



Analisis Normatif terhadap Penyebaran *Deepfake* Sebagai Bentuk Kejahatan Siber di Indonesia

Fabrizio Richardo Marvil Wanggai^{1*}, Made Sugi Hartono², Ni Putu Ega Parwati³,

^{1,2,3} Universitas Pendidikan Ganesha

Email: fabrizio@student.undiksha.ac.id, sugi.hartono@undiksha.ac.id, ni.putu.ega.parwati@undiksha.ac.id

Korespondensi penulis: fabrizio@student.undiksha.ac.id

Abstract. *The rapid development of artificial intelligence technology, particularly deepfake, poses significant challenges to legal protection due to its potential misuse for identity manipulation, defamation, and other cybercrimes. This phenomenon highlights a gap between technological advancement and the readiness of legal regulations in Indonesia. This study aims to analyze forms of deepfake misuse and to assess the effectiveness of existing legal frameworks in providing legal protection and certainty. The research employs a normative legal method using statutory and conceptual approaches by examining legislation, legal doctrines, and relevant scholarly literature. The findings indicate that Indonesian positive law does not yet specifically regulate deepfake technology, resulting in law enforcement relying on general provisions of criminal law and the Electronic Information and Transactions Law. The implications of this study emphasize the urgency of regulatory reform and the formulation of adaptive legal policies to address digital technological developments in order to ensure legal protection and justice for society.*

Keywords: *Deepfake, Cybercrime, Criminal Law, Digital Technology, Legal Protection.*

Abstrak. Perkembangan teknologi kecerdasan buatan, khususnya *deepfake*, menimbulkan tantangan serius dalam perlindungan hukum karena potensinya disalahgunakan untuk manipulasi identitas, pencemaran nama baik, dan kejahatan siber lainnya. Fenomena ini menunjukkan adanya kesenjangan antara kemajuan teknologi dan kesiapan regulasi hukum di Indonesia. Penelitian ini bertujuan untuk menganalisis bentuk penyalahgunaan teknologi *deepfake* serta menilai efektivitas pengaturan hukum yang berlaku dalam memberikan perlindungan dan kepastian hukum. Metode penelitian yang digunakan adalah penelitian hukum normatif dengan pendekatan perundang-undangan dan konseptual, melalui penelaahan terhadap peraturan perundang-undangan, doktrin hukum, dan literatur ilmiah yang relevan. Hasil penelitian menunjukkan bahwa pengaturan hukum positif di Indonesia belum secara spesifik mengatur *deepfake*, sehingga penegakan hukum masih bergantung pada norma umum dalam hukum pidana dan Undang-Undang Informasi dan Transaksi Elektronik. Implikasi penelitian ini menekankan pentingnya pembaruan regulasi dan perumusan kebijakan hukum yang adaptif terhadap perkembangan teknologi digital guna menjamin perlindungan hukum dan keadilan bagi masyarakat.

Kata kunci: *Deepfake, Kejahatan Siber, Hukum Pidana, Teknologi Digital, Perlindungan Hukum.*

1. LATAR BELAKANG

Perkembangan teknologi informasi dan komunikasi di era digital telah membawa transformasi besar dalam berbagai aspek kehidupan masyarakat, termasuk dalam bidang hukum. Digitalisasi yang semakin masif tidak hanya menghadirkan kemudahan dalam mengakses dan menyebarkan informasi, tetapi juga membuka ruang bagi lahirnya berbagai bentuk kejahatan baru yang berbasis teknologi. Kejahatan siber (*cyber crime*) menjadi salah satu konsekuensi dari kemajuan tersebut, dengan karakteristik yang lintas batas, sulit dilacak, serta terus berkembang seiring dengan inovasi teknologi digital (Susanto, 2021).

Salah satu fenomena teknologi yang saat ini menimbulkan perhatian serius adalah penggunaan teknologi *deepfake*. *Deepfake* merupakan teknologi berbasis kecerdasan buatan (*artificial intelligence*) dan *machine learning* yang memungkinkan manipulasi wajah, suara, dan ekspresi seseorang dalam bentuk gambar atau video sehingga tampak seolah-olah autentik. Kemampuan teknologi ini dalam menciptakan konten visual dan audio yang sangat realistis menjadikan *deepfake* sulit dibedakan dari konten asli oleh masyarakat awam (Kietzmann et al., 2020).

