201910110311210
Ryaas Rais Hasby Maukar
Prodi Hukum

BAB II

TINJUAUAN PUSTAKA

2.1 Tinjauan Umum tentang Deep Fake

Salah satu perkembangan teknologi di era Revolusi Industri 4.0 adalah Artificial Intelligence (AI). AI adalah sebuat disiplin ilmu yang mengembangkan intelegensia pada sistem komputer.[14] AI merujuk pada kemampuan mesin atau komputer untuk meniru kecerdasan manusia. Sistem AI dirancang untuk dapat melakukan tugas-tugas yang biasanya memerlukan kecerdasan manusia, seperti pemahaman bahasa, penalaran, pembelajaran, pengenalan pola, dan pengambilan keputusan.

Artificial intelligence (AI) adalah pengembangan dari sistem komputer yang bisa melakukan tugas yang biasanya dilakukan manusia. Beberapa istilah yang dikaitkan dengan kecerdasan buatan (AI), antara lain machine learning, deep learning, artificial neural network (ANN) atau jaringan syaraf tiruan, Natural Language Processing (NLP) atau pemrosesan bahasa alami, dan lain-lain. Kecerdasan Buatan (AI) telah memberikan dampak signifikan terhadap sejumlah industri, termasuk pengenalan suara dan wajah, kendaraan otonom, dan layanan kesehatan. Bahkan AI sudah digunakan dalam bisnis pribadi atau bisa dikatakan mencari peluang keuntungan pribadi.[15]

Salah satu contoh dari bentuk AI adalah aplikasi deepfake. Konsep dari deepfake adalah user interface sebuah hasil dari kecerdasan buatan deep fake yang membuat tampilan muka dengan sebuah gambar dan video digabungkan sehingga

[14] Thomas Dean, James Allen, and John Aloimonos, ob.cit., h. 2.
[15] Emi Sita Eriana and Afrizal Zein, ob.cit, h.1

tampak lebih nyata. Deepfake menggunakan algoritma machine learning yang terinspirasi pada struktur kerja otak manusia. Deepfake menggunakan dua data yang berasal dari data sumber (rekaman asli orang yang ingin dimanipulasi) dengan data target (rekaman wajah dan suara orang lain yang ingin dicantumkan). Kemudian, algoritma mempelajari karakteristik dari dua data tersebut. adanya fenomena deepfake inilah yang menjadi konsep penelitian, deepfake memiliki potensi merugikan bagi orang lain seperti penyebaran informasi hoax, pencemaran nama baik, merusak reputasi bagi seseorang yang tidak pernah melakukan hal tersebut, dan hilangnya kepercayaan publik pada media online.[16]

Deepfake adalah hasil dari kecerdasan buatan atau artificial intelligence (AI). Siapapun dapat mengakses aplikasi deepfake serta membuat video atau gambar editan sesuai dengan yang diinginkan. Tujuan awal dari penggunaan Deepfake yaitu untuk hiburan di TV maupun media sosial. Akan tetapi seiring berjalannya waktu, teknologi tersebut digunakan sebagai alat untuk menyesatkan orang dan menyebarkan informasi palsu.[17]

Kemampuan Deepfake untuk menghasilkan data yang nyata dan meyakinkan, membuatnya sebagai alat yang ideal untuk menciptakan deepfake. Cara kerja deepfake adalah memakai metode generative adversarial networks, GAN terdiri dari dua JST: generator dan diskriminator. Generator dilatih untuk membuat video baru, sedangkan diskriminator dilatih untuk membedakan antara video nyata dan video palsu. Proses ini berulang, dengan generator dan diskriminator saling

[16] Bramcov Stivens Situmeang, Inggrid Yolanda Silitonga, Reskina Felida Silaen, Tiurmaida Siringo-ringo, Ester Esari Sipayung, "Pengaruh Artificial Intelligence Terhadap Tingkat Kasus Deep Fake Pada Selebritas Di Twitter, Jurnal Device 1, Vol14, mei 2024, h.85
[17] Heny Novyanti, "Jerat Hukum Penyalahgunaan Aplikasi Deepfake Ditinjau Dari Hukum Pidana", ejournal.unesa,1, Vol 1, 2021, h.2

meningkatkan. Hasilnya adalah video yang sangat realistis yang hampir tidak dapat dibedakan dari video nyata.

Deep learning, sebagai komponen inti dari teknologi ini, merupakan metode pembelajaran mesin yang melibatkan jaringan saraf tiruan (neural networks), sebuah sistem komputer yang dirancang untuk meniru cara kerja otak manusia dalam memproses data.[18] Melalui algoritma ini, sistem dapat mengidentifikasi pola dalam data visual atau audio, belajar dari pola-pola tersebut, dan kemudian menggunakan informasi tersebut untuk menciptakan representasi baru yang sangat realistis. Hasil dari proses ini adalah konten yang secara visual atau auditori sangat mirip dengan yang asli, sehingga sulit bagi mata manusia atau pendengaran biasa untuk membedakan antara yang asli dan yang palsu.

