

Pertanggungjawaban Pidana Dalam Kasus Penggunaan Teknologi Digital Cerdas Untuk Pemalsuan Dokumen

Nofha Sahas Vivian Sahal¹, Tri Abriana Ma'ruf², Satrih Hasyim³

Fakultas Hukum, Universitas Muslim Indonesia, Indonesia

Koresponden: nofhasahasviviansahal@gmail.com

Abstrak:

Penelitian ini bertujuan Untuk mengetahui dan menentukan pengaturan hukum pidana terkait pemalsuan dokumen dengan teknologi digital cerdas dan untuk mengetahui dan menentukan kendala hukum dalam pembuktian tindak pidana pemalsuan dokumen yang melibatkan teknologi digital cerdas. Penelitian ini ialah jenis penelitian hukum normatif merupakan penelitian hukum yang dilakukan dengan cara meneliti bahan pustaka atau Bahan Hukum dengan mengambil isu dari hukum sebagai sistem norma yang digunakan maka penelitian hukum normatif menjadikan sistem norma sebagai pusat kajian. Hasil penelitian ini mengindikasikan bahwa Pengaturan hukum pidana terkait pemalsuan KTP berbasis teknologi digital cerdas pada dasarnya telah memiliki dasar normatif yang memadai melalui Pasal 263 KUHP, UU ITE, dan UU Administrasi Kependudukan. Ketiga regulasi tersebut dapat diterapkan secara alternatif atau kumulatif berdasarkan prinsip *lex specialis derogat legi generali*. Namun, perbedaan dan keterpisahan pengaturan menuntut adanya harmonisasi serta penafsiran yang integratif. Serta Kendala Dalam Pembuktian Tindak Pidana Pemalsuan Dokumen Yang Dilakukan Dengan Memanfaatkan Teknologi Digital Cerdas Berdasarkan Ketentuan Hukum Pidana Positif Di Indonesia, yaitu Kendala Penentuan Kualifikasi KTP sebagai "Surat" dan "Dokumen Elektronik", Kendala Pembuktian Keaslian Data e-KTP, Kendala Pembuktian Unsur Kesengajaan dalam Pemalsuan KTP Digital, serta Kendala Pembuktian Keterkaitan antara KTP Palsu dan Akibat Hukum.

Kata Kunci: Pertanggungjawaban, Pemalsuan Dokumen, Teknologi Cerdas, E-KTP

Abstract:

This research aims to find out and determine criminal law arrangements related to document forgery with intelligent digital technology and to find out and determine legal obstacles in proving the crime of document forgery involving intelligent digital technology. This research is a type of normative legal research that is legal research that is carried out by researching literature materials or legal materials by taking issues from law as a norm system used, normative legal research makes the norm system the center of study. The results of this study indicate that criminal law regulations related to ID card forgery based on smart digital technology basically have an adequate normative basis through Article 263 of the Criminal Code, the ITE Law, and the Population Administration Law. The three regulations can be

applied alternatively or cumulatively based on the principle of lex specialis derogat legi generali. However, differences and separations of regulations require harmonization and integrative interpretation. As well as obstacles in proving the crime of document forgery carried out by utilizing intelligent digital technology based on the provisions of positive criminal law in Indonesia, namely Obstacles in Determining the Qualification of ID Cards as "Letters" and "Electronic Documents", Obstacles in Proving the Authenticity of e-KTP Data, Obstacles in Proving Intentional Elements in Digital ID Card Forgery, and Obstacles in Proving the Relationship between Fake ID Cards and Legal Consequences.

Keywords: *Liability, Document Forgery, Smart Technology, E-KTP*

A. PENDAHULUAN

Salah satu bentuk AIC yang paling berbahaya dan berpotensi merusak adalah deepfake, atau yang disebut juga audio/video impersonation, yakni praktik pemalsuan atau peniruan identitas seseorang melalui media digital. Teknologi deepfake bekerja dengan memanfaatkan metode deep learning, yaitu proses pembelajaran mesin yang mampu memindai, menganalisis, dan meniru secara mendetail karakteristik visual maupun suara manusia. Dengan kemampuan tersebut, AI dapat menghasilkan rekayasa foto, video, atau audio yang tampak autentik, sehingga berpotensi besar digunakan untuk tujuan penipuan, fitnah, atau pemalsuan dokumen digital.