Pada awal kemunculannya, teknologi *deepfake* dikembangkan untuk kepentingan positif, seperti industri hiburan, pengembangan teknologi visual, dan pendidikan. Namun, dalam perkembangannya, teknologi ini justru lebih banyak disalahgunakan untuk kepentingan yang merugikan. Penyebaran video atau audio *deepfake* kerap digunakan untuk menyebarkan informasi palsu, melakukan pencemaran nama baik, penipuan digital, pemerasan, hingga eksploitasi seksual berbasis daring, khususnya terhadap perempuan dan figur publik (Citron & Chesney, 2019).

Penyebaran *deepfake* sebagai konten manipulatif tidak hanya berdampak pada individu sebagai korban, tetapi juga berpotensi menimbulkan dampak sosial yang lebih luas. Kepercayaan publik terhadap informasi digital dapat menurun secara signifikan ketika masyarakat tidak lagi mampu membedakan antara fakta dan rekayasa teknologi. Kondisi ini berbahaya karena dapat memicu disinformasi massal, konflik sosial, serta mengancam stabilitas demokrasi, terutama apabila *deepfake* digunakan dalam konteks politik dan kepentingan kekuasaan (Wardle & Derakhshan, 2018).

Di Indonesia, fenomena penyalahgunaan teknologi digital menunjukkan tren yang terus meningkat seiring dengan tingginya penetrasi internet dan penggunaan media sosial. Masyarakat Indonesia yang aktif dalam ruang digital menjadi sasaran empuk bagi berbagai bentuk kejahatan siber, termasuk penyebaran konten manipulatif. Namun demikian, kesadaran hukum masyarakat terhadap bahaya *deepfake* masih relatif rendah, sehingga korban sering kali tidak mengetahui mekanisme perlindungan hukum yang dapat ditempuh ketika mengalami kerugian akibat konten tersebut (Sari & Nugroho, 2022).

Dari perspektif hukum, penyebaran *deepfake* menimbulkan persoalan normatif yang kompleks. Hingga saat ini, sistem hukum Indonesia belum memiliki regulasi yang secara khusus dan eksplisit mengatur mengenai *deepfake* sebagai bentuk kejahatan siber. Pengaturan yang ada masih bersifat umum dan tersebar dalam beberapa peraturan perundang-undangan, seperti Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta perubahannya, Kitab Undang-Undang Hukum Pidana, serta peraturan terkait

perlindungan data pribadi. Kondisi ini menimbulkan ketidakjelasan dalam menentukan kualifikasi tindak pidana serta pertanggungjawaban hukum pelaku penyebaran *deepfake* (Makarim, 2020).

Ketiadaan pengaturan khusus tersebut berpotensi menimbulkan kekosongan hukum (*rechtsvacuum*) maupun ketidakpastian hukum (*legal uncertainty*) dalam praktik penegakan hukum. Aparat penegak hukum sering kali harus melakukan penafsiran ekstensif terhadap norma yang ada untuk menjerat pelaku, yang pada akhirnya dapat menimbulkan perbedaan penerapan hukum antar kasus. Situasi ini menunjukkan bahwa hukum positif Indonesia masih menghadapi tantangan besar dalam mengimbangi perkembangan teknologi yang bergerak sangat cepat (Rahardjo, 2019).

Selain itu, penyebaran *deepfake* juga berkaitan erat dengan perlindungan hak asasi manusia, khususnya hak atas privasi, kehormatan, dan martabat manusia. Ketika wajah atau suara seseorang dimanipulasi tanpa persetujuan dan disebarluaskan secara luas, maka terdapat pelanggaran serius terhadap hak personal individu. Oleh karena itu, negara memiliki kewajiban untuk menghadirkan instrumen hukum yang mampu memberikan perlindungan efektif serta menjamin keadilan bagi korban kejahatan berbasis *deepfake* (Asshiddiqie, 2018).

Berdasarkan uraian tersebut, dapat dipahami bahwa penyebaran *deepfake* bukan sekadar persoalan teknologi, melainkan juga persoalan hukum yang memerlukan perhatian serius. Diperlukan kajian normatif yang komprehensif untuk menelaah sejauh mana peraturan perundang-undangan di Indonesia mampu mengakomodasi dan mengantisipasi penyebaran *deepfake* sebagai bentuk kejahatan siber. Melalui analisis normatif ini, diharapkan dapat ditemukan landasan konseptual yang kuat guna memperkuat sistem hukum nasional dalam menghadapi tantangan kejahatan digital di masa depan.

