

Kebijakan Kriminal Dalam Penyalahgunaan Teknologi *Artificial Intelligent*

Sultan Satria Islami¹, Hervina Puspito Sari²

¹ Fakultas Hukum, Hukum, Universitas Pembangunan Nasional “Veteran” Jawa Timur,
20071010030@student.upnjatim.ac.id

² Fakultas Hukum, Hukum, Universitas Pembangunan Nasional “Veteran” Jawa Timur

ABSTRACT

Artificial Intelligence (AI) is the ability of technology that enables machines or computers to perform tasks that typically require human intelligence, such as learning, planning, adaptation, and decision making. Artificial Intelligence technology has the potential to make decisions like humans, but its negative impact can be highly dangerous. For example, deepfake technology is a type of technology that can manipulate images or videos of individuals to make it appear as if they are doing or saying things that are false or never actually happened in reality. This falls under the category of Artificial Intelligence misuse and can be considered a cybercrime. To address this issue, Indonesia needs to develop clear criminal policies. This study uses a normative juridical approach, employing statutory regulations and conceptual approaches. The results indicate that Indonesia does not yet have specific regulations governing the use of Artificial Intelligence, but existing laws such as the Electronic Information and Transactions Law, personal data protection, and pornography can be utilized to address the misuse of Artificial Intelligence technology. Criminal policies to address this issue can be carried out through penal efforts, such as drafting Artificial Intelligence laws and their enforcement regulations, and non-penal efforts, such as public education, enhancing Artificial Intelligence education in the curriculum, and improving cyber security.

Keywords	<i>Criminal Policy; Artificial intelligence; Technology</i>
Cite This Paper	Islami, S. S., & Sari, H. P. (2025). Kebijakan Kriminal Dalam Penyalahgunaan Teknologi Artificial Intelligent. Legal Spirit, 9(2).
Manuscript History: <u>Received:</u> May 2, 2024 <u>Accepted:</u> September 9, 2025 <u>Corresponding Author:</u> Sultan Satria Islami, 20071010245@student.upnjatim.ac.id	 Legal Spirit is Licensed under a Creative Commons Attribution-ShareAlike 4.0 International License Indexed:     Layout Version: V8.2024

PENDAHULUAN

Menurut pandangan Knight dan Rich, kecerdasan buatan adalah bagian dari ilmu komputer yang berfokus pada penciptaan komputer yang dapat berfungsi seperti manusia, bahkan melebihi kemampuan manusia dalam beberapa tugas.¹ Kecerdasan buatan merupakan langkah menuju pengembangan komputer, robot, atau aplikasi yang dapat beroperasi secara cerdas, mirip dengan manusia. Dengan penjelasan tersebut, dapat disimpulkan bahwa kecerdasan buatan mengacu pada pembuatan mesin pintar yang dapat

¹ Jamaaluddin dan Indah Sulistyowati, *Buku Ajar Kecerdasan Buatan*, Umsida Press, Sidoarjo, 2021, Hal. 4

berpikir, belajar, dan mengambil keputusan seperti manusia. Teknologi kecerdasan buatan telah diterapkan dalam berbagai sektor, termasuk kendaraan otonom, asisten virtual, deteksi penipuan, dan lain-lain.

Adanya teknologi *artificial intelligent* ini memberikan dampak positif terhadap pekerjaan manusia, diantaranya adalah *artificial intelligent* dapat meningkatkan efisiensi dan produktivitas suatu pekerjaan. *artificial intelligent* memiliki kemampuan untuk mengerjakan tugas – tugas yang bersifat repetitif sehingga mempermudah pekerjaan manusia dan meningkatkan efisiensi dan produktivitas. *artificial intelligent* juga bermanfaat untuk mengotomatisasi pekerjaan. Sebagai contohnya, *artificial intelligent* dapat melakukan proses *input* data, analisis data, dan layanan pelanggan secara otomatis sehingga hal tersebut dapat mempermudah pekerjaan manusia. Selain itu, *artificial intelligent* juga dapat bertindak sebagaimana perilaku manusia. *artificial intelligent* dapat mengoperasikan kendaraan dengan sendirinya seperti teknologi yang dimiliki Tesla. *artificial intelligent* juga dapat melakukan percakapan dengan manusia seperti yang dapat dilakukan pada aplikasi Chat GPT. *artificial intelligent* juga dapat menggantikan pekerjaan manusia, seperti halnya trobosan yang dilakukan oleh TV One. Pada tanggal 21 April 2023, TV One mempersembahkan tiga pembawa acara berbasis artificial intelligence.² Ketiga pembawa acara artificial intelligence ini dipergunakan untuk segmen berita yang singkat dan padat, seperti berita mendadak dan ringkasan berita.

Namun di samping dampak positif tersebut, *artificial intelligent* dapat menimbulkan dampak negatif yang dapat membahayakan. Salah satu contoh nyata dari bahaya *artificial intelligent* adalah diciptakannya teknologi *deepfake* menggunakan algoritma *artificial intelligent* tersebut.

Deepfake adalah proses yang melibatkan proses pertukaran wajah dari seseorang ke orang yang ditargetkan dalam video dan membuat ekspresi wajah serupa dengan orang yang ditargetkan dan bertindak seperti orang yang ditargetkan serta mengucapkan kata-kata yang sebenarnya diucapkan oleh orang lain.³ Dengan teknologi *deepfake*, gambar atau video seseorang dapat diubah sedemikian rupa sehingga terlihat seolah-olah orang tersebut sedang melakukan atau mengatakan hal-hal yang sebenarnya tidak pernah terjadi. Jika teknologi ini disalahgunakan oleh individu dengan niat jahat, teknologi ini bisa digunakan sebagai alat untuk merusak reputasi seseorang. Sudah terjadi banyak kasus di mana teknologi ini digunakan untuk menyebarkan informasi palsu yang dapat merusak reputasi seseorang. Contohnya, pada tahun 2018, terdapat sebuah video yang menampilkan Donald Trump yang disinyalir meminta Belgia untuk keluar dari perjanjian Paris Agreement.⁴ Namun, setelah penyelidikan, ternyata video tersebut dibuat dengan teknologi *deepfake* dan Trump tidak pernah mengeluarkan pernyataan tersebut. Contoh lain adalah kejadian baru-baru ini di mana muncul video yang menampilkan Presiden Ukraina Volodymyr Zelensky yang diduga menyatakan menyerah kepada Rusia, padahal video tersebut adalah hasil manipulasi dari teknologi *deepfake*.⁵ Selain itu, teknologi *deepfake* juga telah digunakan untuk membuat konten pornografi dengan mengganti wajah pemeran dengan wajah

