

## KEKOSONGAN HUKUM DEEFAKE SEBAGAI ALAT KEJAHATAN DALAM SISTEM HUKUM PIDANA INDONESIA

<sup>1</sup>Benediktus Budi Darmawan Wicaksono

<sup>1</sup>Fakultas Hukum, Universitas Katolik Darma Cendika, Indonesia

E-mail Koresponden: [benediktus.darmawan@student.ukdc.ac.id](mailto:benediktus.darmawan@student.ukdc.ac.id)

<b>Article History</b>	<b>Submitted:</b> 01/02/25	<b>Revised:</b> 20/01/25	<b>Accepted:</b> 21/01/25
<b>Keywords:</b> <i>Deepfake, Legal gap, Criminal law, Artificial intelligence, Cybercrime</i>	<b>Abstract</b> <i>The rapid development of artificial intelligence has led to the emergence of deepfake technology, which enables the manipulation of images, audio, and video in a highly realistic manner. While this technology offers benefits in creative industries and education, it also poses significant risks when misused for criminal purposes, such as fraud, defamation, identity theft, and political disinformation. This study aims to analyze the adequacy of Indonesian positive law in regulating deepfake as a tool of crime and to identify the existing legal gaps. This research employs a normative legal method using statutory and conceptual approaches. The findings indicate that existing regulations have not explicitly addressed deepfake technology, resulting in reliance on general legal interpretations. Legal gaps are identified in the absence of clear definitions, lack of digital forensic standards, and unclear liability frameworks involving multiple actors. Therefore, legal reform is necessary to ensure legal certainty and effective protection for society against emerging digital crimes.</i>		
<b>DOI</b>	<a href="https://doi.org/10.37477/sev.v10i2">https://doi.org/10.37477/sev.v10i2</a>		

### A. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi dalam beberapa dekade terakhir telah membawa perubahan yang sangat signifikan dalam berbagai aspek kehidupan manusia. Transformasi digital yang didorong oleh kemajuan kecerdasan buatan (*artificial intelligence*) telah menciptakan berbagai inovasi yang tidak hanya mempermudah aktivitas manusia, tetapi juga mengubah cara manusia berinteraksi, berkomunikasi, serta memproduksi dan mendistribusikan informasi. Dalam konteks ini, teknologi tidak lagi sekadar menjadi alat bantu, melainkan telah menjadi bagian integral dari kehidupan sosial yang membentuk pola perilaku masyarakat modern. Namun demikian, di balik berbagai manfaat yang ditawarkan, perkembangan teknologi juga menghadirkan tantangan baru, khususnya dalam bidang hukum, yang sering kali tidak mampu mengikuti laju perkembangan teknologi tersebut secara cepat dan adaptif. Salah satu inovasi teknologi yang berkembang pesat dalam beberapa tahun terakhir adalah teknologi *deepfake*. Secara konseptual, *deepfake* merupakan teknik manipulasi media berbasis kecerdasan buatan yang memungkinkan pembuatan konten audiovisual sintetis yang menyerupai realitas secara sangat akurat. Teknologi ini umumnya memanfaatkan algoritma pembelajaran

mesin, khususnya *generative adversarial networks* (GANs), untuk menghasilkan gambar, suara, maupun video yang tampak autentik meskipun sebenarnya merupakan hasil rekayasa digital. Dengan kemampuan tersebut, *deepfake* mampu menampilkan seseorang seolah-olah mengatakan atau melakukan sesuatu yang pada kenyataannya tidak pernah terjadi.

Pada awal kemunculannya, teknologi *deepfake* dikembangkan untuk tujuan yang bersifat positif, seperti dalam industri hiburan, pendidikan, dan penelitian. Dalam industri perfilman, misalnya, teknologi ini digunakan untuk menciptakan efek visual yang lebih realistis atau merekonstruksi wajah aktor secara digital guna kepentingan artistik. Dalam bidang pendidikan, *deepfake* dapat digunakan untuk menghadirkan simulasi interaktif yang membantu proses pembelajaran. Namun demikian, seiring dengan semakin mudahnya akses terhadap teknologi ini serta meningkatnya kemampuan komputasi, *deepfake* mulai disalahgunakan untuk berbagai tujuan yang merugikan. Penyalahgunaan teknologi *deepfake* telah menimbulkan berbagai permasalahan serius, baik dalam aspek sosial, ekonomi, maupun hukum. Dalam praktiknya, *deepfake* telah digunakan sebagai sarana untuk melakukan penipuan berbasis suara (*voice cloning*), di mana pelaku meniru suara seseorang untuk memberikan instruksi tertentu yang menyesatkan. Selain itu, teknologi ini juga digunakan untuk menciptakan video palsu yang menampilkan tokoh publik seolah-olah mengucapkan pernyataan tertentu yang dapat merusak reputasi atau memengaruhi opini publik. Dalam konteks yang lebih ekstrem, *deepfake* bahkan digunakan untuk membuat konten pornografi non-konsensual, yang jelas melanggar hak privasi dan martabat individu. Fenomena ini menunjukkan bahwa *deepfake* tidak hanya menjadi isu teknologi, tetapi juga telah berkembang menjadi ancaman nyata yang membutuhkan perhatian serius dari perspektif hukum.

Salah satu contoh konkrit penyalahgunaan teknologi *deepfake* dapat dilihat dari beredarnya video yang menampilkan tokoh publik Benjamin Netanyahu seolah-olah meninggal dunia di dalam bunker akibat serangan militer. Video tersebut diketahui merupakan hasil manipulasi berbasis kecerdasan buatan yang tidak sesuai dengan fakta sebenarnya. Meskipun demikian, konten tersebut sempat dipercaya oleh sebagian masyarakat dan menyebar luas melalui berbagai platform media sosial. Peristiwa ini menunjukkan bahwa *deepfake* memiliki kemampuan untuk menciptakan realitas semu yang sangat meyakinkan, sehingga sulit dibedakan dari kenyataan oleh masyarakat awam. Dampaknya tidak hanya terbatas pada individu yang menjadi objek manipulasi, tetapi juga dapat memengaruhi stabilitas sosial, politik, dan keamanan suatu negara melalui penyebaran disinformasi yang masif. Fenomena tersebut menunjukkan bahwa batas antara realitas dan rekayasa digital semakin kabur. Dalam konteks ini, masyarakat dihadapkan pada tantangan baru dalam memverifikasi kebenaran suatu informasi. Ketidakmampuan untuk membedakan antara konten asli dan manipulatif dapat menyebabkan menurunnya tingkat kepercayaan publik terhadap informasi digital, bahkan terhadap institusi sosial dan politik. Dalam jangka panjang, kondisi ini berpotensi merusak fondasi

kepercayaan yang menjadi dasar dalam kehidupan bermasyarakat. Oleh karena itu, *deepfake* tidak hanya menjadi persoalan teknologi, tetapi juga menjadi isu serius yang berkaitan dengan stabilitas sosial dan tata kelola informasi.