Salah satu bentuk penyalahgunaan tersebut adalah praktik pemalsuan dokumen yang dilakukan dengan memanfaatkan kecerdasan buatan. Melalui teknologi AI, pelaku kejahatan dapat menciptakan dokumen palsu, mengubah isi dokumen asli, atau bahkan membuat dokumen digital tiruan (deepfake documents) yang sulit dibedakan dengan dokumen sah. Fenomena ini menjadi bentuk baru dari kejahatan siber (cybercrime) yang dikenal sebagai Artificial Intelligence Crime (AIC). Dengan kemampuan AI untuk memanipulasi data, gambar, tanda tangan, atau bahkan identitas digital seseorang, muncul tantangan serius bagi penegak hukum dalam menentukan siapa yang harus dimintai pertanggungjawaban pidana.

Pasal 263 sampai dengan Pasal 276. Ketentuan ini menegaskan bahwa setiap orang yang dengan sengaja membuat, memalsukan, atau menggunakan surat palsu dengan maksud untuk menimbulkan akibat hukum tertentu dapat dikenakan sanksi pidana. Tujuan utama dari pengaturan ini adalah untuk melindungi keaslian, kepercayaan, dan nilai pembuktian dari suatu dokumen atau surat, baik yang bersifat pribadi maupun resmi, agar tidak disalahgunakan untuk kepentingan yang melawan hukum.¹

Pasal 263 KUHP merupakan dasar utama dalam tindak pidana pemalsuan. Pasal ini memuat dua bentuk perbuatan, yaitu membuat atau memalsukan surat, dan menggunakan surat palsu seolah-olah asli. Dalam rumusan Pasal 263 ayat (1), unsur utama yang dilarang adalah tindakan membuat atau mengubah suatu surat sehingga tidak sesuai dengan kebenaran, dengan maksud agar surat tersebut dipakai atau dianggap benar oleh orang lain. Sedangkan Pasal 263 ayat (2) mengatur perbuatan menggunakan surat palsu tersebut untuk menimbulkan kerugian bagi pihak lain. Kedua bentuk perbuatan ini sama-sama diancam dengan pidana penjara paling lama enam tahun.

Seiring dengan perkembangan teknologi informasi di era Revolusi Industri 4.0 dan Society 5.0, pengertian tentang "surat" telah berevolusi. Jika sebelumnya surat identik dengan dokumen fisik yang ditandatangani secara manual, kini hukum positif Indonesia melalui Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) beserta perubahannya, telah memperluas makna tersebut menjadi dokumen elektronik. Dokumen elektronik memiliki kedudukan hukum yang sama dengan dokumen tertulis, asalkan memenuhi persyaratan keotentikan, integritas, dan keterbacaan.

Lebih lanjut, pemaknaan hukum terhadap pemalsuan elektronik tidak dapat dilepaskan dari asas *lex specialis derogat legi generali*, di mana UU ITE sebagai undang-undang khusus melengkapi KUHP sebagai hukum umum. Dengan demikian, ketika pemalsuan dilakukan menggunakan sistem elektronik atau berbasis AI, maka selain Pasal 263 KUHP,

¹ Hamzah, A. (2008). Delik-delik tertentu dalam KUHP. Jakarta: Sinar Grafika. Hal 15

pelaku dapat dijerat pula dengan ketentuan Pasal 35 jo. Pasal 51 ayat (1) UU ITE yang mengatur tentang manipulasi atau pemalsuan informasi elektronik.²

Dalam konteks pembuktian, penggunaan teknologi berbasis algoritma cerdas dalam pemalsuan dokumen menempatkan alat bukti elektronik sebagai instrumen yang sangat penting. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 telah mengakui informasi elektronik dan/atau dokumen elektronik beserta hasil cetaknya sebagai alat bukti hukum yang sah. Dengan demikian, data digital, metadata, log sistem, serta rekam jejak penggunaan perangkat lunak cerdas dapat dijadikan dasar pembuktian untuk menelusuri proses pembuatan dokumen palsu dan keterkaitannya dengan pelaku.