² Restu Almalita, *Presenter artificial intelligent TV One, Pertama di Indonesia dan Berhasil Curi Perhatian Publik*, Kaltim Today, 2 Mei 2023, diakses pada 3 November 2023, <https://kaltimtoday.co/presenter-ai-tv-one-pertama-di-indonesia-dan-berhasil-curi-perhatian-publik>

³ Bahar Uddin Mahmud dan Afsana Sharmin, *Deep Insights of deepfake Technology: a Review*, Jurnal: Dujase, Vol. 5, Nomor 1 & 2, Bangladesh, 2020, Hal. 13

⁴ Hans Von Der Burchard, "Partai sosialis Belgia mengedarkan video Donald Trump yang 'palsu'", Politico, 21 Mei 2018, diakses pada 3 November 2023, <https://www.politico.eu/article/spa-donald-trump-belgium-paris-climate-agreement-belgian-socialist-party-circulates-deep-fake-trump-video/>

⁵ Tim CNN Indonesia, "Viral Video Deepfake Presiden Ukraina Zelensky Menyerah ke Rusia", CNN Indonesia, 17 Maret 2022, diakses pada 3 November 2023, <https://www.cnnindonesia.com/teknologi/20220317161051-192-772698/viral-video-deepfake-presiden-ukraina-zelensky-menyerah-ke-rusia>

selebriti, seperti yang terjadi dengan video porno yang menampilkan wajah yang mirip dengan Nagita Slavina.⁶

Dalam menghadapi fenomena ini, Indonesia mengatur mengenai penggunaan alat elektronik sebagai perangkat yang digunakan untuk mengakses teknologi *artificial intelligent* di dalam Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. Namun, peraturan tersebut belum mengatur penyalahgunaan *artificial intelligence* menggunakan agen elektronik dan bagaimana bentuk pertanggungjawabannya. Hal tersebut kemudian menjadi celah hukum di dalam Undang-Undang tersebut. Sehingga kemudian permasalahan tersebut menjadi fokus utama dalam penelitian yang penulis lakukan.

Berdasarkan latar belakang tersebut, terdapat 2 rumusan masalah yang penulis tetapkan, diantaranya bagaimana penyalahgunaan teknologi *artificial intelligent* dapat diklasifikasikan sebagai tindak pidana dan bagaimana kebijakan kriminal terhadap penyalahgunaan teknologi *artificial intelligent* di Indonesia. Tujuan dari penelitian ini adalah untuk mengetahui dan menganalisis klasifikasi penyalahgunaan *artificial intelligeng* dalam tindak pidana dan untuk mengetahui dan menganalisis kebijakan kriminal terhadap penyalahgunaan teknologi *artifiial intelligent* di Indonesia.

METODE

Penelitian ini adalah jenis penelitian hukum normatif yang memeriksa hukum sebagai norma atau aturan yang berlaku dalam masyarakat dan digunakan sebagai pedoman perilaku. Metode penelitian hukum normatif ini mencakup analisis terhadap aturan-aturan perundang-undangan, baik dari segi hirarki perundang-undangan (vertikal) maupun keselarasan antara berbagai peraturan perundang-undangan (horizontal).⁷

Pendekatan perundang-undangan (*statute approach*) dan pendekatan konseptual (*conceptual approach*) digunakan dalam penelitian ini. Pendekatan perundang-undangan dilakukan dengan mengkaji semua peraturan perundang-undangan yang terkait dengan isu hukum yang sedang dibahas.⁸ Sedangkan pendekatan konseptual digunakan ketika tidak ditemukan aturan hukum yang relevan, karena belum ada atau tidak ada aturan yang mencakup masalah yang sedang diteliti.⁹

HASIL DAN PEMBAHASAN

Klasifikasi Penyalahgunaan *Artificial Intelligent* dalam Tindak Pidana

Menurut Knight dan Rich, *artificial intelligence* (AI) adalah bagian dari ilmu komputer yang mempelajari cara membuat komputer dapat bertindak seperti manusia, bahkan dengan kualitas yang melebihi kemampuan manusia.¹⁰ Komputer dirancang untuk memiliki kecerdasan dan kinerja yang memungkinkan mereka mengeksekusi tugas-tugas yang serupa dengan manusia, dengan mencontoh beberapa fungsi otak manusia seperti pemahaman bahasa, pengetahuan, pemikiran, penalaran, pemecahan masalah, dan pengambilan keputusan.

⁶ Galuh Putri Riyanto dan Wahyunanda Kusuma Pertiwi, "Menilik Teknologi "Deepfake" di Balik Video Diduga Mirip Nagita Slavina", Kompas.com, 18 Januari 2022, diakses pada tanggal 25 Desember 2023,

<https://teknomorkompas.com/read/2022/01/18/15490077/menilik-teknologi-deepfake-di-balik-video-diduga-mirip-nagita-slavina?page=all>

⁷ *Ibid*, Hal. 30

⁸ *Ibid*, Hal. 56

⁹ Nur Solikin, *Pengantar Metodologi Penelitian Hukum*, Qiara Media, Pasuruan, 2021, Hal. 60

¹⁰ Jamaaluddin dan Indah Sulistyowati, *Loc.cit*.

Secara umum, ada empat kategori dalam menjelaskan *artificial intelligence*:

1. Sistem yang mampu berpikir seperti manusia;
2. Sistem yang mampu bertindak seperti manusia;
3. Sistem yang mampu berpikir secara rasional; dan
4. Sistem yang mampu bertindak secara rasional.

Artificial intelligence memungkinkan komputer untuk memperoleh pengetahuan melalui data yang diberikan oleh manusia melalui proses simulasi penalaran. Hal ini memungkinkan komputer untuk berpikir seperti manusia karena data yang diberikan oleh manusia dapat diolah oleh sistem *artificial intelligence*.

Di era modern ini, *artificial intelligence* telah menghasilkan teknologi canggih seperti *deepfake*. *Deepfake* adalah teknik yang menggunakan kecerdasan buatan untuk menyintesis citra manusia, di mana gambar atau video dapat disatukan dengan cara tertentu sehingga tampak nyata.¹¹ Teknologi ini sering digunakan untuk mengganti wajah dalam video dengan wajah lain dan membuat ekspresi serta ucapan yang serupa dengan orang yang ditargetkan.¹²

Selain *deepfake*, teknologi *artificial intelligence* juga menghasilkan teknologi lain seperti *Voice Changer* yang dapat mengubah suara seseorang menjadi suara lain dengan teknik tertentu.¹³ Asisten virtual juga merupakan contoh teknologi *artificial intelligence* yang memungkinkan interaksi manusia dengan mesin melalui bahasa alami.¹⁴

Meskipun *artificial intelligence* memberikan dampak positif seperti meningkatkan efisiensi pekerjaan dan otomatisasi, namun juga dapat menimbulkan dampak negatif. Salah satu contohnya adalah *deepfake* yang dapat digunakan untuk menyebarkan informasi palsu dan merusak reputasi seseorang. Teknologi ini juga telah digunakan untuk konten pornografi dan manipulasi informasi lainnya yang dapat membahayakan individu.

