake* itu sendiri sebagai *user*, yang menggunakan *deepfake* untuk tujuan tertentu.[22] Dalam hal ini, pencipta dilarang untuk mendistribusikan dan/atau mentransimisikan informasi elektronik dan/atau dokumen elektronik yang mempunyai muatan yang mengandung kesusilaan, perjudian, penghinaan dan/atau pencemaran nama baik, pemerasaan dan/atau pengancaman. Hal ini sesuai dengan perlindungan yang dicakup dalam aspek *deepfake*, karena mengingat bahwa rata-rata efek negatif yang ditimbulkan oleh *deepfake*, mengandung hal-hal terkait di atas, baik itu mencemarkan nama baik *artist*, *influencer* hingga politikus, ataupun muatan yang melanggar kesusilaan seperti memasukkan gambar seorang wanita dengan bintang film porno, dan mengubah wajahnya

---

18 Pasal 4 ayat (2) *Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.*

19 Pasal 20 ayat (2) huruf (a) dan (f) *Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.*

20 Pasal 67 ayat (1) *Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.*

21 *Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.*

22 Enni Soerjati Priowirjanto, "Urgensi Pengaturan Mengenai Artificial Intelligence Pada Sektor Bisnis Daring Dalam Masa Pandemi Covid-19 di Indonesia," *Jurnal Bina Mulia Hukum* 6, no. 2 (March 2022): 254–272, https://doi.org/10.23920/jbmh.v6i2.355.

menjadi gambar seorang wanita yang bahkan tidak pernah berbuat asusila, untuk mencemarkan nama baik, sehingga melanggar kesusilaan yang ada.[23]

Sehingga dengan adanya UU PDP dan UU ITE, dapat membantu untuk melindungi warga negara Indonesia terhadap kemungkinan buruk dari *deepfake* itu sendiri. Namun balik lagi seperti yang sudah dijelaskan bahwa terkadang sering kali pihak korban juga akan mengalami kesulitan, di mana secara implementasinya, jalur hukum bagi para korban bisa lebih menantang. Dalam banyak kasus, tidak mungkin bagi korban untuk bisa mengidentifikasi pelaku yang sering beroperasi secara anonim. Selain itu korban mungkin juga kekurangan sumber daya yang diperlukan untuk memulai prosedur peradilan, sehingga sering kali membuat mereka rentan terhadap *deepfake*.

3.3 Urgensi Untuk Melakukan Regulasi Terhadap AI

Artificial Intelligence telah memberikan manfaat sosial yang luas, mulai dari kemajuan medis hingga memitigasi perubahan iklim. Misalnya, teknologi AI yang dikembangkan oleh DeepMind, perusahan bisnis AI yang berada di Inggris, sekarang dapat memprediksi struktur terhadap hampir setiap protein yang diketahui oleh ilmu pengetahuan. Hal ini dapat mempercepat penelitian ilmiah hingga beberapa kali lipat dan dari hal tersebut, ilmuwan bisa melakukan pengembangan obat penyelamat jiwa, dan pengembangan tersebut telah membantu para ilmuwan membuat kemajuan besar dalam memerangi malaria, antibiotik, hingga limbah plastik.[24] AI juga dapat berkontribusi terhadap mitigasi perubahan iklim, misalnya melalui efisiensi energi atau dengan mengurangi emisi dari transportasi, pertanian, dan industri. AI dapat membantu kita beradaptasi dengan dampak perubahan iklim dengan meningkatkan kemampuan kita untuk memprediksi kejadian cuaca ekstrem dan menyediakan alat pendukung keputusan untuk membantu kita merespons dengan lebih efektif. AI juga dapat memainkan peran penting dalam meningkatkan ketahanan kita terhadap dampak perubahan iklim dengan membantu kita mengidentifikasi faktor risiko dan mengembangkan rencana untuk memitigasinya.[25]