Dalam perspektif hukum, perkembangan teknologi *deepfake* menimbulkan berbagai permasalahan yang kompleks, khususnya dalam sistem hukum pidana. Hukum pidana Indonesia pada dasarnya masih bertumpu pada konsep kejahatan konvensional yang dirumuskan dalam Kitab Undang-Undang Hukum Pidana (KUHP), yang disusun dalam konteks sosial yang sangat berbeda dengan kondisi saat ini. Meskipun terdapat peraturan perundang-undangan lain seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan Undang-Undang Perlindungan Data Pribadi (UU PDP), pengaturannya masih bersifat umum dan belum secara eksplisit mengakomodasi karakteristik teknologi *deepfake*. Hal ini menimbulkan kesulitan dalam mengkuilifikasikan perbuatan sebagai tindak pidana, serta dalam menentukan bentuk pertanggungjawaban hukum terhadap pelaku. Kondisi tersebut menunjukkan adanya kesenjangan antara perkembangan teknologi dan perkembangan hukum atau yang dikenal sebagai legal lag. Konsep legal lag berakar dari teori cultural lag yang dikemukakan oleh William F. Ogburn, yang menjelaskan bahwa perkembangan unsur non-material seperti hukum sering kali tertinggal dari perkembangan unsur material seperti teknologi. Dalam praktiknya, legal lag terjadi ketika hukum tidak mampu merespons secara cepat terhadap fenomena baru yang muncul akibat perkembangan teknologi, sehingga menimbulkan kekosongan atau ketidakcukupan norma hukum. Dalam konteks *deepfake*, kondisi ini terlihat dari belum adanya definisi hukum yang jelas mengenai *deepfake*, belum adanya standar pembuktian digital yang spesifik, serta belum jelasnya mekanisme pertanggungjawaban pidana terhadap pihak yang terlibat dalam pembuatan dan penyebaran konten *deepfake*.

Sejumlah penelitian sebelumnya telah mengkaji fenomena *deepfake* dari berbagai perspektif. Penelitian yang dilakukan oleh Robert Chesney dan Danielle Keats Citron membahas dampak *deepfake* terhadap privasi, demokrasi, dan keamanan nasional. Penelitian tersebut menunjukkan bahwa *deepfake* memiliki potensi besar untuk digunakan sebagai alat disinformasi dan manipulasi publik dalam skala global. Selain itu, penelitian lain mengkaji *deepfake* dari perspektif teknologi, etika, dan hukum secara komprehensif, dengan menyoroti dampaknya terhadap penyebaran misinformasi, pencurian identitas, serta pelanggaran privasi. Penelitian tersebut memberikan gambaran menyeluruh mengenai fenomena *deepfake*, namun masih bersifat umum dan belum berfokus pada sistem hukum tertentu. Selanjutnya, penelitian dari perspektif psikologis menunjukkan bahwa *deepfake* dapat memengaruhi emosi dan tingkat kepercayaan masyarakat terhadap informasi digital, sehingga berpotensi menimbulkan kebingungan antara realitas dan manipulasi. Meskipun demikian, sebagian besar penelitian terdahulu masih berfokus pada aspek global, teknologi, etika, maupun dampak sosial dari *deepfake*, dan belum secara spesifik mengkaji kekosongan hukum dalam sistem hukum pidana Indonesia. Padahal, analisis terhadap konteks hukum nasional sangat penting untuk memahami

sejauh mana sistem hukum yang ada mampu merespons perkembangan teknologi tersebut. Oleh karena itu, penelitian ini memiliki nilai kebaruan (*novelty*) dalam mengkaji secara sistematis kekosongan hukum yang muncul akibat perkembangan teknologi *deepfake* dalam perspektif hukum pidana Indonesia, serta merumuskan kebijakan hukum yang lebih adaptif dan responsif terhadap perkembangan teknologi. Dengan demikian, penelitian ini tidak hanya bertujuan untuk mengidentifikasi kelemahan regulasi yang ada, tetapi juga untuk memberikan kontribusi dalam pengembangan hukum pidana yang lebih modern dan adaptif terhadap perkembangan teknologi. Dalam konteks ini, hukum tidak hanya berfungsi sebagai alat represif untuk menindak kejahatan, tetapi juga sebagai instrumen preventif yang mampu mengantisipasi perkembangan teknologi di masa depan. Hal ini menjadi penting mengingat perkembangan teknologi yang semakin pesat tidak dapat dihentikan, sehingga hukum harus mampu beradaptasi agar tetap relevan dan efektif dalam menjaga ketertiban dan keadilan dalam masyarakat. Berdasarkan latar belakang yang telah diuraikan, maka rumusan masalah dalam penelitian ini adalah: (1) bagaimana hukum positif Indonesia mengatur penggunaan *deepfake* sebagai alat kejahatan?; dan (2) di mana letak kekosongan hukum dalam pengaturan tersebut serta bagaimana formulasi kebijakan hukum yang ideal untuk mengatasinya?