Fenomena deep fake telah menimbulkan kekhawatiran yang mendalam di berbagai kalangan, mulai dari pemerintah, akademisi, hingga masyarakat umum. Teknologi ini memiliki potensi untuk digunakan dalam berbagai sektor, baik positif maupun negatif. Dalam dunia hiburan, deep fake dapat digunakan untuk menciptakan efek visual yang lebih realistis, seperti mereplikasi aktor dalam adegan tertentu atau menciptakan ulang sosok yang telah meninggal dunia. Namun, yang menjadi masalah adalah ketika teknologi ini digunakan untuk tujuan yang merugikan, seperti penyebaran berita palsu (fake news), penipuan, pornografi non-konsensual, pencemaran nama baik, dan bahkan manipulasi politik.

Dalam konteks media sosial, deep fake sering kali digunakan untuk menciptakan konten yang menipu, baik dengan mengubah wajah seseorang dalam

[18] Tribuana, D., Maramis, L., Resky, A. M., & Hidayat, R. (2025). *Deep Learning*. Serasi Media Teknologi.

video maupun meniru suara orang tertentu. Akibatnya, banyak orang yang mungkin menjadi korban manipulasi visual atau suara tanpa menyadarinya. Ini menjadi masalah serius di era informasi digital, di mana media sosial sering kali menjadi sumber utama penyebaran informasi. Penggunaan deep fake untuk menciptakan berita palsu atau informasi menyesatkan dapat berdampak pada stabilitas politik dan sosial suatu negara, karena mampu membingungkan masyarakat dan menyebarkan kebohongan dengan cepat dan luas.

Di sisi lain, dari sudut pandang hukum, deep fake memberikan tantangan baru yang signifikan. Kejahatan siber (cyber crime) melalui penggunaan teknologi deep fake tidak hanya mengancam individu tetapi juga institusi dan bahkan negara. Kejahatan semacam ini bisa memanfaatkan manipulasi konten untuk melakukan penipuan, memeras, atau merusak reputasi seseorang. Misalnya, seorang tokoh publik dapat dijadikan target deep fake untuk menciptakan video atau audio yang merusak citra mereka, meskipun konten tersebut sepenuhnya palsu.

Pada skala yang lebih luas, deep fake dapat digunakan dalam skenario geopolitik untuk menciptakan ketegangan atau konflik internasional. Misalnya, sebuah video yang dibuat dengan teknologi deep fake yang memperlihatkan pemimpin negara tertentu memberikan pernyataan kontroversial bisa memicu ketegangan diplomatik antara negara-negara. [19] Oleh karena itu, penting untuk memahami implikasi teknologi ini tidak hanya dari sudut pandang teknis, tetapi juga dari sudut pandang hukum dan sosial.

[19] Widayanthi, D. G. C., & Wulandari, C. I. A. S. (2025). *Communication Ethics: Etika Komunikasi Modern di Era Digital*. Deepublish.

Deep fake juga menimbulkan pertanyaan mendalam tentang perlindungan privasi dan hak individu. Karena kemampuan teknologi ini untuk meniru wajah dan suara seseorang, deep fake berpotensi melanggar hak privasi individu, terutama ketika digunakan tanpa persetujuan. Misalnya, banyak kasus di mana deep fake digunakan untuk menciptakan konten pornografi yang melibatkan wajah individu yang sebenarnya tidak terlibat dalam pembuatan konten tersebut.[20] Fenomena ini dikenal sebagai "pornografi non-konsensual," di mana wajah seseorang ditempelkan secara digital pada tubuh orang lain dalam video porno, tanpa sepengetahuan atau persetujuan orang tersebut.

Fenomena deep fake ini telah mendorong banyak negara dan pakar hukum untuk mulai memikirkan bagaimana regulasi hukum dapat diterapkan untuk menangani penyalahgunaan teknologi ini. Mengingat potensi kerusakan yang bisa ditimbulkan oleh deep fake, hukum harus mampu beradaptasi dengan cepat untuk memberikan perlindungan yang cukup bagi individu dan masyarakat secara keseluruhan. Perkembangan teknologi yang cepat ini menuntut hukum untuk lebih fleksibel dalam mengatur dan melindungi dari kejahatan baru yang belum pernah terjadi sebelumnya.

Banyak ahli hukum berpendapat bahwa tantangan utama dalam mengatur deep fake adalah sifat teknologinya yang sangat canggih dan terus berkembang. Setiap kali ada upaya untuk menciptakan alat atau sistem yang dapat mendeteksi deep fake, teknologi tersebut selalu mampu berkembang lebih cepat, menciptakan

[20] Respati, A. A., Setyarini, A. D., Parlagutan, D., Rafli, M., Mahendra, R. S., & Nugroho, A. A. (2024). Analisis Hukum Terhadap Pencegahan Kasus Deepfake Serta Perlindungan Hukum Terhadap Korban. *Media Hukum Indonesia (MHI)*, *2*(2).

versi baru yang lebih sulit dideteksi.[21] Ini berarti bahwa upaya untuk melawan kejahatan deep fake harus melibatkan tidak hanya perubahan dalam hukum, tetapi juga inovasi teknologi yang terus-menerus untuk mengidentifikasi dan mencegah penyalahgunaannya.