Namun, meskipun AI seolah-olah dipuja-puja akan potensinya untuk membantu umat manusia, yang memang sudah mulai sangat terlihat akan hasilnya, bau akan kecemasan terhadap AI masih tercium hingga kini. Hal ini bisa terlihat dari beberapa aksi yang belakangan waktu ini dilakukan oleh CEO Tesla, Elon Musk, dan salah satu pendiri Apple Steve Wozniak yakni dengan melakukan penandatangan surat terbuka yang ditandatangani oleh lebih dari 2.600 pemimpin dan peneliti terdepan di industri teknologi. Surat terbuka tersebut menyerukan penghentian sementara pengembangan AI lebih lanjut. Petisi tersebut berisi berbagi keprihatinan bahwa AI dengan kecerdasan kompetitif manusia dapat menimbulkan bahaya serius bagi masyarakat dan umat manusia. Hal ini mendesak semua perusahaan AI untuk "segera menghentikan" pengembangan sistem AI yang lebih kuat daripada *Generative Pre-trained Transformer* 4 (GPT-4) setidaknya selama enam bulan. GPT-4 adalah model bahasa besar multimodal yang dibuat oleh OpenAI — yang keempat dalam seri GPT-nya.[26]

---

[23] Muhamad Ariq Aqbir and Akbar Kurnia Putra, "Aspek Hukum Internasional Dalam Pemanfaatan Deepfake Technology Terhadap Perlindungan Data Pribadi," *Uti Possidetis: Journal of International Law* 2, no. 1 (2021): 31–57, https://doi.org/10.22437/up.v2i1.11093.

[24] Alaá Rateb Mahmoud Al-shamasneh and Unaizah Hanum Binti Obaidellah, "Artificial Intelligence Techniques for Cancer Detection and Classification: Review Study," *European Scientific Journal* 13, no. 3 (January 2017), https://doi.org/10.19044/esj.2016.v13n3p342.

[25] Secretary of State for Science, Innovation and Technology, *A pro-innovation approach to AI regulation* (United Kingdom: HH Associates Ltd, 2023), 4.

[26] Prashant Jha, "Elon Musk-led Petition to Halt AI Development Divides Tech Community," *CoinTelegraph,* March 31, 2023, https://cointelegraph.com/news/elon-musk-led-petition-to-halt-ai-development-divides-tech-community.

Antonio Guterres, yakni *Secretary General of United Nations*, juga menyerukan bahwa AI mempunyai potensi yang sama atau bahkan lebih berbahaya daripada perang nuklir, sehingga ia menyerukan semua anggota PBB untuk segera membentuk *multilateral body* untuk membantu membentuk suatu regulasi terhadap perkembangan teknologi yang cepat ini. Komentar yang dilontarkan oleh Antonio Guterres ini muncul setelah ratusan ilmuwan AI terkemuka, termasuk eksekutif tingkat tinggi di Microsoft dan Google, mengatakan bahwa "memitigasi risiko kepunahan manusia terhadap AI harus menjadi prioritas global di samping risiko skala sosial lainnya".[27]

Pergerakan untuk memitigasi AI ini juga bisa terdeteksi dari langkah-langkah yang mulai diambil oleh negara-negara seperti Uni Eropa, di mana mereka mulai bergerak untuk membuat AI Act, yang bertujuan untuk melindungi masyarakat dari kemungkinan-kemungkinan pelanggaran yang dilakukan oleh AI, yang diharapkan, setidaknya adanya tercapai kesepakatan pada akhir tahun 2023 ini.[28] Hal ini juga terjadi di Amerika Serikat, di mana dimunculkannya *Executive Order* (EO) dari White House yang menyuarakan perlindungan terhadap warga negaranya dari potensi kerugian yang akan bisa ditimbulkan oleh AI, serta pembuatan kebijakan baru terhadap AI, sehingga Amerika Serikat bisa menjadi contoh yang terdepan terkait mitigasi dan pemanfaatan AI.[29]