## B. METODE PENELITIAN

Penelitian ini merupakan penelitian hukum normatif, yaitu penelitian yang berfokus pada kajian terhadap norma hukum yang berlaku dalam sistem hukum positif. Penelitian hukum normatif dilakukan dengan cara menelaah bahan pustaka atau data sekunder, yang meliputi peraturan perundang-undangan, literatur hukum, serta hasil penelitian terdahulu yang relevan dengan permasalahan yang dikaji. Menurut Peter Mahmud Marzuki, penelitian hukum normatif adalah penelitian yang dilakukan untuk menemukan aturan hukum, prinsip hukum, dan doktrin hukum guna menjawab isu hukum yang dihadapi. Pendekatan yang digunakan dalam penelitian ini meliputi pendekatan perundang-undangan (*statute approach*), pendekatan konseptual (*conceptual approach*), dan pendekatan kasus (*case approach*). Pendekatan perundang-undangan dilakukan dengan menelaah berbagai peraturan hukum yang berkaitan dengan kejahatan berbasis teknologi, seperti Kitab Undang-Undang Hukum Pidana (KUHP), Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), serta Undang-Undang Perlindungan Data Pribadi (UU PDP). Pendekatan ini bertujuan untuk mengidentifikasi sejauh mana hukum positif Indonesia telah mengatur penggunaan teknologi *deepfake* sebagai alat kejahatan. Selanjutnya, pendekatan konseptual digunakan untuk memahami konsep-konsep hukum yang berkembang dalam doktrin dan literatur, seperti konsep *deepfake*, kejahatan berbasis kecerdasan buatan, serta konsep legal lag dalam perkembangan hukum. Pendekatan ini penting untuk memberikan landasan teoritis dalam menganalisis kekosongan hukum yang muncul akibat perkembangan teknologi. Selain itu, penelitian ini juga menggunakan pendekatan kasus (*case approach*), yaitu dengan menelaah kasus-

kasus yang relevan sebagai ilustrasi konkret dari permasalahan yang dikaji. Salah satu contoh yang digunakan adalah fenomena penyebaran video manipulatif berbasis kecerdasan buatan yang menampilkan Benjamin Netanyahu seolah-olah berada dalam situasi tertentu yang tidak sesuai dengan fakta. Pendekatan ini bertujuan untuk menunjukkan bagaimana teknologi deepfake digunakan dalam praktik serta potensi dampaknya dalam kehidupan nyata.

Jenis dan sumber bahan hukum dalam penelitian ini terdiri dari bahan hukum primer, bahan hukum sekunder, dan bahan hukum tersier. Bahan hukum primer meliputi peraturan perundang-undangan yang berkaitan dengan objek penelitian, seperti seperti Kitab Undang-Undang Hukum Pidana, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta perubahannya, serta Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Bahan hukum primer ini digunakan sebagai dasar utama dalam menganalisis pengaturan hukum yang berlaku. Bahan hukum sekunder terdiri dari literatur hukum, jurnal ilmiah, serta hasil penelitian terdahulu yang relevan dengan topik penelitian. Literatur yang digunakan mencakup kajian mengenai hukum pidana, hukum teknologi informasi, serta studi tentang kecerdasan buatan dan *deepfake*. Bahan hukum sekunder ini berfungsi untuk memberikan pemahaman yang lebih mendalam mengenai permasalahan yang diteliti, serta untuk memperkuat analisis yang dilakukan dalam penelitian. Sementara itu, bahan hukum tersier meliputi kamus hukum, ensiklopedia, serta sumber-sumber lain yang dapat membantu menjelaskan istilah-istilah yang digunakan dalam penelitian. Bahan hukum tersier ini digunakan sebagai pelengkap untuk memastikan bahwa istilah dan konsep yang digunakan dalam penelitian dapat dipahami dengan jelas.

Teknik pengumpulan bahan hukum dalam penelitian ini dilakukan melalui studi kepustakaan (*library research*), yaitu dengan mengumpulkan dan mengkaji berbagai sumber yang relevan dengan topik penelitian.<sup>1</sup> Studi kepustakaan dilakukan dengan cara menelusuri literatur hukum, jurnal ilmiah, serta peraturan perundang-undangan yang berkaitan dengan *deepfake* dan hukum pidana. Proses ini dilakukan secara sistematis untuk memastikan bahwa bahan hukum yang digunakan dalam penelitian ini relevan dan mutakhir. Teknik analisis bahan hukum dalam penelitian ini dilakukan secara kualitatif dengan menggunakan metode deskriptif-analitis. Metode deskriptif digunakan untuk menggambarkan secara sistematis dan faktual mengenai peraturan hukum yang berlaku serta fenomena *deepfake* yang berkembang di masyarakat. Sementara itu, metode analitis digunakan untuk mengkaji dan menilai kecukupan norma hukum yang ada dalam mengatur penggunaan teknologi *deepfake* sebagai alat kejahatan. Dalam proses analisis, peneliti juga melakukan interpretasi hukum untuk memahami makna dan ruang lingkup ketentuan peraturan perundang-undangan yang relevan. Selanjutnya, metode penarikan kesimpulan yang digunakan dalam penelitian ini adalah metode deduktif,

---

<sup>1</sup> Moeljatno, *Asas-Asas Hukum Pidana* (Jakarta: Rineka Cipta, 2008), 25.

yaitu dengan menarik kesimpulan dari hal-hal yang bersifat umum menuju hal-hal yang bersifat khusus. Dalam hal ini, peneliti mengkaji prinsip-prinsip umum dalam hukum pidana dan regulasi teknologi, kemudian mengaplikasikannya pada permasalahan khusus mengenai penggunaan *deepfake* sebagai alat kejahatan dalam konteks hukum pidana Indonesia. Dengan demikian, penelitian ini diharapkan mampu memberikan analisis yang komprehensif mengenai kekosongan hukum yang ada serta menawarkan solusi yang relevan dalam pengembangan hukum di masa depan.

Penafsiran yang digunakan dalam penelitian ini meliputi penafsiran gramatikal, sistematis, dan teleologis. Penafsiran gramatikal dilakukan dengan memahami makna kata atau istilah dalam peraturan perundang-undangan berdasarkan bahasa yang digunakan. Penafsiran sistematis dilakukan dengan melihat hubungan antara suatu norma dengan norma lain dalam satu sistem hukum. Sementara itu, penafsiran teleologis dilakukan dengan memahami tujuan dari pembentukan suatu norma hukum. Penggunaan berbagai metode penafsiran ini bertujuan untuk memperoleh pemahaman yang komprehensif terhadap peraturan perundang-undangan yang dianalisis, serta untuk mengidentifikasi kekosongan hukum yang mungkin tidak terlihat secara eksplisit. Dengan demikian, penelitian ini tidak hanya melihat hukum secara tekstual, tetapi juga secara kontekstual. Selain itu, penelitian ini juga menggunakan metode argumentasi hukum untuk menyusun analisis yang logis dan sistematis. Argumentasi hukum dilakukan dengan mengaitkan antara norma hukum yang ada dengan fakta atau fenomena yang terjadi, dalam hal ini penggunaan *deepfake* sebagai alat kejahatan. Melalui argumentasi hukum, penelitian ini berupaya menunjukkan bahwa terdapat ketidaksesuaian antara norma yang ada dengan kebutuhan hukum yang berkembang di masyarakat.