Di Indonesia, meskipun teknologi deep fake belum secara luas dibahas dalam ranah hukum formal, potensi dampak negatif dari penggunaannya jelas terlihat. Mengingat Indonesia adalah negara dengan populasi pengguna media sosial yang sangat besar, bahaya penyalahgunaan teknologi ini semakin nyata. Penyebaran hoaks yang sering kali terjadi melalui media sosial bisa semakin diperparah dengan adanya konten deep fake yang sulit dibedakan dari yang asli.

Dalam konteks ini, penting bagi Indonesia untuk segera mengembangkan kerangka hukum yang lebih jelas untuk menangani ancaman yang muncul dari penggunaan teknologi deep fake. Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) yang saat ini menjadi landasan hukum untuk menangani kejahatan siber dapat menjadi langkah awal, tetapi regulasi yang lebih spesifik mengenai deep fake perlu dipertimbangkan untuk melindungi masyarakat dari bahaya yang ditimbulkan oleh teknologi ini.

Dengan demikian, pengertian deep fake tidak hanya berkisar pada aspek teknis pembuatannya, tetapi juga mencakup dampak sosial, politik, dan hukum yang lebih luas. Sebagai salah satu produk teknologi yang paling canggih dan kontroversial saat ini, deep fake menuntut perhatian serius dari para pembuat

[21] Budiasto, J., Jayawardana, H., Juansa, A., Hirzan, A. M., Agusdi, Y., Harjoseputro, Y., ... & Rianty, E. (2025). *Pengantar Ilmu Komputer: Pengenalan Dasar Komputer dan Teknologi Informasi Modern*. Henry Bennett Nelson.

kebijakan, penegak hukum, serta masyarakat agar teknologi ini tidak disalahgunakan untuk tujuan yang merugikan.

Adapun perkembangan deepfake dari masa ke masa adalah:[22]

1. Tahun 2011-2016: Peneliti mengembangkan Generative Adversarial Networks (GANs), yang merupakan dasar untuk pembuatan deepfake. Ian Goodfellow dan timnya menciptakan GAN, sebuah teknik pembelajaran mesin yang memungkinkan pembuatan gambar dan video realistis, termasuk deepfake.
2. Tahun 2017: Peneliti Google mengembangkan model transformer yang berperan dalam pembuatan model bahasa besar (LLM), yang kemudian berkontribusi pada pengembangan teknologi deepfake berbasis teks dan gambar.
3. Tahun 2018-2020: Perkembangan lebih lanjut dalam teknik deepfake terjadi dengan kemajuan pada model bahasa generatif dan pengenalan gambar yang mendalam. Pada 2020, OpenAI merilis GPT-3 yang meningkatkan kemampuan model teks dalam menghasilkan konten mirip manusia, serta teknologi lainnya yang digunakan dalam aplikasi deepfake.
4. Tahun 2021-2022: Teknologi multimodal AI semakin berkembang, termasuk model seperti DALL-E yang dapat menghasilkan gambar dari teks. Pada 2022, Intel meluncurkan FakeCatcher, sistem deteksi deepfake dengan akurasi 96%, yang menunjukkan upaya untuk mengidentifikasi dan mengatasi penyalahgunaan teknologi deepfake.

[22] Ron Karjian, "The history of artificial intelligence: Complete AI timeline" dalam https://www.techtarget.com/searchenterpriseai/tip/The-history-of-artificial-intelligence-CompleteAI-timeline, diunduh tanggal 30 Juni 2024.

5. Tahun 2023: ChatGPT berkembang menjadi GPT-4, LLM multimodal yang dapat menerima input berupa teks dan gambar, semakin meningkatkan kemampuan aplikasi deepfake dalam menciptakan konten multimedia realistis.

Secara keseluruhan, perkembangan deepfake sangat dipengaruhi oleh kemajuan dalam GANs, model bahasa besar, serta kemampuan pengenalan dan manipulasi gambar dan video, yang dimanfaatkan untuk menciptakan media palsu yang tampak sangat realistis.

2.2 Tinjauan Konstruksi Hukum

2.2.1 . Definisi kontruksi hukum

"Konstruksi hukum" adalah metode atau proses penafsiran terhadap norma-norma hukum yang ada, yang bertujuan untuk memahami dan menerapkan peraturan hukum sesuai dengan maksud pembuat undang-undang dan konteks sosial yang berlaku.[23] Dalam konstruksi hukum, hakim, ahli hukum, atau penegak hukum akan menganalisis teks undang-undang atau peraturan, serta menafsirkan maknanya agar dapat diterapkan dalam situasi tertentu. Beriku adalah definisi konstruksi hukum menurut beberapa ahli:

1. Satjipto Rahardjo menyatakan bahwa konstruksi hukum adalah metode untuk memahami hukum secara menyeluruh, mencakup pemaknaan, interpretasi, dan aplikasi hukum di dalam konteks yang nyata. Menurutnya, konstruksi hukum merupakan proses kreatif yang diperlukan agar hukum tidak hanya sekadar teks, tetapi dapat

[23] Hamidi, Jazim. *Hermeneutika hukum: Sejarah, filsafat, & metode tafsir*. Universitas Brawijaya Press, 2011.

mengakomodasi nilai-nilai sosial yang berkembang. Dalam pandangannya, konstruksi hukum membantu mengatasi rigiditas dari aturan hukum tertulis yang kerap kali tidak mampu menyesuaikan diri dengan perubahan sosial yang cepat.[24]