Pengenalan teknologi AI mempunyai potensi untuk menciptakan risiko di kehidupan bermasyarakat. Meskipun teknologi AI bertujuan untuk menambah atau menggantikan pengambilan keputusan manusia, yang mengarah pada lebih sedikit keputusan yang salah, tidak ada keraguan bahwa terkadang AI masih salah. Dan cara AI melakukan kesalahan cenderung sangat berbeda dari cara manusia membuat kesalahan. Hal ini tentunya memiliki potensi yang berbahaya bagi masyarakat. Masyarakat tentunya ingin mengetahui risiko-risiko apa saja yang dipunyai dengan adanya implementasi AI dalam kehidupan bermasyarakat, dan argumen yang berisikan statistik murni yang mengatakan bahwa AI membuat kehidupan manusia lebih aman tidak akan cukup untuk meyakinkan populasi yang lebih luas, sehingga dibutuhkan nya suatu bukti yang konkret dan jelas. Oleh sebab itu, adanya suatu urgensi untuk membuat regulasi yang mengatur mengenai AI.

Regulasi yang baik ini akan meningkatkan persepsi masyarakat tentang keselamatan, dan juga persepsi bahwa manusia tetap memegang kendali. Dengan adanya regulasi, ia dapat mengurangi risiko baru apa pun yang diciptakan oleh penggunaan AI. Namun pada sisi lain, regulasi yang buruk bisa berisiko untuk menghambat pengembangan dan penerapan solusi AI yang bermanfaat, bahkan mungkin tanpa adanya hasil terhadap peningkatan keamanan dan kontrol yang direncanakan dengan dikeluarkannya oleh undang-undang baru. Oleh karena itu, tentunya terdapat urgensi untuk melakukan pembentukan regulasi yang mengatur tentang AI, namun pada saat yang bersamaan kita perlu memahami apa yang bisa dan tidak bisa dilakukan oleh regulasi sehingga kita bisa membentuknya dengan tepat. AI mempunyai kapabilitas *multi-faceted,* atau dalam artinya mempunyai banyak sekali kegunaan yang bisa digunakan oleh hampir seluruh bidang yang ada yang dikenal oleh manusia, sehingga satu regulasi saja yang berusaha untuk menampung ini semua atau istilahnya regulasi "*one size fits all*" akan memiliki efek negatif

---

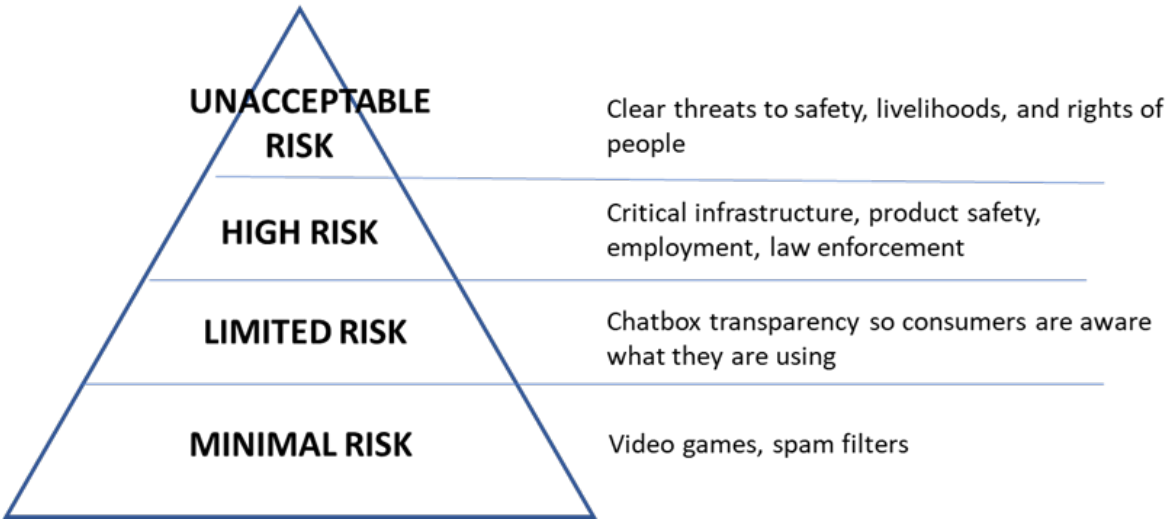
27 Adla Massoud, "UN Chief Warns AI Threat on Par with 'Nuclear War'," *The National News,* June 12, 2023, https://www.thenationalnews.com/world/2023/06/12/un-chief-warns-ai-threat-on-par-with-nuclear-war/.