Seperti halnya Kasus penggunaan artificial intelligence (AI) untuk pemalsuan dokumen nyata terjadi di Indonesia, terutama dalam konteks pemalsuan data rekening perbankan dengan teknologi AI. Salah satu kasus penting adalah penangkapan dua tersangka yang memanfaatkan AI untuk membuat rekening bank palsu dengan menggunakan data orang lain tanpa izin, serta melakukan rekayasa video verifikasi wajah untuk aktivasi akun bank tersebut. Pemalsuan yang dilakukan dengan alat AI ini membuat video verifikasi wajah dianggap sebagai milik asli sehingga akun dapat diaktifkan secara ilegal. Kasus ini terungkap oleh Direktorat Siber Polda Metro Jaya pada periode Desember 2024 hingga Januari 2025 dengan tersangka PM.[Detikcom, <https://news.detik.com/berita/d-7768549/polda-metro-tangkap-2-tersangka-pemalsuan-rekening-menggunakan-ai>, Diakses pada 15 Oktober 2025.]

Dalam konteks hukum Indonesia, penggunaan AI untuk pemalsuan identitas seperti ini menimbulkan tantangan serius dalam menanggulangi fenomena penyalahgunaan AI dalam pemalsuan dokumen atau identitas. Ada kebutuhan mendesak untuk pembaruan aturan hukum dan penegakan hukum yang lebih efektif, seperti regulasi perlindungan data dan pengaturan AI yang diadopsi di beberapa negara seperti Uni Eropa (misalnya

² Andi Hamzah. (2005). Hukum pidana Indonesia: Pokok-pokoknya (ed. revisi). Jakarta: Rineka Cipta. Hal 21

GDPR dan AI Act). Hal ini untuk menyesuaikan perkembangan teknologi dengan perlindungan hukum yang memadai bagi korban pemalsuan identitas menggunakan AI.

Contoh kasus lainnya, Pada awal tahun 2025, banyak laporan penipuan dengan modus pemalsuan bukti transfer menggunakan AI. Modus ini melibatkan pembuatan dokumen digital palsu berupa bukti transfer yang sangat realistis termasuk hologram pada gambar transfer. Tujuannya menipu korban agar percaya mereka sudah menerima pembayaran, padahal tidak. Kementerian Komunikasi dan Informatika telah menerbitkan etika AI dan melakukan koordinasi dengan OJK serta Bank Indonesia guna mencegah kerugian akibat penyalahgunaan teknologi AI ini³

B. METODE

Adapun bahan hukum sekunder seperti buku-buku, jurnal-jurnal, hasil penelitian, doktrin dan lain-lain; serta bahan hukum tersier. Teknik pengumpulan bahan hukum dengan mengumpulkan bahan-bahan penulisan berkaitan dengan penelitian ini yaitu buku-buku, referensi jurnal, karya-karya ilmiah dibidang pembiayaan dan pihak ketiga , internet, artikel dan lainnya.

C. PEMBAHASAN

1. Pengaturan Hukum Pidana Terkait Pemalsuan Dokumen Dengan Teknologi Digital Cerdas.

Pasal 263 ayat (1) KUHP memberikan rumusan dasar mengenai pemalsuan surat, yaitu perbuatan membuat surat palsu atau memalsukan surat yang dapat menimbulkan suatu hak, perikatan, atau pembebasan utang, atau yang diperuntukkan sebagai alat bukti mengenai suatu hal, dengan maksud untuk menggunakan atau menyuruh orang lain menggunakan surat tersebut seolah-olah surat itu asli dan tidak dipalsukan. Rumusan ini menegaskan bahwa esensi tindak pidana pemalsuan terletak pada adanya perbuatan aktif yang ditujukan untuk menciptakan atau mengubah suatu dokumen