2. Soerjono Soekanto mengartikan konstruksi hukum sebagai upaya sistematis untuk menghubungkan antara kaidah hukum yang ada dengan fakta-fakta sosial yang terjadi di lapangan. Proses ini melibatkan metode penafsiran, analogi, dan argumentasi untuk menjamin bahwa hukum dapat berfungsi secara efektif dalam memecahkan konflik sosial. Konstruksi hukum, menurut Soekanto, diperlukan agar hukum tidak menjadi alat yang kaku, tetapi menjadi solusi yang adil bagi masyarakat.[25]
3. Lili Rasjidi mendefinisikan konstruksi hukum sebagai proses intelektual untuk menjelaskan aturan-aturan hukum agar dapat diterapkan pada situasi yang konkrit. Konstruksi hukum melibatkan pemahaman terhadap teks hukum (legal text) dan bagaimana teks tersebut diterjemahkan ke dalam praktik hukum yang nyata. Menurutnya, konstruksi hukum melibatkan berbagai disiplin, termasuk filsafat hukum, sosiologi hukum, dan ilmu-ilmu sosial lainnya. Hans Kelsen dalam "Theory of Pure Law" menganggap konstruksi hukum sebagai alat untuk memahami struktur normatif dari suatu sistem hukum. Ia menekankan bahwa hukum harus dibangun di

[24] Satjipto Rahardjo, Membedah Hukum Progresif, (Jakarta: Buku Kompas, 2008)
[25] Soekanto, S. (1982). Kesadaran Hukum & Kepatuhan Hukum. Penerbit CV Rajawali.

atas asas-asas yang rasional dan logis, sehingga setiap konstruksi hukum harus dapat dipertanggungjawabkan secara ilmiah. Kelsen menganggap konstruksi hukum sebagai upaya untuk memberikan kejelasan dan kohesi terhadap norma-norma yang kadang saling bertentangan.[26]

4. Hans Kelsen: Menurut Kelsen, konstruksi hukum adalah bagian dari teori hukum yang berfungsi untuk menjelaskan bagaimana norma-norma hukum diterapkan dan diinterpretasikan dalam praktik.[27]
5. Ronald Dworkin: Dworkin berpendapat bahwa konstruksi hukum melibatkan pencarian makna hukum yang paling tepat dengan mempertimbangkan prinsip-prinsip moral dan keadilan.[28]

2.2.2. Pentingnya Konstruksi Hukum

Konstruksi hukum penting karena:[29]

1. Memastikan Kepastian Hukum: Dengan memberikan interpretasi yang konsisten, konstruksi hukum membantu menjaga kepastian dan stabilitas hukum.
2. Menyesuaikan Hukum dengan Perkembangan Sosial: Konstruksi hukum memungkinkan hukum untuk beradaptasi dengan perubahan dalam masyarakat, termasuk perkembangan teknologi seperti deep fake.
3. Menegakkan Keadilan: Melalui konstruksi hukum, prinsip-prinsip keadilan dapat ditegakkan dalam penerapan hukum.

[26] Rasjidi, L. Dasar-dasar filsafat hukum. 2004.
[27] Kelsen, Hans. *General theory of law and state*. Routledge, 2017.
[28] Dworkin, Ronald. Law as interpretation. *Critical Inquiry*, 1982, 9.1: 179-200.
[29] Bell, J., & Engle, G. (2005). Cross: Statutory Interpretation. Oxford: Oxford University Press.

2.2.3 Metode Konstruksi Hukum

Beberapa metode yang sering digunakan dalam konstruksi hukum meliputi:[30]

1. Interpretasi Gramatikal: Penafsiran kata-kata dalam teks hukum berdasarkan kaidah bahasa dan hukum. Artinya dapat lebih mendalam dari teks asli karena satu kata bisa memiliki berbagai makna.
2. Interpretasi Sosiologis: Penafsiran undang-undang berdasarkan maksud pembuatnya, lebih fokus pada tujuan hukum daripada teksnya. Ini penting untuk menyelaraskan hukum dengan realitas sosial.
3. Interpretasi Sistematis: Penafsiran peraturan dengan menghubungkannya pada sistem hukum secara keseluruhan. Setiap peraturan dipahami dalam konteks sistem hukum yang lebih luas.
4. Interpretasi Historis: Penafsiran berdasarkan latar belakang sejarah hukum atau proses penetapan undang-undang. Hal ini mencakup asas, aliran hukum, atau dokumen pembentukan undang-undang.
5. Interpretasi Komparatif: Penafsiran dengan membandingkan sistem hukum yang berbeda untuk mencari kejelasan antara undang-undang dalam satu sistem hukum.
6. Interpretasi Antisipatif: Penafsiran berdasarkan perkiraan bahwa undang-undang yang belum disahkan akan menjadi hukum, seperti rancangan undang-undang yang sedang dibahas.