28 "EU AI Act: First Regulation on Artificial Intelligence," European Parliament, last modified June 14, 2023, https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence.

29 "FACT SHEET: Biden-Harris Administration Announces New Actions to Promote Responsible AI Innovation that Protects Americans' Rights and Safety," The White House, last modified May 4, 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/04/fact-sheet-biden-harris-administration-announces-new-actions-to-promote-responsible-ai-innovation-that-protects-americans-rights-and-safety.

tersendiri. Regulasi yang ada akan mempunyai dua kemungkinan besar skenario yang bisa terjadi, yakni ia bisa *overregulate* atau *underregulate* dalam hal-hal tertentu.

Dalam hal ini, perencanaan *Regulatory Framework on AI* atau yang dikenal dengan *AI Act* yang sedang digarap oleh Uni Eropa, sejauh ini mempunyai potensi yang baik terhadap perlindungan serta perkembangan untuk AI yang dapat dicontoh oleh negara-negara lain, di mana *AI Act* ini mempunyai *multi-layered assessment* terhadap potensi dampak yang ditimbulkan oleh AI, dan setiap lapisan yang ada mempunyai keketatan peraturan terhadap AI. *AI Act* ini akan memiliki 4 lapisan terhadap risiko yang ditimbulkan oleh AI seperti gambar piramida yang ada di bawah ini:



Gambar 2. *Risk Based AI Regulatory Framework*
Sumber: Brookings.edu, 2023[30]

Pada gambar yang ada di atas dapat dilihat bahwa Uni Eropa membagi risiko yang ada menjadi empat, yakni *minimal risk, limited risk, high risk dan unacceptable risk*. *Minimal risk* mengacu kepada AI yang memiliki potensi berbahaya yang rendah dan hampir tidak ada terhadap pelanggaran fundamental hak asasi manusia, dan keamanan data *natural person* itu sendiri, di mana contoh dari AI ini adalah seperti AI yang ada di *video game*, ataupun *spam filter* yang ada. *Limited risk* mengacu kepada AI seperti *chatbot* yang digunakan oleh perusahaan-perusahaan untuk menangani *customer service* kepada para pelanggannya, di mana tipe dari AI ini biasanya digunakan untuk berinteraksi dengan *natural person*, dan juga biasanya digunakan untuk membuat atau memanipulasi gambar, audio, video untuk membuat *deepfake*, sehingga *deepfake* masuk dalam kategori *Limited risk* berdasarkan *AI Act* yang dikeluarkan oleh Uni Eropa.

High risk mengacu kepada penggunaan sistem AI yang mempunyai potensi dampak negatif terhadap hak fundamental manusia serta kesehatan dan keamanan dari subjek hukum perorangan itu sendiri. Dan yang terakhir adalah *Unnaceptable risk*, *AI Act* melarang sistem AI yang masuk dalam kategori ini untuk beroperasi, karena pada tingkat ini, sistem AI biasanya dianggap melanggar hak fundamental manusia serta regulasi yang ada dari

[30] Tom Wheeler, "The Three Challenges of AI," *Brookings*, June 15, 2023, https://www.brookings.edu/articles/the-three-challenges-of-ai-regulation.