Unsur-unsur tindak pidana dapat dibedakan menjadi unsur objektif dan unsur subjektif.¹⁵ Unsur objektif dalam tindak pidana mencakup perbuatan orang, akibat yang terlihat dari perbuatan tersebut, dan mungkin keadaan tertentu yang terjadi bersamaan dengan perbuatan, seperti yang diatur dalam Pasal 181 KUHP terkait dengan keadaan di muka umum. Sementara itu, unsur subjektif dalam tindak pidana melibatkan orang yang memiliki kemampuan untuk bertanggung jawab dan adanya kesalahan (*dolus* atau *culpa*).

Menurut Moeljatno, unsur-unsur tindak pidana terdiri dari perbuatan (kelakuan dan akibat), hal-hal atau keadaan yang terjadi bersamaan dengan perbuatan, keadaan tambahan yang dapat memberatkan pidana, unsur melawan hukum yang bersifat objektif, dan unsur melawan hukum yang bersifat subjektif.¹⁶

Tindakan penyalahgunaan *artificial intelligent* telah memenuhi unsur-unsur tindak pidana sebagaimana yang telah diuraikan oleh D. Simons diantaranya:

- a. Suatu perbuatan manusia, meskipun manipulasi informasi elektronik tersebut dilakukan oleh otomatisasi sistem menggunakan algoritma *artificial intelligent*, perbuatan tersebut tetap didasari oleh perintah yang diberikan oleh manusia sehingga manipulasi informasi elektronik menggunakan algoritma *artificial intelligent* telah memenuhi unsur perbuatan manusia;

¹¹ Heny Novyanti dan Pudji Astuti, *Loc.cit*

¹² Bahar Uddin Mahmud dan Afsana Sharmin, *Loc.cit*

¹³ Bambang Sugiantoro, *Loc.cit*

¹⁴ Rangga Putera Perdana, Irwansyah. *Loc.cit*

¹⁵ *Ibid.*

¹⁶ *Ibid.*

- b. Perbuatan yang dilarang dan diancam oleh Undang-Undang, manipulasi informasi elektronik yang ditujukan untuk pencemaran nama baik atau untuk menciptakan konten pornografi dapat diancam dengan berbagai pasal diantaranya Pasal 27 ayat (3) Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik yang mengatur tentang pencemaran nama baik, Pasal 27 ayat (1) Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik yang mengatur tentang pendistribusian sisten informasi elektronik yang memiliki muatan yang melanggar kesusilaan, Pasal 66 Undang-Undang nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi yang mengatur tentang pemalsuan data pribadi yang dapat mengakibatkan kerugian bagi orang lain, dan pasal 4 ayat (1) Undang-Undang Nomor 44 Tahun 2008 tentang Pornografi yang mengatur tentang produksi pornografi. Berikut beberapa Undang-Undang yang dapat digunakan untuk menjerat pelaku penyalahgunaan *artificial intelligent* dengan tujuan pencemaran nama baik atau konten pornografi. Dengan demikian penyalahgunaan *artificial intelligent* telah memenuhi unsur perbuatan yang dilaran dan diancam oleh Undang-Undang;
- c. Perbuatan dilakukan oleh orang yang dapat bertanggungjawab, penyalahgunaan *artificial intelligent* apabila dilakukan oleh yang dapat bertanggungjawab maka kemudian dapat diartikan telah memenuhi unsur tindak pidana tersebut.

Maka dengan demikian, penyalahgunaan *artificial intelligent* dapat digolongkan sebagai tindak pidana sebagaimana telah memenuhi unsur-unsur tindak pidana seperti yang telah diuraikan di atas.

Salah satu jenis dari tindak pidana adalah tindak pidana siber. Secara umum, tindak pidana siber atau *cybercrime* merujuk pada kegiatan kriminal yang terkait dengan dunia maya (*cyberspace*) dan komputer, yang didasarkan pada kemajuan teknologi internet sebagai media utama untuk melancarkan kejahatan.¹⁷ Istilah "*cyber crime*" dapat diklasifikasikan ke dalam dua kategori. Secara spesifik, istilah tersebut mengacu pada "*computer crime*." Secara lebih umum, istilah ini mencakup "*computer-related crime*". Pejelasan lengkapnya sebagai berikut:

"Cyber crime in a narrow sense (computer crime): any legal behaviour directed by means of electronic operations that targets the security of computer system and the data processed byh them. Cyber crime in a broader sense (computer related crime): any illegal behaviour committed by means on in relation to, a computer system or network, including such crime as illegal possess Pion, offering or distributing information by means of a computer system or network."

Berdasarkan penjelasan tersebut dapat dipahami bahwa Secara spesifik, kejahatan dunia maya adalah segala tindakan yang menggunakan teknologi elektronik untuk menyerang keamanan sistem komputer dan data yang terhubung. Sementara itu, kejahatan siber dalam ruang lingkup yang lebih luas mencakup perilaku ilegal yang terkait dengan sistem atau jaringan komputer, termasuk kegiatan seperti memiliki, menyediakan, atau menyebarkan informasi secara ilegal melalui sistem atau jaringan tersebut.

Tindak pidana siber terbagi menjadi beberapa bentuk, antara lain:¹⁸

1. Akses Tanpa Izin terjadi ketika individu masuk atau meretas sistem jaringan komputer tanpa izin atau pengetahuan dari pemiliknya.
2. Konten Ilegal melibatkan konten yang tidak benar, tidak etis, atau melanggar hukum, seperti penyebaran materi pornografi.
3. Penyebaran virus secara sengaja, sering kali melalui email, tanpa sepengetahuan dari pemilik sistem email.