[30] Jazim Hamidi. (2005). Metode Penemuan Hukum. Yogyakarta: UII Press, hlm. 50

7. Interpretasi Restriktif: Penafsiran yang membatasi ruang lingkup ketentuan undang-undang sesuai arti bahasa yang lebih sempit.
8. Interpretasi Ekstensif: Penafsiran yang melampaui batas interpretasi gramatikal untuk memberikan pemahaman yang lebih luas.
9. Interpretasi Subsumtif: Penerapan teks undang-undang pada kasus konkret dengan menggunakan logika deduktif (sillogisme).
10. Interpretasi Interdisipliner: Penafsiran yang melibatkan berbagai disiplin ilmu hukum untuk analisis masalah hukum yang kompleks.
11. Interpretasi Multidisipliner: Penafsiran yang mengacu pada disiplin ilmu di luar hukum untuk kasus hukum yang semakin rumit, seperti terorisme atau cybercrime.

2.2.4 Tantangan dalam Konstruksi Hukum

Dalam konteks teknologi baru seperti deep fake, konstruksi hukum menghadapi sejumlah tantangan, antara lain:

1. Ambiguitas Bahasa Hukum: Bahasa hukum yang digunakan mungkin tidak cukup spesifik untuk menangani isu-isu baru.
2. Perubahan Teknologi: Teknologi yang berkembang pesat dapat membuat hukum tertinggal jika tidak diinterpretasikan secara dinamis.
3. Konflik Antar Norma: Norma hukum yang ada mungkin tidak selaras dengan kebutuhan untuk mengatur teknologi baru.

2.3 Pengaturan Hukum Tindak Pidana Deep Fake di Indonesia

Fenomena deep fake merupakan tantangan baru di era digital yang menghadirkan ancaman terhadap privasi, reputasi, dan keamanan publik. Deep fake adalah teknologi berbasis kecerdasan buatan (Artificial Intelligence/AI) yang

memungkinkan manipulasi gambar, video, atau audio sehingga menyerupai atau meniru seseorang secara akurat. Meskipun teknologi ini pada awalnya dikembangkan untuk keperluan hiburan dan seni, kini telah disalahgunakan untuk berbagai kejahatan, mulai dari penipuan, pencemaran nama baik, hingga pornografi non-konsensual.

Di Indonesia, peraturan yang secara spesifik mengatur tindak pidana deep fake belum ada. Namun, beberapa perangkat hukum yang telah ada dapat dijadikan dasar untuk menjerat pelaku tindak pidana yang menggunakan deep fake, dengan memanfaatkan berbagai aturan di bidang hukum pidana dan hukum teknologi informasi. Upaya untuk mengatur secara khusus deep fake akan sangat penting di masa depan mengingat ancaman yang ditimbulkan oleh teknologi ini semakin meluas.

1. Undang-Undang Informasi dan Transaksi Elektronik (UU ITE)

   Salah satu perangkat hukum yang dapat digunakan untuk menjerat pelaku deep fake adalah Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), khususnya Pasal 27 dan Pasal 28. Kedua pasal ini mengatur mengenai penyebaran informasi yang melanggar kesusilaan, penghinaan, dan pencemaran nama baik, serta penyebaran berita bohong (hoaks).

   Pasal 27 UU ITE mengatur larangan untuk mendistribusikan, mentransmisikan, dan membuat dapat diaksesnya konten elektronik yang mengandung muatan kesusilaan, penghinaan, atau pencemaran nama baik. Pasal 28 mengatur tentang penyebaran berita bohong yang dapat menyebabkan kerugian pada pihak lain atau mengakibatkan keresahan di

masyarakat. Dalam konteks deep fake, konten manipulatif yang menyesatkan dan dibuat dengan tujuan menipu atau mencemarkan nama baik dapat diklasifikasikan sebagai tindak pidana berdasarkan pasal-pasal ini.

Namun, UU ITE belum mengatur secara khusus mengenai deep fake, sehingga penerapan hukum sering kali bergantung pada interpretasi mengenai definisi "informasi elektronik" dan "konten manipulatif." Hal ini menjadi kelemahan dalam penerapan hukum terhadap tindak pidana yang melibatkan teknologi deep fake, karena undang-undang tersebut lebih berfokus pada kejahatan digital secara umum tanpa menyebut teknologi ini secara spesifik.

2. Kitab Undang-Undang Hukum Pidana (KUHP)

Selain UU ITE, Kitab Undang-Undang Hukum Pidana (KUHP) juga memiliki beberapa pasal yang dapat digunakan untuk menjerat pelaku tindak pidana deep fake. Meskipun KUHP tidak menyebutkan secara eksplisit mengenai deep fake, beberapa tindak pidana yang diatur dalam KUHP dapat diterapkan terhadap perilaku yang melibatkan manipulasi konten ini.

Pasal 310 KUHP tentang pencemaran nama baik dan Pasal 311 KUHP tentang penghinaan berat dapat diterapkan jika deep fake digunakan untuk merusak reputasi seseorang. Pembuatan dan penyebaran konten deep fake yang merugikan seseorang dengan cara meniru atau mengubah video atau gambar individu tersebut dapat dianggap sebagai bentuk pencemaran

nama baik. Pelaku dapat dijerat dengan pasal-pasal ini apabila terbukti menyebarkan konten yang merugikan atau merusak martabat korban.