Dalam rangka menjaga validitas dan reliabilitas penelitian, penulis melakukan seleksi terhadap sumber-sumber yang digunakan, dengan mengutamakan sumber yang memiliki kredibilitas tinggi, seperti jurnal ilmiah bereputasi dan buku teks hukum yang diakui. Selain itu, penulis juga membandingkan berbagai sumber untuk memastikan konsistensi informasi yang digunakan dalam penelitian. Dengan menggunakan metode penelitian yang telah diuraikan tersebut, diharapkan penelitian ini dapat memberikan analisis yang mendalam dan komprehensif mengenai kekosongan hukum dalam pengaturan *deepfake* sebagai alat kejahatan dalam sistem hukum pidana Indonesia. Metode ini juga memungkinkan penulis untuk merumuskan rekomendasi kebijakan hukum yang berbasis pada analisis yang kuat dan dapat dipertanggungjawabkan secara akademi ini berisi penjelasan metode penelitian dan tahapan-tahapan dalam penelitian yang digunakan oleh penulis untuk mengkaji rumusan masalah.

## **C. HASIL DAN PEMBAHASAN / PEMBAHASAN**

### **1. Analisis Hukum Positif Indonesia terhadap *Deepfake***

Hukum pidana Indonesia pada dasarnya telah memiliki perangkat regulasi untuk mengatur kejahatan, termasuk yang berbasis teknologi. Kitab Undang-Undang Hukum Pidana dapat digunakan untuk menjerat pelaku melalui pasal-pasal penipuan, pemalsuan, dan pencemaran nama baik. Namun demikian, ketentuan tersebut dirumuskan dalam konteks pembuatan konvensional sehingga tidak sepenuhnya relevan untuk menjangkau kejahatan berbasis teknologi canggih seperti *deepfake*.<sup>2</sup> Selain itu, regulasi mengenai informasi dan transaksi elektronik juga memberikan dasar hukum untuk menindak manipulasi informasi digital. Akan tetapi, norma yang ada masih bersifat umum dan tidak secara eksplisit mengatur manipulasi berbasis kecerdasan buatan. Hal ini menimbulkan ketidakpastian dalam penerapan hukum karena aparat penegak hukum harus melakukan interpretasi yang berpotensi berbeda-beda.<sup>3</sup> Regulasi perlindungan data pribadi juga memiliki keterkaitan dengan *deepfake* karena teknologi ini memanfaatkan data biometrik. Namun regulasi tersebut lebih berfokus pada pengelolaan data, bukan pada manipulasi identitas digital. Dengan demikian, dapat disimpulkan bahwa hukum positif Indonesia belum memiliki pengaturan yang memadai untuk menghadapi fenomena *deepfake*.

Dalam konteks hukum pidana Indonesia, pengaturan mengenai kejahatan yang berkaitan dengan teknologi digital tersebar dalam berbagai peraturan perundang-undangan. Kitab Undang-Undang Hukum Pidana sebagai hukum pidana umum menyediakan dasar untuk menjerat pelaku kejahatan melalui ketentuan mengenai penipuan, pemalsuan, dan pencemaran nama baik. Namun, norma-norma tersebut dirumuskan dalam konteks kejahatan konvensional yang belum mempertimbangkan kompleksitas teknologi digital modern.

Undang-Undang Informasi dan Transaksi Elektronik memberikan dasar hukum yang lebih relevan untuk menangani kejahatan berbasis teknologi. Akan tetapi, pengaturan yang terdapat dalam undang-undang tersebut masih bersifat umum dan belum secara spesifik mengatur manipulasi konten berbasis kecerdasan buatan. Hal ini menimbulkan permasalahan dalam penerapan hukum karena aparat penegak hukum harus melakukan interpretasi yang luas untuk menyesuaikan norma yang ada dengan fenomena baru. Selain itu, Undang-Undang Perlindungan Data Pribadi memberikan perlindungan terhadap data individu, termasuk data biometrik yang sering digunakan dalam pembuatan *deepfake*. Namun demikian, fokus utama regulasi ini adalah pada pengelolaan dan perlindungan data, bukan pada manipulasi identitas digital. Oleh karena itu, regulasi tersebut belum mampu mengatasi secara komprehensif permasalahan yang ditimbulkan oleh *deepfake*. Dengan demikian, dapat disimpulkan bahwa hukum positif Indonesia belum memiliki instrumen yang memadai untuk mengatur *deepfake*

---

<sup>2</sup> Andi Hamzah, *Hukum Pidana Indonesia* (Jakarta: Sinar Grafika, 2017), 87.

<sup>3</sup> Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

sebagai alat kejahatan. Kondisi ini menunjukkan adanya ketidakcukupan norma yang dapat berdampak pada lemahnya penegakan hukum.