¹⁷ Sahat Maruli T. Situmeang, *Loc.cit*

¹⁸ *Ibid.* Hal.9

4. Pemalsuan Data adalah usaha untuk memalsukan data pada dokumen-dokumen penting di internet, yang biasanya dimiliki oleh institusi atau lembaga dengan situs web *database*.
5. Mata-mata Siber, Sabotase, dan Pemerasan melalui jaringan internet terhadap pihak lain.
6. Penyiksaan Siber adalah tindakan mengganggu atau melecehkan seseorang melalui komputer, seperti email, secara berulang-ulang.
7. Pencurian Nomor Kartu Kredit untuk digunakan dalam transaksi online.
8. Peretasan dan Pemecahan Kode, di mana peretas adalah individu yang mempelajari sistem komputer secara mendalam dan meningkatkan kapabilitasnya, sementara pemecah kode adalah peretas yang menggunakan kemampuannya untuk kegiatan yang merugikan, seperti merusak data atau sistem.
9. Mendaftarkan Domain Nama Lain dan Membuat Domain Mirip adalah tindakan mendaftar domain nama orang lain dan menjualnya dengan harga tinggi atau membuat domain yang mirip dengan domain orang lain untuk keuntungan pribadi.
10. Pembajakan Karya Lain, sering kali terjadi dalam bentuk pembajakan perangkat lunak.
11. Terorisme Siber, yang merupakan bagian dari kejahatan siber jika bertujuan mengancam pemerintah atau warganegara dengan cara seperti meretas situs-situs pemerintah atau militer.

Karakteristik tindak pidana siber adalah sebagai berikut:¹⁹

1. Ruang lingkup kejahatan *cybercrime* mencakup dimensi global karena karakteristik internet yang bersifat global. Tindak kejahatan ini seringkali melintasi batas negara, menyulitkan penetapan yurisdiksi hukum yang berlaku.
2. Sifat kejahatan di dunia maya bersifat *non-violent*, tidak menciptakan kekacauan fisik yang mencolok. Berbeda dengan kejahatan konvensional yang seringkali menimbulkan kerusakan langsung, kejahatan di internet cenderung tidak terlihat secara langsung. Namun, kerusakan yang dihasilkan dari kejahatan *cyber* bisa jauh lebih luas dan serius dibandingkan dengan kejahatan fisik.
3. Pelaku kejahatan *cybercrime* memiliki sifat universal dan tidak terbatas pada stereotip tertentu seperti kejahatan konvensional. Mereka berasal dari berbagai latar belakang dan tidak terikat oleh batasan usia atau karakteristik khusus lainnya, namun memiliki pengetahuan yang mendalam tentang penggunaan internet dan aplikasinya.
4. Modus operandi kejahatan *cybercrime* melibatkan penggunaan teknologi informasi sebagai alat utama. Hal ini membuat modus operandi mereka sulit dipahami oleh orang-orang yang kurang familiar dengan dunia komputer, pemrograman, dan aspek teknis dunia *cyber*.
5. Jenis kerugian yang ditimbulkan oleh kejahatan *cybercrime* dapat bersifat material maupun non-material. Dampaknya dapat meluas ke berbagai sektor seperti politik, ekonomi, dan sosial budaya dengan intensitas yang lebih besar dibandingkan dengan kejahatan konvensional yang bersifat fisik.

Berdasarkan penjelasan tersebut, analisis tindakan penyalahgunaan *artificial intelligent* terhadap karakteristik tindak pidana siber adalah sebagai berikut:

- a. Ruang lingkup kejahatan, tindak pidana siber memiliki ruang lingkup kejahatan yang bersifat global. Hal ini karena tindak pidana siber dilakukan menggunakan media internet yang terhubung diseluruh negara. Pelaku penyalahgunaan *artificial intelligent* juga menggunakan media internet dalam melancarkan aksinya. Oleh karenanya, tindakan ini dapat memenuhi karakteristik tindak pidana siber yang pertama;

¹⁹ *Ibid*, Hal. 24

- b. Sifat kejahatan, tindak pidana siber tidak menimbulkan kekacauan yang mudah terlihat. Ketakutan atas tindakan ini tidak mudah timbul meskipun akibatnya dapat lebih dahsyat dari pada kejahatan lain. Masyarakat cenderung tidak memiliki ketakutan yang luar biasa terhadap penyalahgunaan *artificial intelligent* ini karena potensi berbahaya dari penyalahgunaan *artificial intelligent* masih jarang terlihat walaupun memiliki potensi yang sangat berbahaya di kemudian hari;
- c. Pelaku kejahatan, pelaku kejahatan siber adalah orang-orang yang menguasai teknologi komputer, internet beserta aplikasinya. Pelaku penyalahgunaan *artificial intelligent* adalah orang-orang yang menguasai teknologi-teknologi sebagaimana pelaku kejahatan tindak pidana siber tersebut;
- d. Modus kejahatan, modus kejahatan pelaku tindak pidana siber menggunakan teknologi informasi sebagai media tindak pidananya. Hal ini sama dengan pelaku penyalahgunaan *artificial intelligent* yang menggunakan teknologi informasi sebagai media tindak pidananya;
- e. Jenis kerugian, jenis kerugian dari tindak pidana siber dapat bersifat material maupun non material. Tindak pidana siber berpotensi menimbulkan kerugian pada bidang politik, ekonomi, sosial dan budaya. Hal ini juga berlaku pada pelaku penyalahgunaan *artificial intelligent*. Kerugian yang dapat dialami dari penyalahgunaan *artificial intelligent* juga dapat bersifat material maupun non material.

Berdasarkan uraian tersebut, dapat dipahami bahwa penyalahgunaan *artificial intelligent* merupakan tindak pidana berupa tindak pidana siber. Hal ini karena penyalahgunaan *artificial intelligent* telah memenuhi karakteristik tindak pidana siber. Penyalahgunaan *artificial intelligent* dapat memenuhi seluruh 11 jenis tindak pidana siber apabila tindak pidana siber tersebut dilakukan menggunakan *artificial intelligent*.

Sebagaimana penjelasan sebelumnya bahwa penyalahgunaan *artificial intelligent* dapat digolongkan sebagai tindak pidana siber. Uraian dalam sub bab ini akan menjelaskan mengenai tindakan penyalahgunaan *artificial intelligent* sebagai tindak pidana kecerdasan buatan atau *artificial intelligent crime (AIC)*.

"AI Crimes comprise every form of illegal or harmful act to a digital structure committed using a computer or digital device.²⁰ Artificial intelligence crime is a criminal act designed primarily to harm the interests of others through various electronic means. Artificial intelligence crimes may be either crimes against national security, against persons, or against funds. an AI system maybe be considered the subject of a crime, in which case the crime is assault on the computer's physical components and hardware.

