

BAB 1

PENDAHULUAN

1.1 Latar Belakang

Teknologi sangat penting bagi banyak kegiatan manusia. Teknologi tidak hanya mempercepat dan mempermudah penyebaran informasi, tetapi juga membantu masyarakat dalam banyak hal, dapat memudahkan kegiatan ekonomi seperti pemasaran, penjualan, pembelian, dan operasi komersial. Perkembangan teknologi informasi, di satu sisi memberi kemudahan, di sisi lain menimbulkan masalah. Kemajuan teknologi menyebabkan terjadinya evolusi kejahatan. Jika dulu kejahatan hanya berupa tindakan konvensional, kini muncul kejahatan baru yaitu kejahatan dunia maya yang merupakan tindakan kejahatan yang memanfaatkan internet serta perangkat elektronik untuk melakukan kejahatan.¹

Kemajuan teknologi telah memengaruhi berbagai aspek kehidupan, mulai dari pekerjaan rumah tangga, misalnya pekerjaan rumah tangga, sampai bidang lebih kompleks misalnya pekerjaan kreatif yang semakin bergantung pada teknologi. Perkembangan teknologi ini tak terpisahkan dari perkembangan media. Teknologi telah melahirkan bentuk media baru yang dikenal selaku media online yang beroperasi lewat internet. Teknologi internet memberi peluang untuk mewujudkan mekanisme yang lebih canggih dan efisien.²

Artificial intelligence (AI) adalah sistem cerdas yang muncul sebagai hasil

¹ Ferry Irawan Febriansyah, Alfalachu Indiantoro, dan Afiful Ikhwan, "Model Kejahatan Dunia Maya (*Cybercrime*) sebagai Upaya Pembentukan Hukum Nasional," *Legal Standing: Jurnal Ilmu Hukum*, Vol. 7 No. 2, (September, 2023): hlm. 242.

² Vika Oktallia & I Gede Putra Ariana, "Perlindungan terhadap Korban Penyalahgunaan Teknik *Deepfake* terhadap Data Pribadi," *Kertha Desa*, Vol. 10 No. 11, (November, 2022), hlm. 1255.

dari terobosan teknologi yang pesat. Maraknya *Artificial intelligence* (AI) menunjukkan bahwa kemajuan teknologi informasi di era digital dapat meningkatkan kualitas hidup manusia.³ Perkembangan *Artificial intelligence* adalah salah satu contohnya. Salah satu ilustrasi nyata dari kemajuan teknis terkini adalah *Artificial intelligence*. Kata "*artificial*" artinya buatan, serta "*intelligence*" artinya kecerdasan, membentuk istilah bahasa untuk *Artificial intelligence* (AI). Mesin, gawai, atau alat yang memiliki kecerdasan atau kemampuan untuk bernalar dan berpikir seperti manusia disebut memiliki *Artificial intelligence*. *Artificial intelligence*, yang dioperasikan oleh mesin, dikatakan lebih cepat dan lebih akurat daripada manusia dalam menjalankan instruksi atau program.⁴

Teknologi *deepfake* merupakan salah satu pemanfaatan inovasi teknologi yang saat ini tengah menjadi sorotan. Teknologi *deepfake* termasuk dalam kategori seni yang dihasilkan komputer, terkadang disebut sebagai media sintetis. Istilah "teknologi *deepfake*" mengacu pada media pemrosesan audiovisual yang dapat diubah atau disintesis untuk memberikan kesan autentik, meskipun *Artificial intelligence* digunakan untuk memfasilitasi prosesnya. Teknologi *deepfake* memungkinkan terciptanya keluaran yang sangat mirip dengan kenyataan dengan menggabungkan foto, audio, atau video dengan berbagai item dan konten. Sederhananya, *Deepfake* adalah alat kecerdasan buatan (AI) terkenal yang sering digunakan untuk tujuan jahat. Misalnya, merekayasa suara atau video untuk

³ Rizgita Nurul Fauzyah, Putri Hafidati, dan Sunarya, "Perlindungan Hukum terhadap Korban Tindak Pidana Pembuat Video Pornografi Palsu (*Deepfake Porn*) Berbasis *Artificial Intelligence* (AI) di Indonesia," *Lex Veritatis*, Vol. 3 No. 3, (November, 2024), hlm. 74.