Dalam sistem hukum pidana Indonesia, pengaturan mengenai kejahatan pada dasarnya masih berakar pada paradigma konvensional yang menitikberatkan pada tindakan fisik dan hubungan langsung antara pelaku dan korban. Kitab Undang-Undang Hukum Pidana sebagai fondasi utama hukum pidana Indonesia disusun dalam konteks sosial yang sangat berbeda dengan kondisi masyarakat digital saat ini. Oleh karena itu, ketika dihadapkan pada fenomena *deepfake* yang berbasis teknologi kecerdasan buatan, norma-norma yang ada sering kali tidak mampu menjangkau kompleksitas permasalahan yang timbul. Dalam praktiknya, beberapa ketentuan dalam KUHP dapat digunakan untuk menjerat pelaku penyalahgunaan *deepfake*, seperti pasal mengenai penipuan, pemalsuan, dan pencemaran nama baik. Namun, penerapan pasal-pasal tersebut menghadapi berbagai kendala, terutama karena unsur-unsur dalam tindak pidana tersebut tidak secara eksplisit mencakup manipulasi digital berbasis kecerdasan buatan. Sebagai contoh, dalam kasus *deepfake* yang digunakan untuk penipuan suara, sulit untuk membuktikan adanya pemalsuan dalam pengertian tradisional, karena tidak ada dokumen fisik yang dipalsukan. Undang-Undang Informasi dan Transaksi Elektronik memberikan kerangka hukum yang lebih relevan dalam menangani kejahatan berbasis teknologi. Ketentuan mengenai penyebaran informasi yang merugikan atau manipulasi data elektronik dapat digunakan untuk menindak pelaku *deepfake*.<sup>4</sup> Namun demikian, norma yang ada masih bersifat umum dan tidak secara spesifik mengatur teknologi *deepfake*. Hal ini menyebabkan adanya ketergantungan pada interpretasi hukum oleh aparat penegak hukum, yang berpotensi menimbulkan perbedaan penafsiran. Sementara itu, Undang-Undang Perlindungan Data Pribadi memberikan perlindungan terhadap data individu, termasuk data biometrik yang sering digunakan dalam pembuatan *deepfake*. Namun fokus utama undang-undang ini adalah pada pengumpulan, pengolahan, dan penyimpanan data, bukan pada manipulasi identitas melalui teknologi digital. Dengan demikian, meskipun memiliki relevansi, regulasi ini belum mampu mengatasi secara komprehensif permasalahan yang ditimbulkan oleh *deepfake*. Berdasarkan analisis tersebut, dapat disimpulkan bahwa hukum positif Indonesia belum memiliki pengaturan yang spesifik dan memadai untuk menangani *deepfake* sebagai alat kejahatan.<sup>5</sup> Kondisi ini mencerminkan adanya ketidakcukupan norma (*normative insufficiency*), di mana norma yang ada tidak mampu menjawab kebutuhan hukum yang berkembang di masyarakat.

## 2. Analisis Kekosongan Hukum *Deepfake*

Kekosongan hukum dalam pengaturan *deepfake* tidak hanya berupa ketiadaan norma, tetapi juga mencerminkan ketidakcukupan norma yang ada.

---

<sup>4</sup> Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

<sup>5</sup> Danielle Keats Citron, "Law's Expressive Value in Combating Deepfake Harms," *Journal of Law and Technology* (2021): 44.

Kekosongan pertama terletak pada aspek definisional, yaitu tidak adanya rumusan hukum yang secara eksplisit mendefinisikan *deepfake*. Hal ini menyebabkan ketidakjelasan dalam menentukan batasan perbuatan yang dapat dikategorikan sebagai tindak pidana. Kekosongan kedua berkaitan dengan aspek operasional, khususnya dalam hal pembuktian. Sistem hukum acara pidana belum memiliki standar khusus untuk mengidentifikasi dan memverifikasi konten *deepfake*. Kondisi ini menyulitkan proses pembuktian di pengadilan karena sulit membedakan antara konten asli dan manipulasi. Kekosongan ketiga terletak pada aspek pertanggungjawaban. Kejahatan *deepfake* melibatkan berbagai pihak, mulai dari pengembang teknologi hingga pengguna akhir. Sistem hukum pidana yang masih berorientasi pada pelaku tunggal belum mampu menjangkau struktur tanggung jawab yang kompleks tersebut.

Kekosongan hukum dalam pengaturan *deepfake* dapat dianalisis melalui beberapa aspek. Pertama, dari perspektif normatif, tidak adanya definisi hukum mengenai *deepfake* menyebabkan ketidakjelasan dalam menentukan batasan perbuatan yang dapat dikategorikan sebagai tindak pidana. Hal ini bertentangan dengan prinsip kepastian hukum yang merupakan salah satu pilar utama dalam sistem hukum pidana. Kedua, dari perspektif operasional, tidak adanya standar pembuktian yang jelas untuk mengidentifikasi konten *deepfake* menjadi hambatan dalam proses penegakan hukum. Teknologi *deepfake* yang semakin canggih membuat konten manipulatif sulit dibedakan dari konten asli, sehingga membutuhkan metode forensik digital yang lebih maju. Ketiga, dari perspektif pertanggungjawaban pidana, kejahatan *deepfake* melibatkan berbagai pihak, mulai dari pengembang teknologi hingga pengguna akhir. Dalam sistem hukum pidana yang masih berorientasi pada pelaku tunggal, kondisi ini menimbulkan kesulitan dalam menentukan pihak yang harus bertanggung jawab.<sup>6</sup> Keempat, kekosongan hukum juga dapat dilihat dari tidak adanya mekanisme pencegahan yang efektif. Regulasi yang ada lebih bersifat represif, yaitu menindak setelah terjadinya kejahatan, sementara perkembangan teknologi menuntut pendekatan yang lebih preventif. Kekosongan hukum dalam pengaturan *deepfake* tidak hanya berarti ketiadaan norma, tetapi juga mencakup ketidakjelasan dan ketidakcukupan norma yang ada. Kekosongan ini dapat dianalisis dari beberapa dimensi utama, yaitu dimensi definisional, operasional, dan pertanggungjawaban. Dari dimensi definisional, tidak adanya definisi hukum mengenai *deepfake* dalam peraturan perundang-undangan Indonesia menyebabkan ketidakjelasan dalam menentukan batasan perbuatan yang dapat dikategorikan sebagai tindak pidana. Tanpa definisi yang jelas, aparat penegak hukum akan kesulitan dalam mengklasifikasikan suatu perbuatan sebagai pelanggaran hukum. Hal ini berpotensi menimbulkan inkonsistensi dalam penegakan hukum serta mengurangi kepastian hukum bagi masyarakat. Dari dimensi operasional, kekosongan hukum terlihat pada tidak adanya standar pembuktian yang

---

<sup>6</sup> Matthew West, "Synthetic Media and the Law," *Columbia Science and Technology Law Review* (2020): 1.