AIC may involve an assault on the moral or logical components of the information system (software): Such a case occurs when the intangible components of the information system are targeted by the criminal.²¹ In this case, the cybercriminal may assault electronic data and software stored in the computer's memory by deleting, altering, or counterfeiting the software, or other legally prohibited acts. This shows that AI crimes differ from others regarding how they are committed. These crimes are less disturbing in nature because they are not based on violence, but rather on the criminal's ability to handle a computer with the technical skills needed to commit the crime in question. Unlike artificial intelligence crimes, the conventional ones require muscular exertion of diverse forms"

Berdasarkan pernyataan tersebut, dapat dipahami bahwa tindak pidana kecerdasan buatan merupakan segala tindakan ilegal atau melawan hukum yang membahayakan kepentingan publik yang dilakukan menggunakan sistem komputer. Tindak pidana

²⁰ Ibrahim Suleiman Al Qatawneh. *Artificial Intelligence Crimes. Academic Journal of Interdisciplinary Studies*. Vol. 12 Nomor 1. London. 2023. Hal. 144

²¹ *Ibid.*

kecerdasan buatan merupakan tindak pidana yang didesain untuk merugikan kepentingan orang lain menggunakan sistem komputer.

Tindak pidana kecerdasan buatan dapat berupa tindakan yang mengancam keamanan negara, orang, atau terhadap benda. Tindak pidana kecerdasan buatan ini memiliki cara yang berbeda dari tindak pidana lainnya. Sifat dari tindak pidana kecerdasan buatan ini tidak dapat dirasakan langsung secara fisik karena lingkup dari tindak pidana kecerdasan buatan ini adalah dunia maya. Meskipun demikian, tindak pidana kecerdasan buatan memiliki akibat yang lebih buruk dari tindak pidana siber. Hal ini karena pada tindak pidana kecerdasan buatan, sebagian besar tindakan dilakukan oleh kecerdasan buatan yang mampu menyamai kemampuan manusia.

Salah satu contoh bahaya tindak pidana kecerdasan buatan adalah penggunaan *artificial intelligent* dalam melakukan serangan *malware*. *Malware* atau Perangkat Lunak Berbahaya adalah *software* yang secara khusus dirancang untuk melakukan aktivitas berbahaya atau merusak perangkat lunak lainnya.²² Secara garis besar, *malware* terangkum dalam 4 macam tindak pidana siber, diantaranya: Penolak Akses; Pemerasan; Spionase; dan Pencurian Informasi. Adanya teknologi *artificial intelligent* mengakibatkan tindakan *malware* secara otomatis yang lebih berbahaya. Kombinasi antara *artificial intelligent* dengan *malware* dapat menciptakan modus operandi baru diantaranya:²³

- a) Mengembangkan jenis *malware* yang tidak terdeteksi melalui penggunaan algoritma dan pembelajaran mesin untuk menciptakan teknik yang dapat diperbarui dan ditingkatkan secara terus-menerus dalam memahami jenis *malware* dengan kemungkinan deteksi yang rendah, lalu melancarkan serangan dengan ciri-ciri yang serupa.
- b) Menyamarkan *malware* dari jaringan dengan cara memantau perilaku jaringan target dan meniru pola yang serupa dengan jaringan yang sah.
- c) Gabungan berbagai teknik serangan untuk menemukan pilihan paling efektif dalam menghindari deteksi dan mengutamakan alternatif dari serangan yang kurang berhasil.
- d) Menyesuaikan ciri atau fokus *malware* sesuai dengan situasi lingkungan, sehingga penyerang yang menargetkan browser bisa menyusup tanpa perlu daftar lengkap browser, hanya dengan menggunakan informasi umum karena bantuan algoritma AI yang telah dipelajari.
- e) Menerapkan mekanisme penghancuran otomatis dalam *malware* jika perilaku mencurigakan terdeteksi, sebagai upaya menghindari deteksi.
- f) Mendeteksi situasi yang mencurigakan dan menghentikan aktivitas untuk menghindari deteksi, termasuk alat-alat yang dipakai oleh peneliti anti-*malware*.
- g) Meningkatkan kecepatan serangan yang penting dalam pencurian data, dengan algoritma yang dapat mengekstraksi data lebih cepat daripada manusia sehingga sulit dideteksi dan hampir tidak mungkin dicegah.
- h) Memfasilitasi perangkat lain untuk belajar bersama dan mengenali bentuk serangan yang paling efektif dalam satu jaringan botnet, di mana setiap bot digunakan untuk menguji teknik infiltrasi secara bersamaan dan memberikan laporan untuk mempelajari target dalam waktu singkat.

²² Donovan Typhano Rachmadie, Supanto. *Regulasi Penyimpangan Artificial Intelligent pada Tindak Pidana Malware berdasarkan Undang-Undang Republik Indonesia Nomor 19 Tahun 2016*. Recidive, Vol.9, Nomor 2, Surakarta, 2020, Hal. 130

²³ *Ibid.*

Kebijakan Kriminal Penyalahgunaan *Artificial Intelligent*

Negara Indonesia masih belum memiliki undang-undang yang secara khusus mengatur tentang *Artificial Intelligent*. Namun, Negara Indonesia memiliki beberapa peraturan perundang-undangan yang mengatur terkait penyalahgunaan *Artificial Intelligent*. Peraturan perundang-undangan yang dapat digunakan dalam kasus penyalahgunaan *Artificial Intelligent* menggunakan teknologi *Deepfake* adalah sebagai berikut:

- 1) Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik;
- 2) Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik;
- 3) Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik;
- 4) Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi;
- 5) Undang-Undang Nomor 44 Tahun 2008 tentang Pornografi.
- 6) Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana

Berdasarkan wawancara yang penulis lakukan dengan bapak Andry Indrady, A.Md.Im., M.P.A., Ph.D., Direktur Teknologi Informasi Direktorat Jenderal Administrasi Hukum Umum Kementerian Hukum dan HAM pada tanggal 20 November 2023, pelaku penyalahgunaan *artificial intelligent* menggunakan teknologi *deepfake* dapat dipidana menggunakan beberapa peraturan perundang-undangan.²⁴ Peraturan perundang – undangan tersebut antara lain pasal 27 Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik yang menyatakan “Setiap Orang dengan sengaja dan tanpa hak menyiarkan, mempertunjukkan, mendistribusikan, mentransmisikan, dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan untuk diketahui umum”.

Pelaku tersebut juga dapat dikenakan pasal 4 ayat 1 Undang-Undang Nomor 44 tahun 2008 tentang Pornografi yang menyatakan bahwa “Setiap orang dilarang memproduksi, membuat, memperbanyak, menggandakan, menyebarluaskan, menyiarkan, mengimpor, mengekspor, menawarkan, memperjualbelikan, menyewakan, atau menyediakan pornografi yang secara eksplisit memuat:

- a. persenggamaan, termasuk persenggamaan yang menyimpang;
- b. kekerasan seksual;
- c. masturbasi atau onani;
- d. ketelanjangan atau tampilan yang mengesankan ketelanjangan;
- e. alat kelamin; atau
- f. pornografi anak.”