Uni Eropa serta membahayakan keamanan dan keselamatan dari *natural person* itu sendiri.[31] Tentunya dengan adanya *Risk-based approach* ini, pengaturan terhadap AI bisa lebih fleksibel, sehingga regulasi yang ada tidak malah menghalangi inovasi, namun memberikan keseimbangan, antara perlindungan dan invosi agar bisa bergerak berbanding lurus, dan adanya pemerataan yang lebih tepat, di mana pada lapisan tertentu yang mempunyai potensi rendah terhadap pelanggaran keamanan *natural person* itu sendiri, sistem AI bisa diberikan ruang yang lebih besar dan pengaturan yang lebih tidak ketat dibandingkan AI yang ada pada lapisan yang lebih tinggi, sehingga harus diatur dengan lebih ketat.

Seperti contoh, penggunaan AI dalam *video game*, misalnya, tentunya memiliki efek yang berbeda — dan harus diperlakukan berbeda dengan AI yang dapat mengancam keamanan infrastruktur kritis atau membahayakan manusia.[32] Strategi yang lebih baik dalam melakukan regulasi terhadap AI adalah dengan mendekati masalah tersebut secara inkremental dan melakukan *risk-based approach* berdasarkan potensi bahaya yang dimiliki oleh AI sesuai dengan draft *AI Act*, sehingga regulasi yang ada tidak mencekik sektor-sektor lain dalam AI yang memerlukan pengaturan yang lebih rendah dibandingkan sektor AI yang mempunyai potensi lebih berisiko seperti yang sudah dijelaskan di atas.

Beberapa risiko yang sudah muncul atau yang sudah ada yang disebabkan oleh teknologi AI, seperti *Deepfake*, bisa langsung ditindak dengan regulasi yang sudah ada, seperti GDPR contohnya, dan mengambil langkah yang tepat untuk menanganinya; dampak dari AI sisanya akan muncul sendiri seiring dengan berjalannya waktu dan seiring dengan perkembangan teknologi serta pemakaian teknologi AI yang meningkat di kehidupan masyarakat. Pada titik tertentu, akan menjadi jelas apakah peraturan khusus diperlukan, dan jika ruang lingkup dan fokus peraturan tersebut akan memungkinkan untuk dibuat. Namun, selain AI sendiri, penting juga untuk diingat bahwa mereka yang memproduksi dan menggunakan teknologi AI juga benar-benar dapat mematuhi regulasi, dan regulasi tersebut tidak menghambat kemajuan teknologi yang bermanfaat. Di luar regulasi yang biasanya diatur secara khusus, hukum dan peraturan biasanya harus mengizinkan adanya inovasi secara bebas, tetapi pada saat yang bersamaan mereka yang bertanggung jawab harus menanggung akibatnya jika inovasi tersebut menyebabkan beberapa jenis kerugian.[33]

4. KESIMPULAN

Sudah tidak diragukan lagi bahwa perkembangan dan kemajuan AI di dalam era globalisasi ini sangatlah cepat dan masif. Setiap saat muncul teknologi-teknologi serta aplikasi-aplikasi *based AI* yang bermunculan yang kian hari kian pintar, yang membantu manusia untuk bisa menjalani kehidupan mereka dengan lebih gampang dengan efesien. Namun dengan perkembangan yang positif ini, tentunya juga memunculkan isu hukum pada aspek AI, di mana salah satu isu hukum ini adalah munculnya teknologi *deepfake*. *Deepfake* ini dipakai untuk mengimpersonasi seseorang baik itu wajah, suara, atau tubuh yang bahkan bukan milik orang itu sendiri, sehingga seringkali *deepfake* ini bisa digunakan

---

[31] "The EU AI Act's Risk-Based Approach: High-Risk Systems and What They Mean for Users," European Commission, last modified January 16, 2023, 13, https://futurium.ec.europa.eu/en/european-ai-alliance/document/eu-ai-acts-risk-based-approach-high-risk-systems-and-what-they-mean-users.