spesifik untuk mengidentifikasi konten *deepfake*. Dalam sistem hukum pidana, pembuktian merupakan aspek yang sangat penting, karena menentukan apakah seseorang dapat dinyatakan bersalah atau tidak. Teknologi *deepfake* yang semakin canggih membuat konten manipulatif sulit dibedakan dari konten asli, sehingga membutuhkan metode forensik digital yang lebih maju. Tanpa adanya standar yang jelas, proses pembuktian akan menjadi sangat kompleks dan berpotensi menimbulkan kesalahan dalam penilaian. Dari dimensi pertanggungjawaban, kejahatan *deepfake* melibatkan berbagai pihak, mulai dari pengembang teknologi, penyedia platform, hingga pengguna akhir. Dalam sistem hukum pidana yang masih berorientasi pada pelaku tunggal, kondisi ini menimbulkan kesulitan dalam menentukan pihak yang harus bertanggung jawab. Misalnya, apakah pengembang teknologi dapat dimintai pertanggungjawaban atas penyalahgunaan teknologi yang mereka ciptakan, atau apakah tanggung jawab sepenuhnya berada pada pengguna yang menyalahgunakan teknologi tersebut. Selain itu, kekosongan hukum juga terlihat pada tidak adanya mekanisme pencegahan yang efektif. Regulasi yang ada lebih bersifat represif, yaitu menindak setelah terjadinya kejahatan, sementara perkembangan teknologi menuntut pendekatan yang lebih preventif. Tanpa adanya upaya pencegahan yang memadai, penyalahgunaan *deepfake* akan terus meningkat dan sulit dikendalikan.

### 3. Implikasi Kekosongan Hukum

Kekosongan hukum dalam pengaturan *deepfake* berdampak langsung terhadap prinsip kepastian hukum. Ketidakjelasan norma menyebabkan masyarakat tidak memiliki pedoman yang jelas mengenai batasan perilaku yang diperbolehkan dan dilarang. Selain itu, kondisi ini juga meningkatkan potensi impunitas karena pelaku kejahatan dapat lolos dari jerat hukum. Di sisi lain, korban kejahatan *deepfake* tidak memperoleh perlindungan hukum yang optimal. Hal ini menunjukkan bahwa kekosongan hukum tidak hanya berdampak pada penegakan hukum, tetapi juga pada perlindungan hak-hak masyarakat.

Kekosongan hukum dalam pengaturan *deepfake* memiliki implikasi yang luas terhadap sistem hukum pidana. Salah satu implikasi utama adalah terganggunya kepastian hukum. Ketidakjelasan norma menyebabkan masyarakat tidak memiliki pedoman yang jelas mengenai perilaku yang diperbolehkan dan dilarang.<sup>7</sup> Selain itu, kekosongan hukum juga dapat menyebabkan terjadinya impunitas, yaitu kondisi di mana pelaku kejahatan tidak dapat dijatuhi sanksi karena tidak adanya dasar hukum yang jelas. Hal ini dapat menurunkan kepercayaan masyarakat terhadap sistem hukum. Dari sisi korban, kekosongan hukum mengakibatkan kurangnya perlindungan terhadap individu yang dirugikan oleh *deepfake*. Korban sering kali mengalami kerugian yang bersifat non-material, seperti kerusakan reputasi, yang sulit

---

<sup>7</sup> Barda Nawawi Arief, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana* (Jakarta: Kencana, 2018), 45.

dipulihkan melalui mekanisme hukum yang ada. Kekosongan hukum dalam pengaturan *deepfake* memiliki implikasi yang signifikan terhadap kepastian hukum dan efektivitas penegakan hukum. Salah satu implikasi utama adalah munculnya ketidakpastian hukum, di mana masyarakat tidak memiliki pedoman yang jelas mengenai batasan perilaku yang diperbolehkan dan dilarang. Hal ini bertentangan dengan prinsip dasar hukum pidana yang menekankan pada kepastian dan kejelasan norma.

Ketidakpastian hukum juga berdampak pada aparat penegak hukum, yang harus mengandalkan interpretasi dalam menerapkan norma yang ada. Kondisi ini berpotensi menimbulkan inkonsistensi dalam putusan pengadilan, di mana kasus yang serupa dapat diputus secara berbeda. Selain itu, ketergantungan pada interpretasi juga membuka peluang bagi penyalahgunaan wewenang. Implikasi lainnya adalah meningkatnya potensi impunitas, yaitu kondisi di mana pelaku kejahatan tidak dapat dijatuhi sanksi karena tidak adanya dasar hukum yang jelas. Hal ini dapat mendorong pelaku untuk terus melakukan kejahatan, karena merasa tidak akan dihukum. Pada akhirnya, kondisi ini dapat menurunkan kepercayaan masyarakat terhadap sistem hukum. Dari sisi korban, kekosongan hukum menyebabkan kurangnya perlindungan hukum. Korban *deepfake* sering kali mengalami kerugian yang bersifat non-material, seperti kerusakan reputasi dan tekanan psikologis. Namun, tanpa adanya mekanisme hukum yang memadai, korban sulit untuk mendapatkan keadilan dan pemulihan.

#### 4. Formulasi Kebijakan Hukum Ideal

Untuk mengatasi permasalahan tersebut, diperlukan reformasi hukum yang bersifat adaptif. Langkah pertama adalah merumuskan definisi hukum mengenai *deepfake* secara jelas dan komprehensif. Selanjutnya, perlu dikembangkan standar forensik digital yang dapat digunakan dalam proses pembuktian di pengadilan.<sup>8</sup> Selain itu, sistem hukum pidana perlu mengadopsi konsep pertanggungjawaban multiaktor untuk menjangkau berbagai pihak yang terlibat dalam kejahatan *deepfake*. Pendekatan regulasi berbasis risiko juga penting diterapkan agar inovasi teknologi tetap dapat berkembang tanpa mengabaikan perlindungan hukum.

Untuk memahami bagaimana hukum dapat merespons fenomena *deepfake*, penting untuk melihat praktik di negara lain. Beberapa negara telah mulai mengembangkan regulasi khusus untuk mengatasi penyalahgunaan teknologi ini. Di Amerika Serikat, beberapa negara bagian telah mengatur larangan penggunaan *deepfake* dalam konteks politik dan pornografi non-konsensual. Regulasi ini menunjukkan pendekatan yang lebih spesifik dalam menangani dampak negatif teknologi. Di Uni Eropa, pendekatan yang digunakan lebih komprehensif melalui regulasi kecerdasan buatan yang menekankan pada transparansi, akuntabilitas, dan pengelolaan risiko.

---

<sup>8</sup> Neil MacCormick, *Legal Reasoning and Legal Theory* (Oxford: Oxford University Press, 1978), 102.