³ <https://irmapa.org/teknologi-ai-generatif-dan-ancaman-baru-pemalsuan-dokumen/>, Diakses pada 15 Oktober 2025.

sedemikian rupa sehingga menimbulkan kesan seolah-olah dokumen tersebut sah dan memiliki kekuatan hukum.⁴

Dalam konteks perkembangan teknologi digital, unsur “membuat surat palsu” maupun “memalsukan surat” tidak lagi terbatas pada tindakan fisik seperti meniru tulisan tangan atau memalsukan tanda tangan di atas kertas, melainkan juga mencakup pembuatan dokumen elektronik palsu, pengubahan data digital, atau manipulasi identitas melalui perangkat lunak cerdas. Misalnya, pembuatan Kartu Tanda Penduduk (KTP) elektronik palsu dengan mengubah data kependudukan menggunakan aplikasi pengolah gambar atau sistem berbasis kecerdasan buatan, pada hakikatnya tetap memenuhi unsur pemalsuan surat sebagaimana dimaksud dalam Pasal 263 KUHP, karena dokumen tersebut dimaksudkan untuk menimbulkan hak atau digunakan sebagai alat bukti identitas seseorang.

Pemalsuan Kartu Tanda Penduduk (KTP) merupakan salah satu bentuk pemalsuan dokumen yang paling sering terjadi dan memiliki implikasi hukum serius, mengingat KTP berfungsi sebagai identitas resmi yang diterbitkan oleh negara dan menjadi dasar untuk memperoleh berbagai hak keperdataan maupun administratif. Seiring dengan perkembangan teknologi digital cerdas, modus pemalsuan KTP tidak lagi dilakukan secara konvensional, melainkan dengan memanfaatkan teknologi pengolahan data dan kecerdasan buatan. Dalam praktiknya, pemalsuan KTP berbasis teknologi digital cerdas dapat dilakukan dengan cara memanipulasi data kependudukan melalui perangkat lunak pengeditan grafis, mengubah elemen identitas seperti nama, Nomor Induk Kependudukan (NIK), alamat, dan foto wajah, atau bahkan menciptakan KTP palsu secara keseluruhan menggunakan sistem desain digital yang menyerupai format KTP elektronik (e-KTP). Selain itu, teknologi *face swapping* dan *deepfake* memungkinkan pelaku mengganti foto wajah pemilik identitas asli dengan wajah orang lain secara sangat meyakinkan, sehingga sulit dibedakan secara kasat mata.⁵

⁴ Setiawan, E., & Hartwiningsih, H. (2025). *Optimizing the use of digital forensics and information technology in proving criminal acts of electronic document forgery in Indonesia*. *International Journal of Law, Crime and Justice*, 2(2), 75–86

⁵ Zhang, C. J., Gill, A. Q., Liu, B., & Anwar, M. J. (2025). *AI-based identity fraud detection: A systematic review*. *arXiv*.

Dari perspektif hukum pidana, perbuatan pemalsuan KTP tersebut dapat dikualifikasikan sebagai tindak pidana pemalsuan surat sebagaimana diatur dalam Pasal 263 ayat (1) KUHP. KTP memenuhi unsur “surat” karena merupakan dokumen resmi yang dikeluarkan oleh pejabat berwenang dan memiliki fungsi sebagai alat bukti identitas serta dasar untuk menimbulkan hak dan kewajiban hukum. Unsur “membuat surat palsu atau memalsukan surat” terpenuhi ketika pelaku dengan sengaja mengubah atau menciptakan KTP yang tidak sesuai dengan data kependudukan yang sebenarnya. Sementara itu, unsur “maksud untuk menggunakan atau menyuruh orang lain menggunakan seolah-olah asli” terpenuhi apabila KTP palsu tersebut digunakan, misalnya, untuk membuka rekening bank, mengajukan pinjaman daring, atau mengakses layanan publik tertentu.