[32] Tom Wheeler, "The Three Challenges of AI," *Brookings*, June 15, 2023, https://www.brookings.edu/articles/the-three-challenges-of-ai-regulation.

[33] Chris Reed, "How Should We Regulate Artificial Intelligence?" *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 376, no. 2128 (September 2018), https://doi.org/10.1098/rsta.2017.0360.

untuk melakukan disinformasi dan penipuan, seperti mengimpersonasi suara seseorang untuk mengambil uang orang tersebut di ATM, sehingga menimbulkan kerugian secara individual, dan bahkan mengancam institusi-institusi besar sehingga mereka harus lebih berhati-hati untuk memberikan seseorang izin untuk bisa menarik uang mereka hanya melalui telepon dan email saja. Oleh karena itu dibutuhkannya perlindungan dan kepastian hukum yang ada yang mengatur terkait *deepfake* ini, di mana di Eropa sendiri, terdapat GDPR, dan di Indonesia sendiri terdapat UU PDP. Meskipun kedua UU ini tidak mengatur secara khusus terkait *deepfake*, namun mereka tetap melindungi subjek data dari tindakan *deepfake* karena secara umum data merupakan 'bahan bakar' AI, sehingga tanpa adanya data, maka AI tidak akan bisa untuk melakukan hal-hal yang biasanya ia lakukan. Sehingga jika regulasi bisa mengontrol bagaimana data tersebut keluar-masuk, maka perlindungan hukum yang diberikan kepada subjek hukum dari AI masih bisa dilakukan. Dalam UU PDP, telah dinyatakan dengan tegas pada Pasal 65 ayat (1) terdapat larangan secara melawan hukum memperoleh atau mengumpulkan Data Pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian Subjek Data Pribadi. Namun tentunya hal ini tidaklah cukup, sehingga adanya urgensi untuk membuat regulasi yang lebih tajam serta spesifik yang mengatur mengenai AI, seperti adanya *AI Act* di Uni Eropa yang memberikan *risk-based approach* terhadap pendekatan mereka untuk mengatur AI yang bisa dicontoh oleh Indonesia, sehingga memastikan adanya *equilibrium* antara pengaturan dan perkembangan, di mana pengaturan yang ada tidak boleh mengekang berlebihan sehingga menghambat perkembangan, namun pada saat yang bersamaan memastikan bahwa regulasi tersebut cukup untuk melindungi subjek hukum yang ada negara tersebut.

REFERENSI

Artikel Jurnal:

Al-shamasneh, Alaá Rateb Mahmoud, and Unaizah Hanum Binti Obaidellah. "Artificial Intelligence Techniques for Cancer Detection and Classification: Review Study." *European Scientific Journal* 13, no. 3 (January 2017): 342–370. https://doi.org/10.19044/esj.2016.v13n3p342.

Amboro, FL. Yudhi Priyo, and Khusuf Komarhana. "Prospek Kecerdasan Buatan Sebagai Subjek Hukum Perdata Di Indonesia." *Law Review* 21, no. 2 (November 2021): 145–172. https://doi.org/10.19166/lr.v0i2.3513.

Aqbir, Muhamad Ariq, and Akbar Kurnia Putra. "Aspek Hukum Internasional Dalam Pemanfaatan Deepfake Technology Terhadap Perlindungan Data Pribadi." *Uti Possidetis: Journal of International Law* 2, no. 1 (2021): 31-57. https://doi.org/10.22437/up.v2i1.11093.

Borges, Luís, Bruno Martins, and Pável Calado. "Combining Similarity Features and Deep Representation Learning for Stance Detection in the Context of Checking Fake News." *Journal of Data and Information Quality* 11, no. 3 (September 2019): 1–26. https://doi.org/10.1145/3287763.