Selain itu, Pasal 378 KUHP tentang penipuan juga relevan apabila deep fake digunakan dalam konteks penipuan, misalnya dalam penipuan identitas atau skema penipuan yang melibatkan manipulasi video/audio untuk menipu pihak lain dengan motif keuntungan ekonomi. Dalam kasus seperti ini, pelaku dapat dijerat dengan tindak pidana penipuan sesuai dengan ketentuan yang diatur dalam KUHP.

3. Undang-Undang Pornografi

Jika deep fake digunakan dalam konteks pornografi non-konsensual, maka Undang-Undang Pornografi juga dapat dijadikan landasan untuk menjerat pelaku. Undang-Undang Nomor 44 Tahun 2008 tentang Pornografi mengatur mengenai pembuatan, penyebaran, serta penyalahgunaan konten yang mengandung unsur pornografi, baik dalam bentuk gambar, video, maupun audio.

Dalam kasus deep fake pornografi, teknologi ini digunakan untuk menempelkan wajah korban ke dalam konten pornografi secara tidak sah. Meskipun individu tersebut tidak benar-benar terlibat dalam tindakan yang ditampilkan, dampaknya dapat merusak nama baik dan integritas korban secara signifikan. Undang-undang ini dapat menjadi instrumen hukum untuk melindungi korban deep fake yang terlibat dalam konten pornografi non-konsensual, dan pelaku dapat dijerat dengan ketentuan yang terdapat dalam UU Pornografi.

Pasal 4 UU Pornografi melarang siapapun untuk memproduksi, membuat, memperbanyak, menggandakan, mendistribusikan, menyiarkan, mengimpor, mengekspor, menawarkan, menjual, menyewakan, atau menyediakan pornografi. Dalam konteks deep fake, jika konten yang dimanipulasi berisi unsur pornografi dan disebarluaskan tanpa persetujuan, pelaku dapat dikenakan sanksi pidana sesuai pasal tersebut.

4. Undang-Undang Perlindungan Data Pribadi

Perlindungan Data Pribadi (PDP) merupakan suatu konsep yang semakin relevan di era digital saat ini, di mana informasi pribadi individu seringkali diproses, disimpan, dan dibagikan melalui berbagai platform teknologi. Dalam konteks global, PDP merujuk pada serangkaian aturan, kebijakan, dan praktik yang dirancang untuk melindungi data pribadi individu dari penyalahgunaan, akses tidak sah, dan pelanggaran privasi. Data pribadi mencakup setiap informasi yang dapat digunakan untuk mengidentifikasi individu, termasuk nama, alamat, nomor telepon, alamat email, dan data biometrik. PDP berfokus pada pengaturan bagaimana data ini dikumpulkan, digunakan, dan disimpan oleh organisasi, baik pemerintah maupun swasta. Ruang lingkup PDP tidak hanya mencakup data yang dikumpulkan secara langsung, tetapi juga data yang diperoleh melalui interaksi online, transaksi bisnis, dan media sosial.

Ada beberapa prinsip dasar dalam perlindungan data pribadi yang umumnya diadopsi secara internasional. Pertama, prinsip transparansi mengharuskan individu diinformasikan tentang bagaimana dan untuk tujuan

apa data pribadi mereka akan digunakan. Kedua, kepatuhan menekankan bahwa organisasi harus mematuhi peraturan yang ada terkait pengumpulan dan penggunaan data pribadi. Ketiga, prinsip minimisasi data menyatakan bahwa data yang dikumpulkan harus relevan dan tidak lebih dari yang diperlukan untuk mencapai tujuan pengumpulan. Keamanan data juga menjadi fokus utama, di mana organisasi harus menerapkan langkah-langkah yang memadai untuk melindungi data pribadi dari akses tidak sah dan kebocoran. Terakhir, individu memiliki hak akses dan kontrol, yang berarti mereka berhak untuk mengakses, memperbaiki, atau menghapus data pribadi mereka yang disimpan oleh organisasi.

Meskipun beberapa perangkat hukum di Indonesia, seperti UU ITE, KUHP, UU Pornografi, dan UU Perlindungan Data Pribadi dapat digunakan untuk menjerat pelaku kejahatan deep fake, Indonesia masih membutuhkan regulasi yang lebih spesifik dan terarah mengenai tindak pidana deep fake. Peraturan yang ada saat ini tidak secara eksplisit mengatur tentang teknologi deep fake, sehingga interpretasi terhadap undang-undang tersebut sering kali bersifat luas dan belum mampu menjangkau seluruh aspek dari kejahatan yang menggunakan teknologi ini.

Pencemaran nama baik memiliki kaitan erat dengan teknologi deep fake, karena deep fake dapat digunakan untuk memalsukan video atau audio seseorang sehingga tampak melakukan atau mengatakan hal-hal yang merusak reputasi mereka. Konten palsu ini, jika disebarluaskan, bisa menimbulkan kerugian besar bagi korban baik secara pribadi maupun profesional, karena masyarakat sering kali tidak dapat membedakan antara yang asli dan yang direkayasa. Oleh karena itu, penggunaan deep fake dalam konteks menyebarkan informasi palsu termasuk

bentuk pencemaran nama baik digital yang berbahaya dan melanggar hukum serta etika. Pencemaran nama baik dilarang karena dapat menimbulkan berbagai dampak negatif, seperti merusak reputasi pribadi, menghancurkan karier atau bisnis, serta menyebabkan kerugian finansial. Selain itu, korban bisa mengalami tekanan mental, seperti stres, depresi, atau trauma akibat serangan terhadap harga diri mereka. Tindakan ini juga dapat memicu konflik sosial, perpecahan, bahkan kekerasan, serta dianggap sebagai pelanggaran terhadap hak asasi manusia karena merampas hak seseorang untuk dihormati dan dilindungi martabatnya.