Selain dikenakan Pasal 263 KUHP, pemalsuan KTP yang dilakukan melalui sistem elektronik juga dapat dijerat dengan ketentuan Undang-Undang Informasi dan Transaksi Elektronik. Pasal 35 UU ITE mengatur larangan manipulasi, penciptaan, perubahan, penghilangan, atau perusakan informasi elektronik dan/atau dokumen elektronik dengan tujuan agar data tersebut dianggap seolah-olah otentik. Dalam konteks e-KTP, data kependudukan yang tersimpan dalam sistem elektronik merupakan informasi elektronik yang dilindungi hukum. Oleh karena itu, tindakan memanipulasi data e-KTP secara digital, termasuk dengan bantuan teknologi digital cerdas, memenuhi unsur tindak pidana sebagaimana dimaksud dalam pasal tersebut, dengan ancaman pidana sebagaimana diatur dalam Pasal 51 ayat (1) UU ITE.

Lebih lanjut, pemalsuan KTP juga dapat dikaitkan dengan Undang-Undang Nomor 24 Tahun 2013 tentang Administrasi Kependudukan. Undang-undang ini menegaskan bahwa setiap orang dilarang memalsukan dokumen kependudukan, termasuk KTP dan e-KTP. Dengan demikian, pemalsuan KTP berbasis teknologi digital cerdas dapat dikenakan sanksi pidana berdasarkan peraturan khusus di bidang administrasi kependudukan, yang penerapannya dapat bersifat kumulatif dengan ketentuan KUHP dan UU ITE.

Melalui contoh pemalsuan KTP tersebut, dapat dilihat bahwa teknologi digital cerdas telah memperluas bentuk dan dampak pemalsuan dokumen. Tidak hanya merugikan individu tertentu, pemalsuan KTP juga berpotensi mengganggu sistem administrasi kependudukan nasional dan menurunkan tingkat kepercayaan publik terhadap dokumen negara. Oleh karena itu, pengaturan hukum pidana yang ada perlu diinterpretasikan secara progresif agar mampu menjangkau kejahatan pemalsuan identitas di era digital, sekaligus mendorong pembaruan hukum yang lebih adaptif terhadap perkembangan teknologi.

2. Kendala Dalam Pembuktian Tindak Pidana Pemalsuan Dokumen Yang Dilakukan Dengan Memanfaatkan Teknologi Digital Cerdas Berdasarkan Ketentuan Hukum Pidana Positif Di Indonesia.

Secara normatif, pembuktian tindak pidana pemalsuan KTP mengacu pada ketentuan Pasal 184 KUHP mengenai alat bukti yang sah, serta pengakuan dokumen elektronik sebagai alat bukti hukum berdasarkan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Namun, dalam praktik, terdapat berbagai kendala yuridis dan teknis yang menghambat pembuktian pemalsuan KTP berbasis teknologi digital cerdas.

a) Kendala Penentuan Kualifikasi KTP sebagai “Surat” dan “Dokumen Elektronik”

Salah satu kendala fundamental dalam pembuktian tindak pidana pemalsuan KTP adalah penentuan kualifikasi yuridis terhadap objek yang dipalsukan, apakah dikualifikasikan sebagai “surat” sebagaimana dimaksud dalam Pasal 263 KUHP atau sebagai “dokumen elektronik” sebagaimana diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016. Penentuan kualifikasi ini memiliki implikasi langsung terhadap pembuktian unsur objektif

tindak pidana serta pemilihan dasar hukum yang tepat dalam proses penuntutan.⁶ Secara normatif, Pasal 263 ayat (1) KUHP mensyaratkan adanya perbuatan membuat surat palsu atau memalsukan surat yang dapat menimbulkan suatu hak, perikatan, atau yang diperuntukkan sebagai alat bukti. Dalam konteks ini, KTP pada dasarnya memenuhi kualifikasi sebagai “surat”, karena merupakan dokumen resmi negara yang diterbitkan oleh pejabat berwenang dan berfungsi sebagai alat bukti identitas serta dasar untuk memperoleh berbagai hak administratif dan keperdataan. Namun, permasalahan muncul ketika KTP yang dipalsukan tidak lagi semata-mata berbentuk fisik, melainkan berasal dari data elektronik e-KTP yang dimanipulasi melalui sistem elektronik, kemudian dicetak dalam bentuk kartu fisik.