Budianto, Agus. "Legal Research Methodology Reposition in Research on Social." *International Journal of Criminology and Sociology* 9, (2020): 1339–1346. https://doi.org/10.6000/1929-4409.2020.09.154.

Chairani, Meirza Aulia, Angga Pramodya Pradhana, and Taufiq Yuli Purnama. "The Urgency Of Developing Law As A Legal Basis For The Implementation Of Artificial Intelligence In Indonesia." *Law and Justice* 7, no. 1 (2022): 35-45. https://journals2.ums.ac.id/index.php/laj/article/view/760.

Priowirjanto, Enni Soerjati. "Urgensi Pengaturan Mengenai Artificial Intelligence Pada Sektor Bisnis Daring Dalam Masa Pandemi Covid-19 di Indonesia." *Jurnal Bina Mulia Hukum* 6, no. 2 (March 2022): 254–272. https://doi.org/10.23920/jbmh.v6i2.355.

Reed, Chris. "How Should We Regulate Artificial Intelligence?" *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 376, no. 2128 (September 2018). https://doi.org/10.1098/rsta.2017.0360.

Westerlund, Mika. "The Emergence of Deepfake Technology: A Review." *Technology Innovation Management Review* 9, no. 11 (November 2019): 39–52. https://doi.org/10.22215/timreview/1282.

Buku:

Secretary of State for Science, Innovation and Technology. *A pro-innovation approach to AI regulation.* United Kingdom: HH Associates Ltd, 2023.

Lain-lain:

Edwards, Benj. "Among AI dangers, Deepfakes Worry Microsoft President Most." *Ars Technica*, May 26, 2023. https://arstechnica.com/information-technology/2023/05/microsoft-president-declares-deepfakes-biggest-ai-concern.

European Commission. "The EU AI Act's Risk-Based Approach: High-Risk Systems and What They Mean for Users." Last modified January 16, 2023. https://futurium.ec.europa.eu/en/european-ai-alliance/document/eu-ai-acts-risk-based-approach-high-risk-systems-and-what-they-mean-users.

European Parliament. "EU AI Act: First Regulation on Artificial Intelligence." Last modified June 14, 2023. https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence.

European Parliament. *Tackling Deepfakes in European Policy*. LU: Publications Office, 2021. https://data.europa.eu/doi/10.2861/325063.

General Data Protection Regulation.

International Covenant on Civil and Political Rights.

Jha, Prashant. "Elon Musk-led Petition to Halt AI Development Divides Tech Community." *CoinTelegraph*, March 31, 2023. https://cointelegraph.com/news/elon-musk-led-petition-to-halt-ai-development-divides-tech-community.

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

Sosafe. "How to Spot a Deepfake." Last modified August 18, 2022. https://sosafe-awareness.com/blog/how-to-spot-a-deepfake.

The White House. "FACT SHEET: Biden-Harris Administration Announces New Actions to Promote Responsible AI Innovation that Protects Americans' Rights and Safety." Last modified May 4, 2023. https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/04/fact-sheet-biden-harris-administration-announces-new-actions-to-promote-responsible-ai-innovation-that-protects-americans-rights-and-safety.

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Dan Transaksi Elektronik. Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843.

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251, Tambahan Lembaran Negara Republik Indonesia Nomor 5952.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196, Tambahan Lembaran Negara Republik Indonesia Nomor 6820.

Wheeler, Tom. "The Three Challenges of AI." *Brookings*, June 15, 2023. https://www.brookings.edu/articles/the-three-challenges-of-ai-regulation.

Yulika, Nila Chrisna. "Apa Itu Deepfake, Ancaman yang Membayangi Pemilu 2024." *Liputan6,* March 15, 2023. https://www.liputan6.com/news/read/5233665/apa-itu-deepfake-ancaman-yang-membayangi-pemilu-2024.