P-ISSN : 2597-5064
E-ISSN : 2654-8062
DOI : 10.37817/ikraith-humaniora

Analisis Kriminologi Deepfake Melalui Media Sosial Berdasarkan Teori Rational Choice

[1]Andre Herdian, [2]Untung Sumarwan
[1]Program Studi Kriminologi, Universitas Budi Luhur, Jakarta Selatan
[2]Program Studi Kriminologi, Universitas Budi Luhur, Jakarta Selatan

E-mail: [1]2043510060@student.budiluhur.ac.id, [2]untung.sumarwan@budiluhur.ac.id

ABSTRAK

Penelitian ini menganalisis fenomena pencurian identitas yang dilakukan melalui penyalahgunaan teknologi *Artificial Intelligence* (AI) berupa *deepfake* di media sosial yang ditinjau melalui teori *rational choice*. Data yang digunakan dalam penelitian ini diperoleh melalui penyebaran angket kepada narasumber yang menjadi korban dari modus ini. Berdasarkan hasil penelitian yang ditinjau melalui teori *Rational Choice*, pelaku melakukan evaluasi rasional terhadap biaya dan manfaat dengan cara memanfaatkan teknologi *deepfake* yang di kombinasikan dengan anonimitas akun sosial media, sehingga potensi keuntungan dinilai lebih besar dibandingkan risikonya. Penelitian juga menemukan dampak psikologis utama yang dialami korban adalah perasaan malu dan terganggu yang memengaruhi kehidupan sosial serta emosional mereka. Analisis lebih lanjut menunjukkan bahwa teknologi ini dimanfaatkan oleh pelaku untuk memperoleh keuntungan finansial, sementara minimnya kesadaran masyarakat terhadap risiko keamanan digital menjadi faktor pendukung keberhasilan kejahatan ini. Hasil penelitian ini juga menyoroti perlunya upaya peningkatan literasi digital dan penguatan regulasi teknologi untuk meminimalkan kejahatan berbasis *deepfake* pada media sosial.

Kata Kunci: ***Pencurian Identitas, Deepfake, Kriminologi, Teori Rational Choice.***

ABSTRACT

This study analyzes the phenomenon of identity theft through the misuse of Artificial Intelligence (AI) technology in the form of deepfake on social media, examined through the lens of Rational Choice theory. Data for this research were collected through surveys distributed to respondents who had been victims of this modus operandi. Based on the findings analyzed using Rational Choice theory, perpetrators conducted a rational evaluation of costs and benefits by utilizing deepfake technology combined with the anonymity provided by social media accounts, making the potential gains outweigh the risks. The study also revealed that the primary psychological impact experienced by victims was feelings of shame and distress, which significantly affected their social and emotional well-being. Further analysis demonstrated that this technology is exploited by perpetrators to achieve financial gain, while the public's lack of awareness about digital security risks serves as a supporting factor for the success of such crimes. These findings highlight the urgent need for efforts to improve digital literacy and strengthen technology regulations to minimize deepfake-based crimes on social media.

Keywords: Identity Theft, Deepfake, Criminology, Rational Choice Theory.

DOI : 10.37817/ikraith-humaniora
P-ISSN : 2597-5064
E-ISSN : 2654-8062

1. PENDAHULUAN

Perkembangan teknologi kecerdasan buatan atau yang dikenal sebagai *Artificial Intelligence* telah membawa dampak yang signifikan dalam berbagai aspek kehidupan manusia saat ini, mulai dari komunikasi, hiburan, hingga keamanan. Salah satu bentuk inovasi yang paling kontroversial dalam teknologi *Artificial Intelligence* ini adalah *deepfake*, yaitu kemampuan untuk menciptakan gambar, video, atau audio yang menyerupai seorang individu dan terkesan sangat nyata namun pada realitanya hal tersebut hanyalah buatan (Kurniarullah et al, 2024). Teknologi ini dibuat menggunakan algoritma berbasis machine learning untuk mempelajari data visual maupun audio seseorang dan kemudian menghasilkan replika yang cenderung sangat realistis. *Deepfake* pada mulanya menawarkan peluang besar untuk inovasi dalam industri kreatif, pendidikan dan hiburan. Namun, hingga saat ini penggunaannya sering kali disalahgunakan untuk kejahatan dunia maya yang semakin kompleks, seperti pencurian identitas, manipulasi informasi dan serangan terhadap privasi individu (Wibowo et al, 2023).