Sementara itu, UU ITE melalui Pasal 1 angka 4 mendefinisikan dokumen elektronik sebagai setiap informasi elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya yang dapat dilihat, ditampilkan, dan/atau didengar melalui komputer atau sistem elektronik. Lebih lanjut, Pasal 5 ayat (1) UU ITE menegaskan bahwa dokumen elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah. Ketentuan ini menunjukkan bahwa data e-KTP yang tersimpan dalam sistem kependudukan serta hasil cetaknya memiliki kedudukan hukum yang diakui dalam proses pembuktian.⁷ Namun, pengakuan normatif tersebut justru menimbulkan ambiguitas dalam praktik. Ketika pemalsuan terjadi pada tahap manipulasi data e-KTP dalam sistem elektronik, perbuatan tersebut secara normatif lebih tepat dijerat dengan Pasal 35 UU ITE jo. Pasal 51 ayat (1) UU ITE yang mengatur larangan manipulasi, penciptaan, atau perubahan dokumen elektronik agar dianggap seolah-olah data yang otentik. Sebaliknya, ketika hasil manipulasi tersebut dicetak dan digunakan sebagai KTP fisik untuk kepentingan tertentu, muncul pertanyaan apakah perbuatan tersebut

⁶ ari, D. P., & Hidayat, M. (2020). *Pemalsuan dokumen sebagai tindak pidana dan implikasinya terhadap kepastian hukum*. *Jurnal RechtsVinding*, 9(3), 421–436.

⁷ Barda Nawawi Arief. (2018). *Bunga rampai kebijakan hukum pidana*. Jakarta: Kencana Prenadamedia Group.

masih berada dalam rezim UU ITE atau telah beralih menjadi pemalsuan surat sebagaimana diatur dalam Pasal 263 KUHP. Ketidakjelasan batasan antara rezim hukum KUHP dan UU ITE ini diperparah oleh belum adanya pengaturan eksplisit yang mengatur pemalsuan dokumen kependudukan berbasis elektronik secara terintegrasi. Undang-Undang Nomor 24 Tahun 2013 tentang Administrasi Kependudukan memang mengatur larangan pemalsuan dokumen kependudukan, termasuk KTP dan e-KTP, namun pengaturannya lebih bersifat sektoral dan administratif, sehingga dalam praktik penegakan hukum pidana masih diperlukan penafsiran sistematis dengan ketentuan KUHP dan UU ITE.

Akibat dari ketidakpastian kualifikasi hukum tersebut, penegak hukum sering mengalami kendala dalam membuktikan unsur objektif tindak pidana, khususnya unsur “surat” atau “dokumen elektronik” yang dipalsukan. Pemilihan pasal yang tidak tepat berpotensi menimbulkan keberatan hukum dari pihak terdakwa dan melemahkan pembuktian di persidangan. Oleh karena itu, diperlukan pendekatan penafsiran hukum yang komprehensif dan harmonisasi regulasi agar pembuktian pemalsuan KTP berbasis teknologi digital cerdas dapat dilakukan secara efektif dan memberikan kepastian hukum.

b) Kendala Pembuktian Keaslian Data e-KTP

Kendala pembuktian keaslian data e-KTP dalam perkara pemalsuan dokumen berbasis teknologi digital cerdas tidak dapat dilepaskan dari kerangka regulasi yang berlaku di Indonesia. Secara normatif, e-KTP merupakan dokumen kependudukan yang memiliki kekuatan hukum sebagai alat bukti identitas resmi warga negara, sebagaimana ditegaskan dalam Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan sebagaimana telah diubah dengan Undang-Undang Nomor 24 Tahun 2013. Undang-undang ini menempatkan data kependudukan sebagai data yang bersifat strategis dan dilindungi oleh negara,

sehingga pengelolaannya dilakukan secara terpusat dan tunduk pada prinsip kerahasiaan, akurasi, serta keamanan sistem.⁸