Pendekatan ini mencerminkan upaya untuk mengintegrasikan aspek teknologi dan hukum secara sistematis. Sementara itu, di Tiongkok, pemerintah telah menerapkan regulasi yang mewajibkan pelabelan konten sintetis untuk mencegah penyebaran informasi yang menyesatkan. Pendekatan ini menekankan pada pencegahan melalui transparansi informasi. Perbandingan ini menunjukkan bahwa Indonesia masih tertinggal dalam mengembangkan regulasi yang spesifik dan adaptif terhadap perkembangan teknologi *deepfake*. Dalam merumuskan kebijakan hukum yang ideal, diperlukan pendekatan yang komprehensif dan adaptif. Salah satu langkah penting adalah merumuskan definisi hukum mengenai *deepfake* yang jelas dan komprehensif. Definisi ini harus mencakup berbagai bentuk manipulasi digital yang menggunakan teknologi kecerdasan buatan. Selain itu, perlu dikembangkan standar forensik digital yang dapat digunakan dalam proses pembuktian. Standar ini harus mampu mengidentifikasi dan memverifikasi konten *deepfake* secara akurat. Dalam hal pertanggungjawaban pidana, perlu diadopsi konsep pertanggungjawaban multiaktor yang dapat menjangkau berbagai pihak yang terlibat dalam kejahatan *deepfake*. Pendekatan ini penting untuk memastikan bahwa semua pihak yang berkontribusi terhadap terjadinya kejahatan dapat dimintai pertanggungjawaban. Selain pendekatan represif, regulasi juga harus mencakup aspek preventif, seperti kewajiban bagi platform digital untuk mendeteksi dan menghapus konten *deepfake* yang berbahaya. Pendekatan berbasis risiko juga dapat diterapkan untuk mengklasifikasikan penggunaan teknologi berdasarkan tingkat bahayanya.

Untuk memahami bagaimana hukum dapat merespons fenomena *deepfake*, penting untuk melihat bagaimana negara lain mengatur teknologi ini. Di Amerika Serikat, beberapa negara bagian telah mengadopsi regulasi yang melarang penggunaan *deepfake* dalam konteks tertentu, seperti pemilu dan pornografi non-konsensual. Regulasi ini menunjukkan pendekatan yang lebih spesifik dalam menangani dampak negatif teknologi. Di Uni Eropa, pendekatan yang digunakan lebih komprehensif melalui regulasi kecerdasan buatan yang menekankan pada prinsip transparansi, akuntabilitas, dan manajemen risiko. Regulasi ini tidak hanya mengatur penggunaan teknologi, tetapi juga menetapkan kewajiban bagi pengembang dan penyedia layanan untuk memastikan bahwa teknologi yang mereka kembangkan tidak disalahgunakan. Di Tiongkok, pemerintah telah menerapkan kebijakan yang mewajibkan pelabelan konten sintetis untuk mencegah penyebaran informasi yang menyesatkan. Pendekatan ini menekankan pada transparansi sebagai upaya pencegahan. Perbandingan ini menunjukkan bahwa negara-negara lain telah mulai mengembangkan regulasi yang lebih adaptif terhadap perkembangan teknologi. Sementara itu, Indonesia masih berada pada tahap awal dalam merespons fenomena ini.

Dalam menghadapi tantangan yang ditimbulkan oleh teknologi *deepfake*, diperlukan reformasi hukum yang bersifat komprehensif dan adaptif. Salah satu langkah penting adalah merumuskan definisi hukum mengenai *deepfake* yang jelas dan komprehensif. Definisi ini harus mencakup

berbagai bentuk manipulasi digital yang menggunakan teknologi kecerdasan buatan.<sup>9</sup> Selain itu, perlu dikembangkan standar forensik digital yang dapat digunakan dalam proses pembuktian. Standar ini harus mampu mengidentifikasi dan memverifikasi konten *deepfake* secara akurat, sehingga dapat digunakan sebagai alat bukti yang sah di pengadilan. Dalam hal pertanggungjawaban pidana, perlu diadopsi konsep pertanggungjawaban multiaktor yang memungkinkan penegakan hukum terhadap berbagai pihak yang terlibat. Pendekatan ini penting untuk memastikan bahwa tidak ada pihak yang dapat menghindari tanggung jawab. Selain pendekatan represif, regulasi juga harus mencakup aspek preventif, seperti kewajiban bagi platform digital untuk mendeteksi dan menghapus konten *deepfake* yang berbahaya. Pendekatan berbasis risiko juga dapat diterapkan untuk mengklasifikasikan penggunaan teknologi berdasarkan tingkat bahayanya. Dengan demikian, reformasi hukum yang dilakukan harus mampu mengakomodasi perkembangan teknologi tanpa menghambat inovasi. Hukum harus berfungsi sebagai alat untuk mengatur dan mengarahkan perkembangan teknologi agar tetap sejalan dengan nilai-nilai keadilan dan kepentingan masyarakat.

#### D. PENUTUP

Berdasarkan hasil pembahasan, dapat disimpulkan bahwa hukum positif Indonesia belum mampu secara optimal mengatur penggunaan *deepfake* sebagai alat kejahatan. Kekosongan hukum yang terjadi bersifat struktural dan mencakup aspek definisi, pembuktian, serta pertanggungjawaban. Kondisi ini berdampak pada terganggunya kepastian hukum dan perlindungan masyarakat. Oleh karena itu, diperlukan reformasi hukum yang adaptif terhadap perkembangan teknologi. Pembentuk undang-undang perlu merumuskan regulasi yang mampu menjangkau kejahatan berbasis kecerdasan buatan secara komprehensif. Berdasarkan kesimpulan tersebut, penelitian selanjutnya diharapkan dapat mengkaji lebih lanjut mengenai implikasi kecerdasan buatan terhadap konsep subjek hukum dalam hukum pidana modern serta pengembangan sistem pembuktian digital yang lebih akurat.

Perkembangan teknologi *deepfake* telah menghadirkan tantangan baru bagi sistem hukum pidana Indonesia. Hukum positif yang ada belum mampu mengatur secara spesifik fenomena ini, sehingga menimbulkan kekosongan hukum yang berdampak pada kepastian hukum, penegakan hukum, dan perlindungan masyarakat. Kekosongan hukum tersebut mencakup aspek definisi, pembuktian, dan pertanggungjawaban pidana. Kondisi ini menunjukkan bahwa diperlukan reformasi hukum yang adaptif terhadap perkembangan teknologi. Ke depan, pembentuk undang-undang perlu merumuskan regulasi yang lebih komprehensif dan responsif terhadap perkembangan kecerdasan buatan. Selain itu, penelitian lebih lanjut

---

<sup>9</sup> Hans Kelsen, *Pure Theory of Law* (California: University of California Press, 1967), 198.

diperlukan untuk mengkaji implikasi teknologi terhadap konsep hukum pidana modern, khususnya dalam hal subjek hukum dan sistem pembuktian.