Pencurian identitas melalui *deepfake* di media sosial kini menjadi salah satu bentuk kejahatan dunia maya yang berkembang pesat seiring dengan meningkatnya adopsi platform digital dalam kehidupan sehari-hari. Kejahatan ini pada umumnya memanfaatkan teknologi *deepfake* untuk menciptakan konten palsu yang menyerupai wajah, suara hingga informasi pribadi korban dengan tingkat akurasi yang tinggi sehingga sulit dibedakan dari aslinya (Novera & Fitri, 2024). Konten palsu tersebut biasanya mengacu pada narasi yang negatif dan merugikan korban, baik secara sosial, psikologis, maupun finansial. Teknologi *deepfake* umumnya memungkinkan pelaku untuk dengan mudah menciptakan video, foto hingga rekaman suara yang tampak nyata. Dalam banyak kasus, pelaku menggunakan konten ini untuk menipu pihak ketiga dengan berpura-pura menjadi korban. Misalnya, pelaku dapat memanipulasi suara korban untuk meminta uang kepada kerabatnya (*voice phising*), hingga membuat video palsu seolah korban berada dalam situasi yang tidak baik yang kemudian digunakan untuk pemerasan kepada anggota keluarga korban (Gupta & Kumar, 2020). Disisi lain, penyebaran konten palsu ini juga sering kali dimanfaatkan untuk menyebarkan hoaks atau propaganda, yang dapat menimbulkan kekacauan sosial dan kerusakan reputasi korban (Amelia et al, 2024).

Dalam konteks kriminologi, pencurian identitas berbasis *deepfake* mencerminkan ancaman baru dalam kejahatan dunia maya yang semakin sulit diatasi. Kejahatan ini umumnya melibatkan manipulasi teknologi untuk menciptakan konten palsu, seperti video atau audio yang menyerupai wajah, suara, atau data pribadi korban, dengan tujuan untuk menipu pihak lain Kasus-kasus pencurian identitas semacam ini sering kali dimanfaatkan untuk melakukan tindakan kriminal, seperti penipuan finansial, pemerasan hingga penyebaran informasi palsu yang merugikan korban secara langsung (Nurafifah et al, 2024)..

P-ISSN : 2597-5064
E-ISSN : 2654-8062
DOI : 10.37817/ikraith-humaniora

Pencurian identitas berbasis *deepfake* menunjukkan bagaimana pelaku menggunakan celah hukum dan kekurangan regulasi untuk menjalankan aksinya. Sifat canggih teknologi ini, yang mampu menciptakan replika digital hampir sempurna dari korban, membuat pelaku lebih mudah mengelabui pihak lain. Misalnya, dengan memalsukan suara korban, pelaku dapat meyakinkan kerabat atau rekan kerja korban untuk mentransfer sejumlah uang dengan modus pinjaman. Dalam kasus lain, manipulasi wajah korban digunakan untuk menciptakan video yang merusak reputasi mereka yang salah satunya mengarah pada pornografi dan sering kali hal ini dibuat dengan tujuan pemerasan (Jufri & Kurnia, 2021).

Minimnya literasi digital masyarakat tentu dapat memperburuk situasi ini. Banyak individu yang tidak menyadari bahwa data pribadi yang mereka unggah di media sosial, seperti foto atau video, dapat menjadi bahan utama bagi pelaku untuk menciptakan *deepfake*. Korban sering kali tidak menyadari adanya penyalahgunaan identitas mereka hingga dampaknya telah terjadi, seperti hilangnya uang atau kehancuran reputasi (Kurniarullah et al, 2024). Dampak pencurian identitas berbasis *deepfake* sangat luas, tidak hanya secara finansial tetapi juga sosial dan psikologis. Korban sering kali mengalami tekanan emosional akibat reputasi yang tercoreng atau kehilangan kepercayaan dari orang-orang di sekitar mereka. Trauma ini dapat berlangsung lama, terutama jika konten palsu yang tersebar tidak dapat dihapus dari internet. Selain itu, sifat permanen dunia digital juga dapat memperburuk situasi, karena konten palsu dapat dengan mudah muncul kembali atau digunakan ulang oleh pihak lain (Novera & Fitri, 2024).