2. KAJIAN TEORITIS

Kajian teoritis dalam penelitian ini bertumpu pada pemahaman mengenai kejahatan siber sebagai fenomena hukum yang berkembang seiring dengan kemajuan teknologi informasi. Kejahatan siber dipahami sebagai perbuatan melawan hukum yang dilakukan dengan memanfaatkan sistem elektronik dan jaringan digital, baik sebagai sarana maupun sebagai objek kejahatan. Dalam perspektif hukum pidana modern, kejahatan siber memiliki karakteristik lintas batas, berkecepatan tinggi, dan bersifat anonim, sehingga menuntut pendekatan hukum yang adaptif dan progresif (Wall, 2017).

Perkembangan kecerdasan buatan turut melahirkan bentuk kejahatan siber baru yang bersifat lebih kompleks, salah satunya melalui teknologi *deepfake*. *Deepfake* dipahami sebagai teknologi berbasis *deep learning* yang mampu merekayasa visual dan audio seseorang sehingga tampak autentik dan sulit dibedakan dari konten asli. Secara teoretis, keberadaan *deepfake* menantang konsep kebenaran dan keaslian informasi dalam ruang digital, karena teknologi ini memungkinkan penciptaan realitas semu yang dapat menyesatkan publik secara sistematis (Kietzmann et al., 2020).

Dalam kerangka teori perlindungan hukum, negara memiliki kewajiban untuk menjamin hak-hak warga negara dari setiap bentuk penyalahgunaan teknologi. Perlindungan hukum tidak hanya dimaknai sebagai upaya represif melalui pemidanaan pelaku, tetapi juga sebagai langkah preventif dengan menyediakan regulasi yang jelas dan responsif terhadap perkembangan teknologi. Ketika hukum tertinggal dari realitas sosial, maka risiko pelanggaran hak asasi manusia menjadi semakin besar, terutama bagi individu yang menjadi korban kejahatan siber berbasis konten manipulatif seperti *deepfake* (Hadjon, 2015).

Sejumlah penelitian terdahulu menunjukkan bahwa *deepfake* memiliki dampak serius terhadap hak privasi, kehormatan, dan keamanan individu. Chesney dan Citron (2019) menegaskan bahwa *deepfake* berpotensi digunakan sebagai alat pencemaran nama baik dan manipulasi politik yang sulit ditangkal oleh mekanisme hukum konvensional. Temuan ini memperlihatkan bahwa kerugian yang ditimbulkan oleh *deepfake* tidak hanya bersifat individual, tetapi juga dapat mengancam kepentingan publik dan demokrasi.

Penelitian lain yang dilakukan oleh Floridi et al. (2018) menyoroti lemahnya kesiapan hukum dalam menghadapi tantangan etis dan yuridis dari kecerdasan buatan. Studi tersebut menyimpulkan bahwa regulasi teknologi cenderung bersifat reaktif dan baru disusun setelah dampak negatif muncul di masyarakat. Kondisi ini sejalan dengan konteks hukum di Indonesia, di mana pengaturan mengenai kejahatan siber masih berfokus pada norma umum tanpa mengantisipasi secara khusus bentuk kejahatan baru berbasis *artificial intelligence*.

Dalam konteks nasional, beberapa kajian menunjukkan bahwa Undang-Undang Informasi dan Transaksi Elektronik belum sepenuhnya mampu memberikan kepastian hukum terhadap kejahatan berbasis manipulasi konten digital. Penelitian yang dilakukan oleh Susanto (2021) mengungkapkan bahwa norma dalam UU ITE masih membuka ruang multitafsir ketika dihadapkan pada kasus kejahatan digital yang bersifat teknologis tinggi. Hal ini menyebabkan aparat penegak hukum menghadapi kesulitan dalam mengkualifikasikan perbuatan dan menentukan pertanggungjawaban pidana pelaku.

Berdasarkan uraian teori dan penelitian terdahulu tersebut, dapat dipahami bahwa terdapat kesenjangan antara perkembangan teknologi *deepfake* dengan kesiapan hukum positif di Indonesia. Penelitian ini berangkat dari asumsi normatif bahwa hukum seharusnya tidak hanya bersifat reaktif, tetapi juga mampu mengantisipasi perkembangan teknologi yang berpotensi merugikan masyarakat. Oleh karena itu, kajian normatif kritis terhadap penyebaran *deepfake* sebagai bentuk kejahatan siber menjadi relevan untuk dilakukan guna memberikan landasan konseptual bagi pembaruan hukum di Indonesia.