Kehadiran regulasi khusus yang mengatur tentang pembuatan, penggunaan, dan penyebaran konten deep fake akan sangat penting untuk memastikan adanya kepastian hukum bagi korban dan untuk memberikan sanksi yang tepat bagi pelaku. Regulasi ini perlu mengakomodasi perkembangan teknologi informasi yang sangat cepat dan sifat dari kejahatan siber yang terus berkembang, termasuk deep fake yang dapat digunakan untuk berbagai tindak pidana.

Selain itu, kerjasama internasional juga diperlukan mengingat kejahatan deep fake sering kali melibatkan pelaku lintas negara, sehingga aparat penegak hukum memerlukan instrumen hukum yang dapat memfasilitasi penanganan kejahatan siber yang bersifat transnasional. Teknologi ini memungkinkan pelaku untuk menyembunyikan identitas dan lokasi mereka dengan mudah, sehingga upaya kolaboratif antarnegara menjadi penting dalam memerangi kejahatan ini.

Penegakan hukum terhadap kejahatan siber di Indonesia, termasuk deep fake, masih menghadapi berbagai tantangan, seperti kurangnya sumber daya manusia yang memiliki keahlian khusus di bidang forensik digital dan keamanan siber. Pelatihan bagi aparat penegak hukum, termasuk polisi, jaksa, dan hakim,

perlu ditingkatkan agar mereka dapat memahami dan menangani kasus-kasus yang melibatkan deep fake dengan lebih efektif.

Selain itu, infrastruktur teknologi di berbagai instansi pemerintah juga perlu ditingkatkan, mengingat kejahatan siber sering kali menggunakan teknologi canggih yang sulit dideteksi dengan metode konvensional. Dukungan dari sektor swasta dan institusi pendidikan dalam menyediakan solusi teknologi serta pelatihan akan menjadi salah satu kunci untuk memperkuat penegakan hukum di Indonesia dalam menghadapi tantangan deep fake.

2.4 Tinjauan Umum tentang Cybercrime

2.4.1. Pengertian Cybercrime

Cybercrime, atau kejahatan siber, merujuk pada segala jenis aktivitas kriminal yang dilakukan melalui atau menargetkan jaringan komputer, perangkat elektronik, dan internet. Istilah ini mencakup berbagai bentuk kejahatan yang melibatkan teknologi digital sebagai sarana atau target. [31] Seiring dengan kemajuan pesat teknologi informasi dan komunikasi, cybercrime telah menjadi ancaman global yang berdampak luas, baik terhadap individu, organisasi, maupun negara.

Cybercrime dapat dibagi menjadi dua kategori utama:[32]

1. Kejahatan yang menggunakan teknologi informasi sebagai alat utama, seperti pencurian identitas, penipuan daring (online fraud), pembobolan sistem komputer (hacking), dan penyebaran malware atau ransomware.

[31] Widodo, Aspek Hukum Pidana Kejahatan Mayantara. Aswaja Pressindo. 2013.
[32] Ibid

2. Kejahatan yang ditargetkan terhadap sistem atau infrastruktur digital, seperti serangan DDoS (Distributed Denial of Service) yang bertujuan merusak jaringan, sabotase terhadap infrastruktur penting, serta pencurian data atau informasi pribadi melalui peretasan.

2.4.2. Jenis-Jenis Cybercrime

Cybercrime mencakup berbagai bentuk aktivitas kriminal, di antaranya:

1. Phishing: Tindakan penipuan melalui teknik manipulasi sosial, di mana pelaku mengelabui korban untuk memberikan informasi sensitif, seperti nomor kartu kredit atau kata sandi, dengan berpura-pura sebagai entitas tepercaya.
2. Malware dan Ransomware: Malware adalah perangkat lunak berbahaya yang dirancang untuk merusak atau mendapatkan akses tidak sah ke sistem komputer. Ransomware adalah jenis malware yang mengenkripsi data pengguna dan meminta tebusan untuk mendekripsi data tersebut.
3. Pencurian Identitas (Identity Theft): Menggunakan informasi pribadi seseorang, seperti nomor identitas, data finansial, atau akun sosial media, untuk tujuan kriminal, seperti melakukan transaksi penipuan atau menyebarkan hoaks.
4. Cyberbullying: Perundungan atau intimidasi yang dilakukan secara daring, biasanya melalui media sosial, yang bertujuan untuk mempermalukan, mengancam, atau merusak reputasi korban.
5. Fraud Daring (Online Fraud): Penipuan yang dilakukan melalui internet, termasuk dalam transaksi jual-beli daring yang tidak sah, investasi palsu, atau skema ponzi yang mengeksploitasi korbannya.