Untuk menanggulangi ancaman ini, diperlukan langkah strategis yang lebih terfokus pada pengendalian pencurian identitas melalui *deepfake*. Regulasi yang tegas perlu diberlakukan untuk membatasi akses dan penggunaan teknologi ini, khususnya oleh pihak yang tidak bertanggung jawab. Di samping itu, pengembangan teknologi pendeteksi *deepfake* dan edukasi masyarakat tentang risiko penyalahgunaan data pribadi di media sosial perlu menjadi prioritas utama. Pengambilan langkah ini diharapkan dapat meminimalisir ancaman pencurian identitas berbasis *deepfake* yang dapat merugikan masyarakat.

2. LANDASAN TEORI

2.1 *Deepfake*

Deepfake merupakan teknologi yang memanfaatkan kecerdasan buatan, khususnya deep learning, untuk membuat atau mengubah konten digital (seperti gambar, video, atau audio) dengan tingkat akurasi tinggi sehingga sulit dibedakan dari yang asli. Istilah *deepfake* berasal dari dua kata, "deep" yang merujuk pada metode pembelajaran mesin deep learning dan "fake" yang berarti palsu atau tiruan. Menurut Kietzmann et al. (2020), *deepfake* merujuk pada manipulasi visual dan audio menggunakan algoritma kecerdasan buatan yang dapat memalsukan identitas individu, misalnya dengan mengganti wajah atau suara seseorang dengan gambar atau suara yang diproduksi secara sintetis.

DOI : 10.37817/ikraith-humaniora
P-ISSN : 2597-5064
E-ISSN : 2654-8062

2.2 Pencurian Identitas

Pencurian identitas (id*entity theft*) adalah suatu tindakan di mana pelaku mengambil dan menggunakan informasi pribadi seseorang dengan tujuan untuk menipu atau merugikan orang lain, terutama dalam hal keuangan. Definisi ini mencakup berbagai bentuk kejahatan yang melibatkan penyalahgunaan data pribadi seperti nomor identitas, data keuangan, kata sandi dan informasi sensitif lainnya yang dapat digunakan untuk memperoleh keuntungan secara ilegal. Menurut Guedes et al (2022) pencurian identitas dapat terjadi dalam berbagai cara, termasuk pemalsuan dokumen, penyalahgunaan informasi kartu kredit, hingga penggunaan identitas korban untuk membuka rekening bank atau melakukan transaksi keuangan.

2.3 *Rational Choice Theory*

Rational Choice Theory yang diperkenalkan oleh Clarke & Cornish pada tahun 1985. Teori ini berasumsi bahwa pelaku kriminal membuat keputusan secara rasional berdasarkan analisis biaya dan manfaat dari tindakan mereka (Zhao et al, 2020). Teori ini memberikan gambaran terkait bagaimana individu melakukan pertimbangan risiko dan keuntungan sebelum melakukan tindakan kriminal. Dalam konteks pencurian identitas melalui *deepfake*, pelaku sering kali terdorong oleh motif ekonomi, di mana potensi keuntungan finansial dari pemerasan dan penipuan dinilai lebih besar dibandingkan risiko yang mungkin dihadapi. Keputusan untuk melakukan pencurian identitas melalui *deepfake* pada umumnya juga didasari oleh kalkulasi pragmatis, seperti mempertimbangkan kemajuan teknologi, tingkat kerentanan korban dan strategi untuk menghindari deteksi oleh platform atau pihak berwenang (Lenine, 2020). Dalam penelitian ini, *Rational Choice Theory* digunakan untuk memberikan pemahaman tentang bagaimana pelaku merancang strategi untuk memanfaatkan teknologi *deepfake* dan media sosial sebagai sarana untuk mencapai tujuan mereka.