Pelaku tersebut kemudian juga dapat dikenakan pasal 66 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi yang menyatakan “Setiap orang dilarang membuat Data Pribadi palsu atau memalsukan Data Pribadi dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian bagi orang lain”.

Kebijakan kriminal atau politik kriminal adalah upaya sistematis dan terorganisir dari suatu masyarakat untuk mengatasi tindak kejahatan.²⁵ Definisi ini berasal dari Marc Ancel yang menggambarkan pengendalian kejahatan secara rasional oleh masyarakat. G. Peter

²⁴ Wawancara, Direktur Teknologi Informasi, Kementerian Hukum dan HAM, Jakarta, 20 November 2023.

²⁵ John Kenedy, *Op.Cit.* Hal. 39

Hoefnagels juga menyatakan bahwa kebijakan kriminal adalah tindakan sistematis dari reaksi sosial terhadap kejahatan.²⁶

Upaya penanggulangan kejahatan secara garis besar dapat dibagi menjadi dua kebijakan kriminal, yakni upaya penal dan non penal.

Upaya penal ini bertujuan sebagai alat pengendalian sosial yang menggunakan aturan yang mengatur sanksi pidana untuk mengatasi kejahatan.²⁷ Pendekatan penal mengacu pada penggunaan hukum pidana dalam menanggapi kejahatan, di mana hukum pidana digunakan sebagai alat pengendalian sosial dengan mengenakan sanksi pidana sebagai upaya menekan kejahatan. Dengan demikian, diharapkan bahwa norma-norma dalam kebijakan sosial dapat ditegakkan dengan bantuan sanksi yang ada dalam hukum pidana. Oleh karena itu, beberapa upaya penal yang dapat dilakukan adalah sebagai berikut:

Pembuatan Undang-Undang Kecerdasan Buatan

Dasar hukum yang khusus mengatur tentang penggunaan *artificial intelligent* perlu untuk disusun sebagai hukum positif yang berlaku di Indonesia. Undang-Undang Kecerdasan Buatan perlu untuk disusun dimana dalam Undang-Undang ini nantinya perlu untuk mengatur tentang pengertian umum *artificial intelligent*, pelaku atau pengguna *artificial intelligent*, etika penggunaan *artificial intelligent*, pertanggungjawaban pidana pelaku pengguna *artificial intelligent*, perbuatan yang dilarang, sanksi pidana, dan lain sebagainya. Peraturan ini perlu disusun supaya dapat memberikan payung hukum yang jelas dan juga sebagai pedoman bagi masyarakat yang menggunakan teknologi *artificial intelligent* supaya teknologi ini nantinya tidak dipersalahgunakan.

Regulasi yang mengatur tentang penggunaan *artificial intelligent* ini perlu untuk disusun. Sebagaimana yang telah dilaksanakan oleh beberapa negara di dunia, diantaranya:²⁸

1) Uni Eropa

Pada juni 2023, pemerintah parlemen Eropa telah menyetujui Undang-Undang yang bernama "*E.U. artificial intelligent Act*". Undang-Undang ini disusun dengan tujuan untuk melindungi konsumen dari bahaya teknologi *artificial intelligent*.

2) Amerika Serikat

Pada Oktober 2022, Amerika serikat telah menetapkan aturan penggunaan *artificial intelligent* yang bernama "*Blueprint for a artificial intelligent Bill of Rights*". Aturan tersebut disusun dengan tujuan agar teknologi *artificial intelligent* tidak membawa dampak negatif untuk masyarakat. selain itu, pada Januari 2023, Badan Standar dan Teknologi Nasional telah membuat suatu panduan yang berjudul "*Artificial Intelligence Risk Management Framework*". Amerika juga telah merilis suatu rencana dasar terkait hak asasi *artificial intelligent* yang bernama "Rencana untuk Hak Asasi *artificial intelligent*".

3) Inggris

²⁶ *Ibid.*

²⁷ *Ibid.*

²⁸ Alfian Akbar Ghazali, "Peta Regulasi *artificial intelligent*: Bagaimana Negara-negara Mengatur Kecerdasan Buatan" Kompas.com, 7 Juni 2023, diakses pada tanggal 25 Maret 2024, <https://tekNomorkompas.com/read/2023/07/07/07000017/peta-regulasi-ai--bagaimana-negara-negara-mengatur-kecerdasan-buatan?page=all>

Pada maret 2023, pemerintah inggris telah merilis regulasi yang bernama “Regulasi *artificial intelligent*; Pendakatan yang Pro-Inovasi”. Regulasi ini disusun untuk mengevaluasi dampak regulasi ini terhadap penggunaan *artificial intelligent*.

4) Tiongkok

Pada April 2023, pemerintah Tiongkok telah mengeluarkan regulasi yang bernama “*Cyberspace Administration of China (CAC)*”. Regulasi ini mencakup pedoman untuk penelitian, pengembangan, dan penggunaan *artificial intelligent* di sektor publik dan swasta.

Itulah beberapa negara yang telah mengundang regulasi terkait penggunaan *artificial intelligent*. Selain negara-negara yang telah penulis jabarkan, masih terdapat beberapa negara lain yang telah membuat regulasi tentang penggunaan *artificial intelligent* seperti Selandia baru, Kanada, dan Jepang.

Berdasarkan fakta tersebut, dapat dipahami bahwa beberapa negara telah menyadari pentingnya regulasi yang mengatur penggunaan *artificial intelligent*. Maka sudah seharusnya Indonesia juga mengikuti jejak negara-negara tersebut.

Pembuatan Peraturan Pelaksana atas Undang-Undang Kecerdasan Buatan

Peraturan pelaksana dibutuhkan guna mengatur hal-hal yang sifatnya lebih teknis mengenai kebijakan penggunaan teknologi *artificial intelligent* yang diselaraskan dengan Undang-Undang Kecerdasan Buatan.

Upaya non penal lebih fokus pada tindakan preventif untuk mencegah terjadinya kejahatan, dengan menangani faktor-faktor yang dapat menyebabkan atau memperkuat kejahatan.²⁹ Ini mencakup kondisi sosial yang secara langsung atau tidak langsung berkontribusi pada kejahatan. Dalam menghadapi penyalahgunaan *artificial intelligence* melalui pendekatan non penal, fokus utamanya adalah pada langkah-langkah pencegahan untuk masyarakat agar tidak menyalahgunakan *artificial intelligence*.