6. Serangan DDoS: Serangan yang dirancang untuk melumpuhkan suatu sistem atau layanan online dengan cara membanjiri jaringan dengan lalu lintas data yang sangat besar sehingga menyebabkan server tidak dapat menanggapi pengguna normal.
7. Hacking: Aktivitas yang bertujuan untuk mendapatkan akses ilegal ke sistem komputer, jaringan, atau data. Pelaku hacking sering kali mengeksploitasi kerentanan dalam sistem untuk mencuri data, merusak, atau mengubah informasi.

2.4.3. Dampak Cybercrime

Cybercrime memiliki dampak yang signifikan terhadap berbagai aspek kehidupan sosial, ekonomi, dan politik. Di sektor bisnis, misalnya, cybercrime dapat mengakibatkan kerugian finansial yang besar melalui pencurian data pelanggan, sabotase infrastruktur TI, atau penipuan keuangan. Beberapa dampak utama dari cybercrime adalah:

1. Kerugian Ekonomi: Menurut berbagai studi, kejahatan siber telah menyebabkan kerugian ekonomi global yang mencapai triliunan dolar. Selain biaya pemulihan sistem yang rusak, perusahaan juga menghadapi biaya reputasi dan hilangnya kepercayaan pelanggan.
2. Ancaman Keamanan Nasional: Serangan cyber terhadap infrastruktur kritis suatu negara, seperti sistem energi, transportasi, atau kesehatan, dapat mengancam keamanan nasional. Beberapa negara telah menjadi target serangan cyber yang diduga berasal dari kelompok kriminal atau aktor negara tertentu.

3. Kerusakan Reputasi: Banyak perusahaan atau individu yang kehilangan reputasi akibat kebocoran data yang diakibatkan oleh serangan cyber. Kebocoran data ini juga berpotensi menyebabkan tuntutan hukum yang merugikan secara finansial dan merusak kredibilitas entitas yang diserang.
4. Gangguan Sosial dan Politik: Cybercrime dapat digunakan sebagai alat untuk menyebarkan disinformasi atau mempengaruhi opini publik, terutama selama periode pemilu atau ketegangan politik. Beberapa kasus cybercrime telah diketahui memanipulasi hasil pemilihan umum melalui serangan yang menargetkan sistem digital atau kampanye media sosial.

2.4.4. Regulasi dan Penegakan Hukum Cybercrime

Menghadapi tantangan yang ditimbulkan oleh cybercrime, banyak negara telah mengembangkan regulasi yang mengatur tentang kejahatan siber. Di Indonesia, salah satu regulasi utama adalah Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), yang diundangkan untuk melindungi masyarakat dari berbagai ancaman cybercrime, termasuk penyalahgunaan teknologi informasi, pencemaran nama baik secara daring, serta penipuan dalam transaksi elektronik. Namun, masih banyak tantangan dalam penegakan hukum terkait cybercrime, seperti kurangnya infrastruktur teknologi penegak hukum, serta kemampuan pelaku cybercrime yang terus berkembang lebih cepat dibandingkan regulasi yang ada.

Beberapa tantangan lain dalam penanganan cybercrime adalah:

1. Kejahatan Lintas Negara: Cybercrime sering kali melibatkan pelaku dan korban di berbagai negara yang berbeda. Hal ini menyulitkan penegakan hukum karena perbedaan yurisdiksi dan regulasi antarnegara.
2. Anonimitas: Internet memungkinkan pelaku cybercrime beroperasi secara anonim atau menggunakan identitas palsu, yang menyulitkan aparat hukum dalam mengidentifikasi dan menangkap pelaku.
3. Kurangnya Ahli Keamanan Siber: Sektor penegakan hukum masih mengalami kekurangan sumber daya manusia yang memiliki keahlian khusus dalam menangani kejahatan siber. Pelatihan khusus dalam keamanan siber perlu ditingkatkan agar aparat dapat lebih efektif dalam menghadapi ancaman cybercrime.

2.4.5. Upaya Pencegahan Cybercrime

Pencegahan cybercrime memerlukan kolaborasi antara pemerintah, sektor swasta, dan masyarakat umum. Beberapa langkah yang dapat diambil untuk mencegah dan mengurangi risiko cybercrime antara lain:

1. Peningkatan Kesadaran: Masyarakat perlu lebih waspada terhadap potensi ancaman cybercrime. Pendidikan dan kampanye kesadaran tentang pentingnya menjaga keamanan informasi pribadi, seperti penggunaan kata sandi yang kuat, penghindaran email phishing, serta tidak membagikan informasi sensitif di platform yang tidak aman, sangat diperlukan.
2. Pengembangan Teknologi Keamanan: Perusahaan teknologi perlu terus mengembangkan perangkat lunak dan perangkat keras yang

lebih aman, seperti firewall, enkripsi data, dan sistem deteksi ancaman yang canggih.

3. Kerjasama Internasional: Mengingat sifat cybercrime yang sering kali melintasi batas negara, kerjasama internasional sangat penting. Negara-negara harus berbagi informasi dan teknologi untuk mengidentifikasi dan menangkap pelaku cybercrime secara lebih efektif.
4. Penerapan Kebijakan yang Kuat: Pemerintah perlu merumuskan kebijakan yang jelas dan spesifik mengenai keamanan siber, termasuk sanksi yang tegas bagi pelaku cybercrime serta insentif bagi perusahaan yang berinvestasi dalam keamanan siber.