3. METODOLOGI

Penelitian ini merupakan penelitian yang bersifat kualitatif yang mana data yang digunakan berupa hasil penyebaran angket yang dilakukan dengan mengeksplorasi terkait pengalaman korban pencurian identitas berbasis *deepfake* dan bagaimana dampak dari peristiwa tersebut dalam mempengaruhi kehidupannya. Analisis ini dilakukan dengan menekankan analisis yang berdasarkan pada hasil penyebaran angket (*question box*) yang dianalisis dengan menggunakan pertanyaan yang mampu memuat informasi yang diperlukan untuk meneliti lebih dalam terkait ruang lingkup dalam penelitian ini.

Dalam penelitian ini, metode kualitatif digunakan untuk menggambarkan pengalaman dan dampak yang dialami oleh korban akibat dari pencurian identitas. Metode ini melibatkan analisis data hasil pengisian *question box* yang diisi oleh para pelaku dan korban dengan menggunakan pertanyaan-pertanyaan yang telah disiapkan sebelumnya. Penelitian ini diharapkan mampu menyajikan temuan-temuan terbaru berdasarkan hasil identifikasi dalam analisis data hasil pengisian *question*

P-ISSN : 2597-5064
E-ISSN : 2654-8062
DOI : 10.37817/ikraith-humaniora

box dan selanjutnya dibandingkan dengan hasil penelitian yang sudah dilakukan sebelumnya.

Tujuan utama penelitian ini adalah untuk menyoroti motivasi yang dimiliki oleh para pelaku dan bagaimana dampak negatif yang ditimbulkan oleh ancaman pencurian identitas bagi korban serta sejauh mana pengalaman pencurian identitas ini mampu merubah hidup korban kearah negatif dan merugikan. Berdasarkan penjelasan diatas, metode penelitian yang berbentuk kualitatif dan bersifat eksploratif ini dianggap sangat sesuai untuk diterapkan karena memberikan kesempatan kepada para responden untuk menjelaskan dan berkomunikasi secara mendalam namun tetap ada privasi terkait pengalaman buruknya.

Pemilihan penyebaran *question box* dibandingkan kuisioner ini didasari oleh asumsi bahwa peneliti mungkin lebih mampu mendapatkan pemahaman yang lebih baik apabila pengumpulan data dilakukan dengan menggunakan *question box* yang dapat diisi dengan tulisan-tulisan penjelasan dari korban dibandingkan dengan hanya menjawab pertanyaan singkat (Kuisioner). Proses pengambilan data melalui *question box* ini diharapkan dapat membuat penelitian ini menjadi lebih komprehensif dan memperoleh wawasan yang lebih mendalam melalui interaksi dengan responden.

Teknik analisis data yang digunakan dalam penelitian ini merupakan analisis tematik. Menurut Lochmiller (2021) analisis tematik adalah sebuah metode dalam penelitian kualitatif yang digunakan untuk mengidentifikasi, menganalisis, dan menggambarkan pola-pola tematik atau tema-tema utama dalam data kualitatif. Metode ini membantu peneliti untuk memahami makna, pola dan struktur yang muncul dalam wawancara, teks atau data kualitatif lainnya. Proses analisis tematik melibatkan beberapa tahap, seperti transkripsi data, pengkodean, pengelompokan, dan interpretasi. Tujuan dari tahapan-tahapan pada proses tersebut adalah untuk mengidentifikasi tema-tema utama yang muncul dalam data, mengorganisasi informasi menjadi kategori-kategori atau tema-tema dan memahami bagaimana tema-tema tersebut berhubungan satu sama lain. Analisis tematik dapat digunakan untuk menjawab pertanyaan-pertanyaan penelitian, mengembangkan teori, atau menggambarkan fenomena yang terjadi dalam konteks penelitian kualitatif. Metode ini membantu menguraikan data kualitatif menjadi struktur yang lebih teratur dan dapat digunakan untuk menyusun temuan-temuan yang relevan dalam laporan penelitian.