⁴ Luh Putu Ary Sri Tjahyanti, Putu Satya Saputra, dan Made Santo Gitakarma, "Peran *Artificial Intelligence* (AI) untuk Mendukung Pembelajaran di Masa Pandemi Covid-19," *Jurnal Komputer dan Teknologi Sains (KOMTEKS)*, Vol. 1 No. 1, (Oktober 2022), hlm. 15.

menyebarkan informasi palsu atau menjelekkan seseorang. Orang yang menggunakan *deepfake* bisa membuat video palsu seseorang yang bisa melanggar privasi, misalnya mengganti identitas orang itu saat pengecekan hal penting seperti akun bank atau keamanan negara.⁵

Semakin ahli pembuat *deepfake*, konten yang dihasilkan akan sangat mirip dengan aslinya dan sulit dibedakan sebagai hasil *deepfake* oleh masyarakat. Jejak manipulasi menggunakan *Deepfake* semakin sulit terdeteksi karena Teknologi *Generative Adversarial Network* (GAN) terus berkembang dengan pesat. Perkembangan *Deepfake* memang memiliki dampak positif, seperti pemanfaatannya dalam produksi film karena dapat menciptakan efek khusus yang lebih realistis, pemanfaatannya dalam dunia medis karena dapat membantu pasien yang tidak memiliki kemampuan motorik dan bicara, serta pemanfaatan positif lainnya. Namun, perkembangan *deepfake* juga memiliki dampak negatif karena banyaknya penyalahgunaan *deepfake*.

Banyak penyalahgunaan *deepfake* mulai dari penggunaannya untuk penipuan, pemerasan, pencemaran nama baik, hingga pembuatan video pornografi tanpa izin.⁶ Tujuan penciptaan *Artificial intelligence* adalah untuk membantu manusia dalam pekerjaan mereka. *Artificial intelligence*, yang awalnya hanya dapat memproses perintah-perintah dasar, kini mampu memahami tugas-tugas yang lebih rumit, termasuk mengemudikan mobil, memahami bahasa manusia,

⁵ Intan Leliana, Gema Irhamdhika, Achmad Haikal, Rio Septian, dan Eddy Kusnadi, "Etika dalam Era *Deepfake*: Bagaimana Menjaga Integritas Komunikasi," *Jurnal Visi Komunikasi*, Vol. 22 No. 2, (November 2023): 234.

⁶ Ni Kadek Dwi Ika Ardiyani, "Analisis Yuridis Pertanggungjawaban Pidana Pelaku *Deepfake* Porn Berdasarkan Hukum Positif," *Jurnal Kajian Hukum dan Kebijakan Publik* Vol. 2 No. 1, (Desember, 2024), hlm. 603.

mengidentifikasi wajah, dan bahkan meniru suara dan wajah manusia. Akibatnya, muncul berbagai bisnis yang mengembangkan program dengan *Artificial intelligence* sebagai keunggulan utama mereka.⁷

Contoh kasusnya yaitu Kasus penipuan berkedok giveaway Raffi Ahmad marak terjadi di masyarakat. Biasanya, pelaku penipuan mencatut nama Raffi Ahmad untuk meyakinkan korbannya. Mereka menggunakan berbagai cara, seperti membuat akun media sosial palsu, situs *web* palsu, atau bahkan grup *WhatsApp* palsu. Modus yang sering digunakan adalah dengan mengiming-imingi hadiah uang tunai, mobil, atau hadiah menarik lainnya. Para pelaku biasanya meminta data pribadi korban, seperti nomor telepon, alamat rumah, atau bahkan nomor rekening bank. Data disalahgunakan untuk keperluan yang tidak bertanggung jawab, seperti pencurian uang atau penipuan lainnya. Empat video manipulasi disediakan oleh penipu untuk membujuk para korban. Testimoni dari orang yang mengaku telah menerima *giveaway* disertakan dalam video.⁸