Kebijakan kriminal non penal ini berusaha menangani faktor-faktor yang memicu kejahatan, sehingga beberapa upaya yang dapat dilakukan meliputi:

Sosialisasi kepada Masyarakat

Sosialisasi kepada masyarakat dilakukan dengan tujuan untuk memberikan pemahaman kepada masyarakat mengenai segala hal yang berhubungan dengan penggunaan teknologi *artificial intelligent*. Pada sosialisasi atau penyuluhan, hal yang ditekankan adalah upaya untuk memberikan tindakan preventif kepada masyarakat supaya tidak menggunakan teknologi *artificial intelligent* sebagai media melakukan tindak pidana. Hal ini perlu dilakukan karena tidak sedikit masyarakat yang belum mengetahui bahwa suatu tindakan kejahatan menggunakan teknologi *artificial intelligent* dapat digolongkan sebagai tindak pidana siber.

Menambahkan Edukasi Penggunaan Teknologi *Artificial Intelligent* pada Kurikulum Pendidikan di Indonesia

Kementerian Pendidikan Cina telah melaksanakan program kampanye *artificial intelligent* di sekolah-sekolah untuk meningkatkan pendidikan.³⁰ Kampanye ini bertujuan untuk mendorong adopsi pengajaran dan pembelajaran yang terintegrasi dengan kecerdasan buatan, meningkatkan literasi dan keterampilan dalam pendidikan digital, dan mengukuhkan standar etika ilmiah dalam penerapan kecerdasan buatan.

²⁹ *Ibid.*

³⁰ Nikita Rosa, “Cina Luncurkan Pendidikan AI bagi Siswa SD dan Sekolah Menengah, Seperti Apa?”, *detikedu*, 31 Maret 2024, diakses pada tanggal 4 April 2024, <https://www.detik.com/edu/detikpedia/d-7270644/cina-luncurkan-pendidikan-ai-bagi-siswa-sd-dan-sekolah-menengah-seperti-apa>

Langkah sebagaimana diterapkan di Negara Cina tersebut dapat menjadi referensi yang bagus untuk diterapkan di Indonesia. Edukasi mengenai penggunaan *artificial intelligent* tidak hanya perlu untuk diberikan kepada masyarakat, melainkan kepada generasi muda penerus bangsa. Penambahan pendidikan *artificial intelligent* pada kurikulum pendidikan di Indonesia patut untuk dilakukan. Nantinya dalam pembelajaran ini, pemerintah dapat memberikan pendidikan mengenai etika penggunaan *artificial intelligent*, peningkatan inovasi menggunakan *artificial intelligent*, dan masih banyak lainnya. Adanya pendidikan ini, tentunya menjadi suatu langkah preventif untuk mencegah terjadinya tindak pidana penyalahgunaan *artificial intelligent*.

Meningkatkan Sistem Cyber Security di Indonesia

Menurut Peraturan Menteri Pertahanan Republik Indonesia Nomor 82 Tahun 2014 tentang Pedoman Pertahanan Siber, "Keamanan Siber Nasional (*National cyber security*) adalah segala upaya dalam rangka menjaga kerahasiaan, keutuhan dan ketersediaan informasi serta seluruh sarana pendukungnya di tingkat nasional, yang bersifat lintas sektor." Pertahanan siber adalah upaya untuk melawan serangan siber yang dapat mengganggu operasi pertahanan negara. Sementara itu, keamanan siber mencakup berbagai langkah dan teknologi yang digunakan untuk melindungi lingkungan digital, organisasi, dan aset pengguna dari risiko keamanan yang terkait dengan kejahatan siber. Ini mencakup perlindungan terhadap perangkat komputasi yang terhubung, personel, infrastruktur, aplikasi, layanan, sistem telekomunikasi, dan seluruh informasi yang ditransmisikan atau disimpan dalam lingkungan digital. Upaya keamanan siber adalah usaha berkelanjutan untuk menjaga keamanan organisasi dan aset pengguna dari berbagai risiko keamanan yang ada di dunia siber, termasuk melindungi sistem jaringan dan data dari serangan kejahatan siber.³¹

Peningkatan keamanan siber perlu untuk dilakukan guna meningkatkan keamanan aset pengguna supaya tidak disalahgunakan oleh pelaku penyalahgunaan *artificial intelligent*. Peningkatan keamanan siber juga perlu untuk dilakukan agar pemerintah Indonesia mampu melakukan pemantauan terhadap penggunaan teknologi informasi agar tidak terjadi penyalahgunaan *artificial intelligent*. Pemerintah Indonesia melalui keamanan sibernya harus dapat melakukan langkah antisipasi yang dapat berupa pemblokiran informasi elektronik hasil dari penyalahgunaan *artificial intelligent* supaya tidak beredar di *cyber space* atau dunia maya.

PENUTUP

Teknologi *artificial intelligent* dapat menimbulkan dampak negatif apabila disalahgunakan. Salah satu contoh nyata dari bahaya penyalahgunaan *artificial intelligent* adalah kasus pencemaran nama baik dan produksi konten pornografi menggunakan teknologi *deepfake* yang merupakan salah satu produk dari *artificial intelligent*. Tindakan tersebut kemudian dapat digolongkan sebagai tindak pidana siber dengan jenis *illegal content*. Penyalahgunaan *artificial intelligent* haruslah dikenal sebagai tindak pidana kecerdasan buatan sebagai jenis baru dari tindak pidana siber. Hal ini karena tindak pidana kecerdasan buatan dapat melakukan jenis-jenis tindak pidana siber lainnya dengan menggunakan algoritma *artificial intelligent* yang dapat meniru tindakan manusia dan bahkan melampaui kemampuan manusia. Kebijakan kriminal terhadap penyalahgunaan *artificial intelligent* tersebut dapat dilakukan melalui upaya penal yakni menyusun Undang-Undang Kecerdasan Buatan dan menyusun peraturan pelaksana dari Undang-Undang Kecerdasan Buatan dan upaya non penal yakni melakukan sosialisasi terhadap Masyarakat mengenai bijak menggunakan teknologi *artificial intelligent*; menambahkan pendidikan

³¹ Ahmad Fauzi, dkk, *Introduction Cyber Security*, Elmarkazi, Bengkulu, 2022, Hal. 1

artificial intelligent pada kurikulum pendidikan di Indonesia; dan Meningkatkan *Cyber Security* di Indonesia