4. HASIL DAN PEMBAHASAN

4.1 Hasil Penelitian

Berdasarkan hasil penyebaran angket berbentuk *question box* yang telah dilakukan, diperoleh narasumber yang diantaranya merupakan korban pelaku pencurian identitas. Hasil penelitian ini kemudian mengungkapkan bahwa terdapat dampak yang mendalam yang dialami oleh korban pencurian identitas melalui teknologi *deepfake*. Berdasarkan jawaban dari ketiga korban, ditemukan bahwa dampak psikologis menjadi salah satu aspek yang paling signifikan dari peristiwa ini. Dampak yang paling dirasakan

DOI : 10.37817/ikraith-humaniora
P-ISSN : 2597-5064
E-ISSN : 2654-8062

oleh korban adalah perasaan malu. Sarah (nama samaran), mengungkapkan bahwa ia merasa sangat malu ketika mengetahui bahwa rekannya tertipu modus pinjam uang pada aplikasi Instagram: "*Awalnya, teman saya tiba-tiba kirim pesan whatsapp ke saya dan tanya apakah uangnya sudah ada? Saya sempat bingung dan bertanya, uang apa? Karena saya tidak merasa ada sangkutan uang dengan teman saya ini*" tuturnya. Setelah di telusuri kebenarannya, ternyata baru terungkap bahwa seseorang telah menyamar sebagai dirinya dan menggunakan Instagram untuk meminjam uang. Sarah awalnya tidak mengerti kenapa temannya tiba-tiba bertanya tentang uang, padahal ia tidak merasa ada urusan keuangan dengan teman tersebut. Namun, ketika ia menggali lebih dalam, terungkap bahwa pelaku penipuan ini telah menggunakan *voice note* yang suaranya sangat mirip dengan suara Sarah.

Dalam *voice note* tersebut, orang yang menyamar sebagai Sarah menjelaskan bahwa akun WhatsApp-nya sedang bermasalah, sehingga ia tidak bisa menghubungi teman-temannya lewat WhatsApp dan memilih untuk mengirim pesan melalui Instagram. Tentu saja, teman-teman Sarah yang menerima pesan tersebut merasa yakin bahwa itu adalah dirinya, karena suara dalam *voice note* dan foto profil pada Instagram tersebut jelas merupakan Sarah. Pelaku dalam hal ini memanfaatkan teknologi *deepfake* untuk menciptakan kemiripan pada suara untuk menipu teman-teman Sarah agar mereka tidak curiga dan langsung mengirimkan uang yang diminta. Begitu mengetahui hal ini, Sarah merasa sangat malu dan juga sangat terganggu karena identitasnya telah disalahgunakan dengan cara yang sangat merugikan orang lain dan juga merugikan dirinya sendiri tanpa sepengetahuannya.

Selain Sarah yang mengalami kerugian materil, salah satu narasumber yaitu Dimas (nama samaran) juga merasakan hal yang sama. Dimas yang juga mengalami kerugian materil akibat dari modus yang sama namun dengan cara yang berbeda. Dalam kasus Dimas, cara yang digunakan oleh pelaku adalah melakukan video call dengan menggunakan video rekaman yang seolah-olah itu merupakan Dimas; "*Saya pernah mengalami modus serupa dimana wajah saya digunakan untuk menipu orang lain melalui video call."* Disini korban menceritakan pengalamannya menjadi sasaran pencurian identitas menggunakan rekaman video palsu yang seolah-olah menunjukkan dirinya. Dalam video tersebut, pelaku berpura-pura sebagai korban yang membutuhkan bantuan uang karena dompet tertinggal. Pelaku menghubungi teman-teman korban melalui video call WhatsApp, menggunakan rekaman yang tampak meyakinkan. Karena percaya, teman-teman korban mentransfer uang ke pelaku melalui *e-wallet* dengan total kerugian mencapai lima juta rupiah. Korban sangat terkejut, bingung dan merasa dirugikan karena identitasnya telah disalahgunakan untuk melakukan penipuan. Hal ini tentu sangat merugikan korban karena bagaimanapun korban yang harus menanggung kerugian tersebut.