3. METODE PENELITIAN

Penelitian ini menggunakan rancangan penelitian hukum normatif dengan pendekatan konseptual dan perundang-undangan. Penelitian hukum normatif dipilih karena fokus kajian diarahkan pada analisis norma hukum yang berlaku serta konsep hukum yang relevan dalam mengkaji penyebaran *deepfake* sebagai bentuk kejahatan siber di Indonesia. Pendekatan ini memungkinkan peneliti untuk menelaah kesesuaian antara norma hukum positif dengan perkembangan teknologi digital yang menimbulkan permasalahan hukum baru (Soekanto & Mamudji, 2019).

Objek kajian dalam penelitian ini berupa bahan hukum, sehingga tidak menggunakan populasi dan sampel dalam pengertian empiris. Sasaran penelitian difokuskan pada peraturan perundang-undangan yang berkaitan dengan kejahatan siber, khususnya Undang-Undang Informasi dan Transaksi Elektronik beserta peraturan terkait lainnya, serta doktrin dan konsep hukum yang berkembang dalam literatur akademik. Selain itu, penelitian ini juga mengkaji putusan pengadilan dan wacana akademik yang relevan untuk memperkaya analisis normatif terhadap fenomena *deepfake*.

Teknik pengumpulan data dilakukan melalui studi kepustakaan dengan menelusuri bahan hukum primer, sekunder, dan tersier. Bahan hukum primer meliputi peraturan perundang-undangan yang berkaitan dengan teknologi informasi dan kejahatan siber. Bahan hukum sekunder terdiri atas buku teks hukum, artikel jurnal ilmiah, dan hasil penelitian terdahulu yang relevan dan diterbitkan dalam kurun waktu lima belas tahun terakhir pada jurnal bereputasi. Adapun bahan hukum tersier digunakan sebagai penunjang, seperti kamus hukum dan ensiklopedia, guna memperjelas istilah dan konsep yang digunakan (Marzuki, 2021).

Instrumen pengumpulan data dalam penelitian ini adalah pedoman studi dokumen yang digunakan untuk mengidentifikasi norma hukum, konsep teoritis, serta pandangan para ahli yang relevan dengan topik penelitian. Teknik ini dipilih karena penelitian bersifat konseptual dan tidak memerlukan instrumen empiris seperti kuesioner atau wawancara. Validitas data

dijaga melalui seleksi literatur yang ketat dengan mempertimbangkan reputasi penerbit, akreditasi jurnal, dan relevansi substansi kajian.

Analisis data dilakukan dengan teknik analisis kualitatif normatif, yaitu dengan menginterpretasikan bahan hukum secara sistematis dan logis untuk menjawab permasalahan penelitian. Proses analisis dilakukan melalui tahapan inventarisasi norma, interpretasi hukum, serta evaluasi kritis terhadap kecukupan norma dalam mengatur penyebaran *deepfake* sebagai kejahatan siber. Hasil analisis kemudian disusun secara deskriptif-analitis untuk menghasilkan pemahaman yang komprehensif mengenai posisi hukum *deepfake* dalam sistem hukum Indonesia.

Model penelitian yang digunakan dalam penelitian ini bersifat konseptual normatif, dengan alur analisis yang dimulai dari identifikasi perkembangan teknologi *deepfake*, pemetaan norma hukum yang berlaku, hingga penilaian kesenjangan hukum yang muncul. Hubungan antara perkembangan teknologi dan norma hukum dianalisis untuk menilai efektivitas perlindungan hukum yang ada serta kebutuhan akan pembaruan regulasi di masa mendatang. Model ini digunakan untuk memastikan bahwa analisis yang dilakukan tetap konsisten dengan tujuan utama penelitian, yaitu memberikan gambaran normatif kritis mengenai pengaturan kejahatan *deepfake* di Indonesia.