Kekosongan hukum tersebut dapat diidentifikasi dalam beberapa aspek utama. Pertama, tidak adanya definisi hukum mengenai *deepfake* menyebabkan ketidakjelasan dalam menentukan batasan perbuatan yang dapat dikategorikan sebagai tindak pidana. Kedua, tidak adanya standar pembuktian yang spesifik menyulitkan proses penegakan hukum, mengingat teknologi *deepfake* semakin sulit dibedakan dari konten asli. Ketiga, sistem pertanggungjawaban pidana yang masih berorientasi pada pelaku tunggal tidak mampu menjangkau kompleksitas aktor yang terlibat dalam produksi dan distribusi *deepfake*. Keempat, regulasi yang ada masih cenderung bersifat represif dan belum mengakomodasi pendekatan preventif yang diperlukan dalam menghadapi perkembangan teknologi. Implikasi dari kekosongan hukum tersebut sangat luas, terutama terhadap kepastian hukum, efektivitas penegakan hukum, dan perlindungan terhadap korban. Ketidakjelasan norma menyebabkan potensi terjadinya inkonsistensi dalam penegakan hukum, serta membuka peluang terjadinya impunitas. Di sisi lain, korban *deepfake* tidak memperoleh perlindungan hukum yang memadai, sehingga mengalami kerugian baik secara material maupun non-material tanpa adanya mekanisme pemulihan yang efektif. Dalam konteks perbandingan hukum, beberapa negara telah mulai mengembangkan regulasi yang lebih adaptif terhadap fenomena *deepfake*, baik melalui pendekatan sektoral maupun komprehensif. Hal ini menunjukkan bahwa pengaturan hukum terhadap teknologi *deepfake* merupakan kebutuhan yang mendesak dan tidak dapat ditunda. Oleh karena itu, Indonesia perlu segera melakukan reformasi hukum untuk mengatasi kekosongan yang ada. Berdasarkan kesimpulan tersebut, penelitian ini memberikan beberapa rekomendasi. Pertama, pembentuk undang-undang perlu merumuskan definisi hukum mengenai *deepfake* secara jelas dan komprehensif untuk memberikan kepastian hukum. Kedua, perlu dikembangkan standar forensik digital yang dapat digunakan dalam proses pembuktian di pengadilan. Ketiga, sistem pertanggungjawaban pidana perlu diperluas dengan mengadopsi konsep pertanggungjawaban multiaktor yang mampu menjangkau seluruh pihak yang terlibat. Keempat, regulasi yang dibentuk harus mengintegrasikan pendekatan preventif dan represif secara seimbang, termasuk dengan melibatkan peran platform digital dalam mencegah penyebaran konten *deepfake* yang berbahaya. Selain itu, penelitian selanjutnya diharapkan dapat mengkaji lebih lanjut mengenai implikasi perkembangan kecerdasan buatan terhadap konsep-konsep fundamental dalam hukum pidana, seperti konsep kesalahan, subjek hukum, dan sistem pembuktian. Penelitian lanjutan juga dapat mengembangkan pendekatan interdisipliner yang menggabungkan perspektif hukum, teknologi, dan etika untuk menghasilkan solusi yang lebih komprehensif. Dengan demikian, dapat ditegaskan bahwa pembaruan hukum merupakan suatu keniscayaan dalam menghadapi perkembangan teknologi yang semakin pesat.

Hukum harus mampu beradaptasi dan berkembang agar tetap relevan serta mampu memberikan perlindungan yang efektif bagi masyarakat di era digital.

## DAFTAR PUSTAKA

### Jurnal

- Buo, Shadrack Awah. n.d. "The Emerging Threats of Deepfake Attacks and Countermeasures." <https://doi.org/10.13140/RG.2.2.23089.81762>.
- Kietzmann, Jan, Linda W Lee, and Ian P Mccarthy. 2020. "Deepfakes : Trick or Treat ? Deepfakes : Trick or Treat ?" 63 (2): 135–46.
- Mirsky, Yisroel, and Wenke Lee. 2020. "The Creation and Detection of Deepfakes : A Survey" 1 (1).
- "No Title." n.d.
- Passos, Leandro A, Danilo Jodas, Kelton A P Costa, and Luis A Souza. n.d. "A Review of Deep Learning-Based Approaches For."
- Chesney, Robert, and Danielle Citron. 2019. "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security." *California Law Review* 107: 1753–1820.
- Kietzmann, J., et al. 2020. "Deepfakes: Trick or Treat?" *Business Horizons* 63: 135–146.
- Citron, Danielle Keats. 2021. "Law's Expressive Value in Combating Deepfake Harms." *Journal of Law and Technology*: 44–60.
- West, Matthew. 2020. "Synthetic Media and the Law." *Columbia Science and Technology Law Review*: 1–30.
- Calo, Ryan. 2017. "Artificial Intelligence Policy: A Primer." *UCLA Law Review* 64: 399–435.

### Buku

- Soekanto, Soerjono, dan Sri Mamudji. 2004. *Penelitian Hukum Normatif*. Jakarta: PT RajaGrafindo Persada.
- Amiruddin, dan Zainal Asikin. 2012. *Pengantar Metode Penelitian Hukum*. Jakarta: Raja Grafindo.
- Moeljatno. 2008. *Asas-Asas Hukum Pidana*. Jakarta: Rineka Cipta.
- Hamzah, Andi. 2017. *Hukum Pidana Indonesia*. Jakarta: Sinar Grafika.
- Arief, Barda Nawawi. 2018. *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana*. Jakarta: Kencana.
- MacCormick, Neil. 1978. *Legal Reasoning and Legal Theory*. Oxford: Oxford University Press.
- Kelsen, Hans. 1967. *Pure Theory of Law*. California: University of California Press.

### Peraturan Perundang-Undangan

- Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.
- Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
- Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.
- Kitab Undang-Undang Hukum Pidana.