Di sisi lain, terdapat beberapa pernyataan yang diberikan oleh para

P-ISSN : 2597-5064
E-ISSN : 2654-8062
DOI : 10.37817/ikraith-humaniora

pelaku yang memberikan gambaran tentang motivasi dan modus operandi mereka. Motivasi utama pelaku menurut Rudi (nama samara) sebagai pelaku tentu adalah keuntungan finansial. Rudi, mengungkapkan bahwa ia awalnya membuat video *deepfake* untuk mengisi waktu luang dan sebagai hiburan untuk dikirim ke teman-temannya dalam konteks video lucu, tetapi karena respon teman-temannya yang merasa bahwa video itu sangat mirip dengan realitanya, maka Rudi kemudian melihat peluang untuk menghasilkan uang dari cara ini; "*Deepfake ini menurut saya salah satu penipuan yang paling tinggi potensi keberhasilannya karena saya bisa berpura-pura bahwa akun yang saya gunakan merupakan korban."* Pernyataan ini menunjukkan bagaimana pelaku kejahatan memanfaatkan teknologi seperti *deepfake* untuk melakukan penipuan dengan menyalahgunakan identitas korban. Pelaku umumnya memulai aksinya dengan mengumpulkan data dari media sosial korban, seperti foto dan rekaman suara, untuk menciptakan video palsu yang tampak meyakinkan. Video ini kemudian digunakan untuk menghubungi orang-orang terdekat korban, seperti teman atau keluarga, melalui platform komunikasi dan berpura-pura membutuhkan bantuan keuangan. Sasaran utama para pelaku umumnya adalah individu yang aktif di media sosial namun cenderung gagap teknologi; "*Biasanya saya sih carinya yang usianya sudah 30 tahunan, karena mereka awam soal video palsu gini dan biasanya percaya saja*."

4.2 Pembahasan

Hasil penelitian yang mengungkapkan dampak signifikan dari pencurian identitas melalui teknologi *deepfake* menunjukkan adanya kerugian materiil dan psikologis yang dialami oleh korban, seperti Sarah dan Dimas. Dari sisi pelaku, motivasi utama mereka adalah keuntungan finansial, dimana hal ini tercermin dalam keputusan rasional yang mereka buat (Zhao *et al*, 2021). Berdasarkan teori *Rational Choice*, pelaku membuat keputusan untuk memanfaatkan teknologi *deepfake* setelah melihat respons positif dari teman-temannya terhadap video yang mirip dengan identitas orang lain. Dalam kerangka *Rational Choice*, pelaku menilai bahwa potensi keuntungan yang dapat diperoleh dari penipuan ini lebih besar dibandingkan dengan risikonya, karena *deepfake* memungkinkan mereka untuk meniru identitas korban dengan sangat meyakinkan (Lenine, 2020). Dalam hal ini, pelaku melakukan evaluasi rasional mengenai biaya dan manfaat dari tindakan kriminal tersebut.

Berdasarkan hasil penelitian juga ditemukan dampak psikologis yang paling signifikan yang dirasakan oleh korban adalah perasaan malu. Sarah, salah satu korban, merasa sangat terganggu setelah mengetahui bahwa temannya tertipu oleh pelaku yang menyamar menggunakan suaranya di aplikasi Instagram. Modus operandi yang digunakan oleh pelaku adalah dengan menyamar sebagai Sarah melalui *voice note* yang sangat mirip dengan suara aslinya, sehingga teman-teman Sarah merasa yakin dan akhirnya mengirimkan uang yang diminta. Dampak psikologis yang dirasakan oleh korban, terutama rasa

malu dan terkejut atas penyalahgunaan identitasnya, sangat memengaruhi kehidupan sosial dan emosional korban setelah kejadian tersebut (Kurniarullah *et al*, 2024). Selain itu, Dimas juga mengalami hal serupa, namun dengan modus yang berbeda, yakni dengan menggunakan rekaman video dirinya melalui video call. Dalam hal ini, pelaku memanfaatkan kemiripan wajah Dimas dan menciptakan narasi palsu mengenai keadaan darurat untuk meminta uang.

Secara keseluruhan, analisis kriminologis terhadap kasus ini menunjukkan bahwa penggunaan teknologi *deepfake* sebagai sarana untuk melakukan penipuan sangat dipengaruhi oleh faktor-faktor seperti tekanan untuk memperoleh keuntungan secara instan serta minimnya pengetahuan yang dimiliki oleh kebanyakan orang dengan usia tertentu.