4. HASIL DAN PEMBAHASAN

Hasil penelitian menunjukkan bahwa penyebaran *deepfake* sebagai bentuk kejahatan siber di Indonesia belum memperoleh pengaturan hukum yang spesifik dan komprehensif. Berdasarkan analisis terhadap Undang-Undang Informasi dan Transaksi Elektronik beserta peraturan turunannya, tidak ditemukan norma yang secara eksplisit mengatur definisi, unsur, maupun larangan khusus terkait penggunaan dan penyebaran *deepfake*. Akibatnya, penegakan hukum masih bertumpu pada pasal-pasal umum mengenai konten melanggar hukum, seperti pencemaran nama baik atau penyebaran informasi bohong. Padahal, karakteristik *deepfake* yang memanfaatkan kecerdasan buatan menimbulkan kompleksitas tersendiri dalam proses pembuktian dan pertanggungjawaban pidana. Ketergantungan pada norma umum berpotensi menimbulkan multitafsir dan inkonsistensi dalam penerapan hukum. Kondisi ini menunjukkan bahwa hukum positif Indonesia belum sepenuhnya adaptif terhadap perkembangan teknologi digital mutakhir (Sari & Nugroho, 2022).

Dari perspektif perlindungan hak asasi manusia, penyebaran *deepfake* memiliki dampak yang signifikan terhadap hak atas privasi, kehormatan, dan martabat individu. Konten *deepfake* yang dibuat tanpa persetujuan subjek sering kali digunakan untuk merusak reputasi dan

mempermalukan korban di ruang publik digital. Kerugian yang dialami korban tidak hanya bersifat sosial, tetapi juga psikologis dan berpotensi berlangsung dalam jangka panjang. Teori perlindungan hukum menegaskan bahwa negara berkewajiban memberikan perlindungan preventif terhadap warganya dari setiap bentuk penyalahgunaan teknologi. Ketika hukum gagal memberikan batasan normatif yang jelas, korban berada dalam posisi yang rentan tanpa jaminan kepastian hukum. Oleh karena itu, penyebaran *deepfake* perlu dipandang sebagai pelanggaran serius terhadap hak asasi manusia yang memerlukan respon hukum yang tegas dan terarah (Hadjon, 2015).

Kesenjangan antara perkembangan teknologi *deepfake* dan respons hukum nasional menjadi temuan penting dalam penelitian ini. Teknologi kecerdasan buatan berkembang dengan cepat dan terus melahirkan bentuk kejahatan baru, sementara pembentukan hukum cenderung berjalan lambat dan bersifat reaktif. Ketimpangan ini menyebabkan hukum sering kali tertinggal dari realitas sosial yang dihadapinya. Dalam konteks *deepfake*, kondisi tersebut membuka ruang kekosongan hukum yang dapat dimanfaatkan oleh pelaku kejahatan. Aparat penegak hukum pun menghadapi kesulitan dalam mengkualifikasikan perbuatan dan membuktikan unsur kesalahan pelaku. Dari sudut pandang normatif kritis, keadaan ini mencerminkan keterbatasan paradigma hukum pidana yang masih berorientasi pada kejahatan konvensional dan belum sepenuhnya mengakomodasi realitas kejahatan berbasis kecerdasan buatan (Rahardjo, 2019).

Penanganan kejahatan *deepfake* juga tidak dapat diselesaikan hanya melalui pendekatan hukum pidana semata. Sejumlah kajian internasional menunjukkan bahwa pengaturan *deepfake* memerlukan pendekatan multidimensional yang melibatkan hukum pidana, hukum perlindungan data, serta kebijakan etika teknologi. Pendekatan ini bertujuan untuk mencegah penyalahgunaan teknologi sejak tahap awal dan meminimalkan dampak kerugian bagi korban. Dalam konteks Indonesia, temuan ini menunjukkan bahwa pembaruan hukum perlu dilakukan secara komprehensif dan berorientasi pada masa depan. Tanpa regulasi yang jelas dan adaptif, penyebaran *deepfake* berpotensi terus meningkat dan menimbulkan krisis kepercayaan publik terhadap informasi digital. Oleh karena itu, pembentukan kerangka hukum khusus mengenai *deepfake* menjadi kebutuhan mendesak dalam rangka menjamin kepastian hukum dan perlindungan hak asasi manusia di era kecerdasan buatan (Floridi et al., 2018).

5. KESIMPULAN DAN SARAN

Kesimpulan dari penelitian ini menunjukkan bahwa penyebaran *deepfake* sebagai bentuk kejahatan siber di Indonesia belum memperoleh pengaturan hukum yang memadai dan spesifik dalam sistem hukum positif. Ketiadaan norma khusus menyebabkan penegakan hukum masih bergantung pada ketentuan umum yang tidak sepenuhnya mampu menjawab kompleksitas kejahatan berbasis kecerdasan buatan. Kondisi tersebut menimbulkan ketidakpastian hukum, baik dalam aspek kualifikasi tindak pidana maupun dalam penentuan pertanggungjawaban pelaku. Selain itu, penyebaran *deepfake* terbukti berpotensi melanggar hak asasi manusia, khususnya hak atas privasi dan kehormatan individu, sehingga menempatkan korban dalam posisi yang rentan tanpa perlindungan hukum yang optimal. Temuan ini menegaskan bahwa hukum nasional masih bersifat reaktif dan belum sepenuhnya adaptif terhadap perkembangan teknologi digital mutakhir.