DAFTAR PUSTAKA

Buku

- Chandra, Tofik Yanuar. (2022). *Hukum Pidana*. Jakarta: PT Sangir Multi Usaha.
- Fauzi, Ahmad, dkk. (2022). *Introduction Cyber Security*. Bengkulu: El-Markazi
- Hanafi. (2022). *Dasar Cyber Security dan Forensic*. Sleman: CV Budi Utama
- Jamaaluddin dan Sulistyowati, Indah. (2021). *Buku Ajar Kecerdasan Buatan*. Sidoarjo: Umsida Press.
- Jaya, Hendra dkk. (2018). *Kecerdasan Buatan*. Makassar: Fakultas MIPA Universitas Negeri Makassar.
- Karim, Abdul dkk. (2020). *Pengantar Teknologi Informasi*. Sumatera Utara: Yayasan Labuhanbatu Berbagi Gemilang.
- Muhaimin. (2020). *Metode Penelitian Hukum*. Mataram: Mataram University Press.
- Puspitosari, Hervina. (2020). *Cybercrime In The Field Of Decency*. Surabaya: Nas Media Pustaka.
- Raharjo, Budi. (2023). *Teori Etika dalam Kecerdasan Buatan*. Semarang: Yayasan Prima Agus Teknik
- Situmaeng, Sahat Maruli T. (2020). *Cyber Law*. Bandung: CV Cakra.
- Solikin, Nur. (2019). *Masyarakat, dan Penegakan Hukum*. Pasuruan: Qiara Media.
- Solikin, Nur. (2021). *Pengantar Metodologi Penelitian Hukum*. Pasuruan: Qiara Media.
- Suyanto. (2018). *Pengantar Hukum Pidana*. Sleman: CV Budi Utama.

Artikel Jurnal

- Al Qatawneh, Ibrahim Suleiman. (2023). *Artificial Intelligence Crimes. Academic Journal of Interdisciplinary Studies*. 12(1): 143 - 150
- Ardiyanti, Handrini. (2014). *Cyber-Security Dan Tantangan Pengembangannya di Indonesia*. Jurnal Politicia. 5(1): 95 - 110
- Deyianto, Yudo dan Dwiasnati, Saruni. (2020). *Kerangka Kerja Sistem Kecerdasan Buatan dalam Meningkatkan Kompetensi Sumber Daya Manusia Indonesia*. Jurnal Telekomunikasi dan Komputer. 10(1): 19 - 24.
- Mahmud, Bahar Uddin dan Sharmin, Afsana. (2020). *Deep Insights of deepfake Teknologi: a Review*. Jurnal: Dujase. 5(1&2): 13 - 24
- Novyanti, Heny dan Astuti, Pudji. (2012) *Jerat Hukum Penyalahgunaan Aplikasi deepfake Ditinjau dari Hukum Pidana*. Novum: Jurnal Hukum. 1(1): 0-216

Perdana, Rangga Putera. (2019). *Implementasi Asisten Virtual Dalam Komunikasi Pelayanan Pelanggan (Studi Kasus Pada Layanan Pelanggan Telkomsel)*. Jurnal Komunikasi. 11(2): 183 – 196.

Rachmadie, Donovo Typhano, dan Supanto. (2020). *Regulasi Penyimpangan Artificial Intelligence pada Tindak Pidana Malware berdasarkan Undang-Undang Republik Indonesia Nomor 19 Tahun 2016*. Recidive. 9(2): 128 - 136

Sugiantoro, Bambang. (2018). *Analisis Rekaman Suara Voice Changer dan Rekaman Suara Asli Menggunakan Metode Audio Forensik*. Indonesia Journal on Networking and Security. 7(1): 1 – 6.

Peraturan Perundang-undangan

Undang-Undang Republik Indonesia 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 44 Tahun 2008 tentang Pornografi (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 181, Tambahan Lembaran Negara Republik Indonesia Nomor 4928)

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

Undang-Undang Republik Indonesia Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 1, Tambahan Lembaran Negara Republik Indonesia Nomor 6842)

Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem Dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185, Tambahan Lembaran Negara Republik Indonesia Nomor 6400)

Peraturan Menteri Pertahanan Nomor 82 Tahun 2014 tentang Pedoman Pertahanan Siber (Berita Negara Republik Indonesia Tahun 2014 Nomor 1712)

Website

Almalita, Restu. (2023). *Pertama di Indonesia dan Berhasil Curi Perhatian Publik*. Kaltim Today. <https://kaltimtoday.co/presenter-ai-tv-one-pertama-di-indonesia-dan-berhasil-curi-perhatian-publik> diakses pada 3 November 2023

Burchard, Hans Von Der. (2018). *Partartificial intelligent sosialis Belgia mengedarkan video Donald Trump yang 'palsu'*. Politicio. <https://www.politico.eu/article/spa-donald-trump-belgium-paris-climate-agreement-belgian-socialist-party-circulates-deep-fake-trump-video/> diakses pada 3 November 2023

Ghazali, Alfian Akbar. (2023). *Peta Regulasi artificial intelligent: Bagartificial intelligentmana Negara-negara Mengatur Kecerdasan Buatan*. Kompas.com.

<https://tekNomorkompas.com/read/2023/07/07/07000017/peta-regulasi-ai--bagaimana-negara-negara-mengatur-kecerdasan-buatan?page=all> diakses pada tanggal 25 Maret 2024

Riyanto, Galuh Putri dan Pertiwi, Wahyunanda Kusuma. (2022). *Menilik Teknologi "deepfake" di Balik Video Diduga Mirip Nagita Slavina*. Kompas.com. <https://tekNomorkompas.com/read/2022/01/18/15490077/menilik-teknologi-deepfake-di-balik-video-diduga-mirip-nagita-slavina?page=alla> diakses pada tanggal 25 Desember 2023

Rosa, Nikita. (2024). *"Cina Luncurkan Pendidikan AI bagi Siswa SD dan Sekolah Menengah, Seperti Apa?"*, detikedu, <https://www.detik.com/edu/detikpedia/d-7270644/cina-luncurkan-pendidikan-ai-bagi-siswa-sd-dan-sekolah-menengah-seperti-apa> diakses pada tanggal 4 April 2024

Tim CNN Indonesia. (2022). *Viral Video deepfake Presiden Ukrartificial intelligentna Zelensky Menyerah ke Rusia*. CNN Indonesia. <https://www.cnnindonesia.com/teknologi/20220317161051-192-772698/viral-video-deepfake-presiden-ukraina-zelensky-menyerah-ke-rusia> diakses pada 3 November 2023

Turton, Willian. (2024). *"Deepfake" videos like that Gal Gadot porn are only getting more convincing — and more dangerous*, Vice News. <https://www.vice.com/en/article/qvm97q/deepfake-videos-like-that-gal-gadot-porn-are-only-getting-more-convincing-and-more-dangerous> diakses pada 27 Maret 2024

Lain-Lain

Indrady, Andry. 2023. *"Dasar Hukum Penyalahgunaan Artificial Intteligent"*. Hasil Wawancara Pribadi. 20 November 2023. Kementerian Hukum dan HAM