Keadaan serupa juga muncul dalam penipuan *giveaway* yang menggunakan identitas Baim Wong dan melibatkan media sosial, panggilan telepon, dan pesan teks. Penjahat dalam hal ini menyamar sebagai Baim Wong atau kelompoknya. Namun terkadang, penipu akan menggunakan kecerdasan buatan (AI) untuk meniru ucapan Baim Wong, seperti melalui *voice cloning* atau teknologi *deepfake*. Kloning suara AI, juga dikenal sebagai *voice cloning*, merupakan teknologi yang menggunakan kecerdasan buatan guna meniru suara manusia

⁷ Kaharuddin dan Zul Amirul Haq, *Kecerdasan Buatan: Aspek Perlindungan Hukum di Era Digitalisasi* (Jakarta: Prenada Media, 2024), hlm. 1.

⁸ Anfa'un Nisa' Fidinir Rahman, Syariffudin, Fathol Bari, "Perlindungan Hukum terhadap Korban Penyalahgunaan Teknik *Deepfake*," *Perspektif Administrasi Publik dan hukum*, Vol. 2 No. 1, (Januari, 2025), hlm. 253.

secara akurat. Berkat algoritma *machine learning* yang canggih, teknologi ini dapat mengidentifikasi dan meniru nuansa, intonasi, serta pola bicara suara manusia. Langkah pertama proses *voice cloning* AI yaitu mengumpulkan data suara target. Percakapan, wawancara, dan sumber suara lainnya bisa dikenakan untuk mengumpulkan data ini. Setelah pengumpulan data, sistem *machine learning* akan memeriksa dan mengidentifikasi berbagai pola bicara.

Fenomena peniruan suara melalui teknologi AI, seperti *voice cloning* dalam kasus penipuan Baim Wong, hanyalah salah satu dari beragam modus penipuan *online* yang perlu diwaspadai oleh masyarakat guna memberikan gambaran yang lebih jelas terkait ancaman kejahatan siber. Berikut adalah beberapa contoh umum penipuan *online*: Pertama, *phishing* menggunakan pesan palsu (email/SMS) berisi tautan ke situs web penipu untuk mencuri data pribadi. Untuk menghindarinya, verifikasi pengirim pesan sebelum memasukkan informasi.⁹ Kedua, *pharming*, yaitu manipulasi lalu lintas situs atau penyebaran *malware* untuk mencuri data saat pengguna mengunjungi situs palsu yang mirip dengan aslinya.

Ketiga, *sniffing*, metode pengumpulan informasi ilegal melalui jaringan yang diretas, sering terjadi pada koneksi Wifi publik. Keempat, *money mule*, di mana korban tanpa sadar dilibatkan dalam pencucian uang dengan menerima dan meneruskan dana ke rekening lain. Kelima, *social engineering*, yaitu manipulasi psikologis untuk mendapatkan data sensitif seperti OTP. Penipuan juga sering terjadi dalam transaksi jual beli daring lewat media sosial atau *e-commerce*.¹⁰

PT Indonesia Digital Identity (VIDA) melaporkan peningkatan dramatis

⁹ *Ibid.*

¹⁰ Sutarman, *Keamanan Jaringan Komputer*, (Yogyakarta: Andi, 2019), hlm. 112.

sejumlah 1.550 persen dalam kasus penipuan *deepfake* di Indonesia antara tahun 2022 dan 2023. Peningkatan ini terjadi seiring dengan semakin mudahnya akses terhadap teknologi AI dan perangkat lunak manipulasi video. Menurut keterangan Brigjen Himawan Bayu Aji dari Dirlitidsiber Bareskrim Polri, sebelas orang telah menjadi korban penipuan akibat video *deepfake* yang menampilkan pejabat dan tokoh publik. Pelaku yang memproduksi dan menyebarkan video *deepfake* Prabowo Subianto berhasil mengumpulkan keuntungan sebanyak tiga puluh juta rupiah dalam waktu empat bulan.¹¹

Pelaku menggunakan teknologi *deepfake* untuk membuat dan menyebarkan video-video palsu yang menampilkan tokoh-tokoh publik seperti Presiden Prabowo Subianto, Wapres Gibran Rakabuming Raka, serta Menkeu Sri Mulyani. Video tersebut menawarkan bantuan kepada masyarakat dan menyertakan nomor Whatsapp. Masyarakat menghubungi nomor tersebut akan diminta buat mengisi formulir pendaftaran. Mereka akan diminta untuk melakukan transfer sejumlah dana dengan dalih biaya administrasi. Para korban dijanjikan mendapatkan bantuan setelah biaya administrasi dibayarkan. Semua adalah bentuk penipuan.¹²