5. KESIMPULAN

Penelitian ini menyimpulkan bahwa pencurian identitas menggunakan teknologi *deepfake* dapat menimbulkan dampak serius pada individu, baik secara psikologis maupun ekonomi atau dalam hal ini adalah kerugian finansial. Disisi lain, pelaku justru termotivasi oleh keuntungan finansial, dengan memanfaatkan rendahnya literasi digital masyarakat, dimana target utama biasanya adalah individu yang dianggap awam terhadap teknologi *deepfake*.

Sebagai langkah pencegahan terjadinya penipuan ini di masa depan, pemerintah perlu melakukan peningkatan literasi digital masyarakat. Hal ini dapat dilakukan dengan cara memfasilitasi program edukasi yang dilakukan secara masif untuk meningkatkan kesadaran tentang risiko *deepfake* dan cara mengenalinya. Pemerintah juga perlu mempercepat implementasi regulasi yang mengatur penggunaan teknologi ini, termasuk hukuman yang lebih tegas bagi pelaku kejahatan berbasis *deepfake*.

DAFTAR PUSTAKA

Amelia, Y. F., Kaimuddin, A., & Ashsyarofi, H. L. (2024). Pertanggungjawaban Pidana Pelaku Terhadap Korban Penyalahgunaan Artificial Intelligence Deepfake Menurut Hukum Positif Indonesia. *Dinamika*, 30(1), 9675-9691.

Dearden, T. E., & Parti, K. (2021). Cybercrime, differential association, and self-control: Knowledge transmission through online social learning. *American Journal of Criminal Justice*, 46(6), 935-955.

Guedes, I., Martins, M., & Cardoso, C. S. (2022). Exploring the determinants of victimization and fear of online identity theft: An empirical study. *Security Journal*, 1.

Gupta, C. M., & Kumar, D. (2020). Identity theft: A small step towards big financial crimes. *Journal of Financial Crime*, 27(3), 897-910.

Jufri, M. A. A., & Putra, A. K. (2021). Aspek hukum internasional dalam pemanfaatan deepfake technology terhadap perlindungan data pribadi. *Uti*

Possidetis: Journal of International Law, 2(1), 31-57.

Kietzmann, J., Lee, L. W., McCarthy, I. P., & Kietzmann, T. C. (2020). Deepfakes: Trick or treat?. *Business Horizons*, 63(2), 135-146.

Kurniarullah, M. R., Nabila, T., Khalidy, A., Tan, V. J., & Widiyani, H. (2024). Tinjauan kriminologi terhadap penyalahgunaan artificial intelligence: Deepfake pornografi dan pencurian data pribadi. *Jurnal Ilmiah Wahana Pendidikan*, 10(10), 534-547.

Lenine, E. (2020). The pulse-like nature of decisions in rational choice theory. *Rationality and Society*, 32(4), 485-508.

Novera, O. (2024). Analisis pengaturan hukum pidana terhadap penyalahgunaan teknologi manipulasi gambar (deepfake) dalam penyebaran konten pornografi melalui akun media sosial. *El-Faqih: Jurnal Pemikiran dan Hukum Islam*, 10(2), 460-474.

Nurafifah, I., Dewi, S. B. R., & Aprilianti, K. L. (2024). Jelajah media sosial dengan akun alter dan perkembangan teknologi artificial intelligence. *Deliberatio: Jurnal Mahasiswa Komunikasi*, 4(1), 129-141.

Russell, S., & Norvig, P. (2021). *Artificial intelligence: A modern approach (4th ed.)*. Pearson.

Wibowo, A., Wangsajaya, Y., & Surahmat, A. (2023). *Pemolisian digital dengan artificial intelligence*. PT. RajaGrafindo Persada-Rajawali Pers.

Zhao, J., Wang, X., Zhang, H., & Zhao, R. (2021). Rational choice theory applied to an explanation of juvenile offender decision making in the Chinese setting. *International Journal of Offender Therapy and Comparative Criminology*, 65(4), 434-457.