Berdasarkan kesimpulan tersebut, penelitian ini menyarankan perlunya pembaruan regulasi yang secara khusus mengatur penyebaran *deepfake* sebagai kejahatan siber, baik melalui pembentukan norma baru maupun penyempurnaan peraturan yang telah ada. Pendekatan regulatif yang komprehensif perlu mempertimbangkan perlindungan korban, kepastian hukum, serta keseimbangan antara kebebasan berekspresi dan pencegahan penyalahgunaan teknologi. Penelitian ini memiliki keterbatasan karena bersifat normatif dan tidak mengkaji aspek empiris terkait praktik penegakan hukum di lapangan. Oleh karena itu, penelitian selanjutnya disarankan untuk mengombinasikan pendekatan normatif dengan penelitian empiris guna memperoleh gambaran yang lebih utuh mengenai efektivitas penanganan kejahatan *deepfake* di Indonesia.

DAFTAR REFERENSI

- Chesney, R., & Citron, D. K. (2019). Deepfakes and the new disinformation war: The coming age of post-truth geopolitics. *Foreign Affairs*, 98(1), 147–155.
- Citron, D. K., & Chesney, R. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review*, 107(6), 1753–1820. <https://doi.org/10.15779/Z38RV0D15J>
- Floridi, L., Cowls, J., Beltrametti, M., et al. (2018). AI4People An ethical framework for a good AI society. *Minds and Machines*, 28(4), 689–707.
- Kietzmann, J., Lee, L. W., McCarthy, I. P., & Kietzmann, T. C. (2020). Deepfakes: Trick or treat? *Business Horizons*, 63(2), 135–146. <https://doi.org/10.1016/j.bushor.2019.11.006>

- Lyu, S. (2020). Deepfake detection: Current challenges and next steps. *Proceedings of the IEEE International Conference on Multimedia Information Processing*, 1–6.
- Maras, M. H., & Alexandrou, A. (2019). Determining authenticity of video evidence in the age of artificial intelligence and in the wake of deepfake videos. *The International Journal of Evidence & Proof*, 23(3), 255–262. <https://doi.org/10.1177/1365712718807226>
- Mirsky, Y., & Lee, W. (2021). The creation and detection of deepfakes: A survey. *ACM Computing Surveys*, 54(1), 1–41.
- Rahardjo, S. (2019). Hukum dan perubahan sosial di era digital. *Jurnal Hukum Ius Quia Iustum*, 26(3), 489–506.
- Sari, N. K., & Nugroho, A. (2022). Penegakan hukum terhadap kejahatan siber di Indonesia dalam perspektif UU ITE. *Jurnal RechtsVinding*, 11(2), 215–230.
- Susanto, A. (2021). Tantangan hukum pidana dalam penanggulangan kejahatan siber. *Jurnal Hukum dan Pembangunan*, 51(1), 85–101.
- Unger, R. M. (2015). The critical legal studies movement. *Harvard Law Review*, 96(3), 561–675.
- Wardle, C., & Derakhshan, H. (2018). Information disorder: Toward an interdisciplinary framework. *Council of Europe Report*, 1–107.
- Wall, D. S. (2017). Crime and deviance in cyberspace. *The Oxford Handbook of Cybersecurity*. Oxford University Press.
- Westerlund, M. (2019). The emergence of deepfake technology: A review. *Technology Innovation Management Review*, 9(11), 40–53.
- Zhang, C., Benz, P., & Chen, X. (2021). Detecting deepfake videos: A survey. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 43(8), 1–20.
- Asshiddiqie, J. (2018). *Pengantar ilmu hukum tata negara*. Rajawali Pers.
- Hadjon, P. M. (2015). *Perlindungan hukum bagi rakyat di Indonesia*. Peradaban.
- Marzuki, P. M. (2021). *Penelitian hukum* (Edisi Revisi). Kencana.
- Soekanto, S., & Mamudji, S. (2019). *Penelitian hukum normatif: Suatu tinjauan singkat*. Rajawali Pers.
- Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
- Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.