Masalah hukum pidana seperti meningkatnya pencurian, penipuan, penyebaran berita palsu, bahaya terhadap perlindungan data pribadi, pelanggaran privasi pengguna, dan masalah lain yang dapat memengaruhi dan membahayakan

¹¹ CNN Indonesia, "Kasus Penipuan *Deepfake* di Indonesia Naik 1.550 Persen pada 2023," dipublikasikan pada 2 Februari 2024, diakses pada 13 Juli 2026, <https://www.cnnindonesia.com/teknologi/20240202132557-185-1057508/kasus-penipuan-deepfake-di-ri-naik-1550-persen-pada-2023>.

¹² Detik News, "Polri Ungkap Kasus Penipuan Video *Deepfake* Prabowo Rugikan 11 Korban," dipublikasikan pada 15 April 2024, diakses pada 13 Juli 2026, <https://news.detik.com/berita/d-7276390/polri-ungkap-kasus-penipuan-video-deepfake-prabowo-rugikan-11-korban>.

masyarakat dapat diakibatkan oleh penyalahgunaan *deepfake*.¹³ Oleh sebab itu, hukum pidana harus mengatasi masalah ini karena tidak dapat disangkal bahwa kemajuan teknologi akan berdampak buruk pada bidang lain, termasuk munculnya tindak pidana baru. Keberadaan hukum pidana begitu penting, khususnya dalam rangka menanggulangi penyalahgunaan *deepfake*, sebab tujuan utamanya adalah menjaga kepentingan masyarakat dalam hal keamanan, keharmonisan, dan ketertiban dalam kehidupan bermasyarakat.¹⁴

Indonesia belum memiliki undang-undang khusus yang mengatur *deepfake*. Kekosongan hukum menimbulkan persoalan dalam penegakan hukum, karena Indonesia menjunjung tinggi asas legalitas. Penegakan hukum perlu berlandaskan asas hukum yang berlaku. Salah satunya adalah asas *geen straf zonder schuld* yang menyatakan bahwa tidak ada pidana tanpa kesalahan, sebagai dasar dalam menentukan pertanggungjawaban pidana seseorang atas suatu perbuatan.¹⁵

Tindakan penyalahgunaan teknologi *deepfake* dalam penipuan online menimbulkan permasalahan hukum yang penting dalam konteks Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Meskipun UU ITE belum secara khusus mengatur mengenai manipulasi video *deepfake*, ketentuan dalam Pasal 28 ayat (1) UU ITE dapat dijadikan dasar hukum untuk menindak pelaku. Pasal tersebut melarang setiap orang dengan sengaja dan tanpa hak menyebarkan

¹³ Anye Ramadhani, Tasya Safiranita Ramli, dan Ranti Fauza Mayana, "Pemanfaatan *Artificial Intelligence* pada Fitur *PayLater* Aplikasi Shopee dalam Bidang *E-Commerce* Dikaitkan dengan Data Pribadi Konsumen Berdasarkan Hukum Positif Indonesia," *COMSERVA: Jurnal Penelitian dan Pengabdian Masyarakat*, Vol. 3 No. 4, (Agustus 2023), hlm. 1371.

¹⁴ Ismu Gunadi dan Jonaedi Efendi, *Cepat dan Mudah Memahami Hukum Pidana*, (Jakarta: Kencana Prenadamedia Group, 2016), hlm. 8.

¹⁵ Lukman Hakim, *Asas-Asas Hukum Pidana Buku Ajar Bagi Mahasiswa*, (Yogyakarta: Deepublish, 2020), hlm. 45.

informasi bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik. Penggunaan video *deepfake* sebagai sarana untuk meyakinkan korban agar melakukan transaksi atau menyerahkan sejumlah uang memenuhi unsur penyebaran informasi yang menyesatkan sehingga berpotensi menimbulkan kerugian finansial bagi korban.¹⁶

Penerapan Pasal 28 ayat (1) UU ITE terhadap kasus penyalahgunaan *deepfake* menunjukkan bahwa substansi perbuatan yang dipidana bukan terletak pada teknologi yang digunakan, melainkan pada penyebaran informasi bohong yang menimbulkan kerugian dalam transaksi elektronik. Dengan demikian, meskipun *deepfake* merupakan perkembangan teknologi kecerdasan buatan yang belum diatur secara khusus dalam peraturan perundang-undangan, penggunaannya untuk melakukan penipuan tetap dapat dikenakan sanksi berdasarkan ketentuan tersebut apabila terbukti memenuhi unsur-unsur tindak pidana. Oleh karena itu, Pasal 28 ayat (1) UU ITE memiliki peran penting sebagai dasar hukum dalam memberikan perlindungan kepada masyarakat dari praktik penipuan berbasis teknologi digital yang semakin berkembang.¹⁷

Pembuatan dan penggunaan *deepfake* untuk menipu dapat diinterpretasikan sebagai tindakan manipulasi informasi elektronik dengan tujuan agar korban percaya pada representasi palsu dalam video tersebut. Penegakan hukum dalam kasus ini memerlukan pembuktian adanya unsur kesengajaan pelaku untuk menipu dan adanya kerugian yang dialami korban akibat *deepfake* tersebut. Tantangannya terletak pada identifikasi pelaku dan pembuktian keaslian atau

¹⁶ Maskun, *Kejahatan Siber (Cyber Crime)*, (Jakarta: Kencana, 2018), hlm. 91.

¹⁷ *Ibid.*

kepalsuan video *deepfake* secara forensik digital. Peraturan terkait perlindungan hukum data pribadi harus ditetapkan. Peraturan ini harus mencakup perlindungan terhadap penyalahgunaan serta pemalsuan data pribadi melalui penggunaan teknologi *Artificial Intelligence Deepfake*.¹⁸

Penetapan aturan penggunaan teknologi ini sangat penting untuk dapat melindungi masyarakat, mengatasi kekhawatiran terhadap keamanan data pribadi, dan memberikan perlindungan hukum terhadap eksploitasi informasi melalui teknologi *deepfake*. Berdasarkan uraian latar belakang tersebut, penulis tertarik untuk mengkaji dan mengangkat judul mengenai “**Analisis Yuridis Terhadap Penyalahgunaan AI dalam *Deepfake* Video Penipuan Online Ditinjau dalam Hukum Pidana Indonesia**”.

1.2 Rumusan Masalah

Berdasarkan fenomena pada latar belakang masalah, penulis tertarik untuk membahas rumusan masalah pada penelitian ini mengenai “Bagaimana Analisis Yuridis Terhadap Penyalahgunaan AI dalam *Deepfake* Video Penipuan Online Ditinjau dalam Hukum Pidana Indonesia?”.

1.3 Tujuan Penelitian

Tujuan penelitian ini yakni untuk mengetahui dan menganalisis secara yuridis penyalahgunaan AI dalam *deepfake* video penipuan *online* ditinjau dalam hukum pidana Indonesia.

¹⁸ Budi Agus Riswandi, *Hukum dan Teknologi Informasi: Menghadapi Perkembangan Digitalisasi* (Yogyakarta: FH UII Press, 2021), hlm. 85.

1.4 Manfaat Penelitian

1.4.1 Manfaat Teoritis

Penelitian ini diharapkan dapat memberikan kontribusi dalam pengembangan ilmu hukum, khususnya hukum pidana terkait kajian mengenai penyalahgunaan AI dalam bentuk *deepfake* video sebagai sarana penipuan *online*. Penelitian ini dapat menjadi referensi akademik dalam memahami pertanggungjawaban hukum terhadap perkembangan kejahatan berbasis teknologi digital.

1.4.2 Manfaat Praktis

Penelitian ini diharapkan dapat memberikan pemahaman mengenai aspek hukum penyalahgunaan AI dalam *deepfake* video penipuan online. Hasil penelitian ini diharapkan dapat menjadi bahan pertimbangan dalam penegakan hukum dan pembentukan regulasi di Indonesia.