Dalam konteks pembuktian pidana, pemalsuan e-KTP yang menyasar data kependudukan pada dasarnya dapat dijerat dengan ketentuan pemalsuan surat sebagaimana diatur dalam Pasal 263 KUHP, karena e-KTP merupakan dokumen yang menimbulkan hak dan digunakan sebagai alat bukti identitas. Namun, untuk membuktikan unsur “membuat surat palsu atau memalsukan surat”, jaksa penuntut umum harus menunjukkan adanya ketidaksesuaian antara data e-KTP yang digunakan oleh pelaku dengan data kependudukan resmi dalam sistem administrasi kependudukan nasional. Pada titik inilah pembuktian sangat bergantung pada akses terhadap database kependudukan yang secara hukum berada di bawah kewenangan pemerintah.

Keterbatasan akses terhadap data kependudukan tersebut berkaitan erat dengan ketentuan perlindungan data pribadi dan keamanan sistem elektronik. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 mengatur bahwa data elektronik dan sistem elektronik harus dijaga keamanannya dari penyalahgunaan. Ketentuan ini kemudian diperkuat dengan hadirnya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, yang menegaskan bahwa data kependudukan merupakan data pribadi yang bersifat spesifik dan hanya dapat diakses atau dibuka berdasarkan dasar hukum yang sah. Akibatnya, aparat penegak hukum tidak dapat secara bebas mengakses data e-KTP tanpa melalui prosedur hukum dan administratif tertentu.

Selain itu, dari perspektif hukum acara pidana, pengakuan terhadap alat bukti elektronik sebagaimana diatur dalam Pasal 5 ayat (1) dan ayat (2) UU ITE memberikan dasar hukum bahwa informasi elektronik dan/atau dokumen elektronik beserta hasil cetaknya merupakan alat bukti hukum yang sah. Namun,

⁸ Rahman, F., & Wibowo, A. (2023). *Pertanggungjawaban pidana terhadap pelaku pemalsuan identitas digital*. *Jurnal Hukum dan Pembangunan*, 53(1), 134–152.

pengakuan normatif ini belum sepenuhnya menjawab persoalan teknis pembuktian, khususnya terkait mekanisme verifikasi keaslian data e-KTP di persidangan. Untuk membuktikan keabsahan atau ketidakabsahan data tersebut, penegak hukum tetap memerlukan keterangan ahli dan dokumen resmi dari instansi kependudukan, yang proses perolehannya kerap terhambat oleh prosedur birokrasi dan keterbatasan koordinasi antarlembaga.

c) Kendala Pembuktian Unsur Kesengajaan dalam Pemalsuan KTP Digital

Unsur kesengajaan (*mens rea*) merupakan elemen fundamental dalam tindak pidana pemalsuan KTP digital, karena menentukan ada tidaknya pertanggungjawaban pidana pada diri pelaku. Hal ini sejalan dengan ketentuan Pasal 263 ayat (1) KUHP yang mensyaratkan adanya “maksud untuk menggunakan atau menyuruh orang lain menggunakan seolah-olah surat tersebut asli dan tidak dipalsukan”. Dengan demikian, pemalsuan KTP, termasuk yang berbasis teknologi digital, bukan sekadar dinilai dari adanya dokumen yang tidak sah, tetapi juga dari sikap batin pelaku yang secara sadar mengetahui dan menghendaki perbuatan pemalsuan tersebut.⁹

Dalam praktiknya, pembuktian unsur kesengajaan dalam pemalsuan KTP digital menghadapi kendala yang cukup serius. Pelaku kerap beralasan bahwa perubahan data kependudukan terjadi akibat kesalahan sistem, gangguan teknis, atau dilakukan oleh pihak ketiga yang memiliki akses terhadap sistem elektronik. Penggunaan perangkat lunak otomatis dan teknologi kecerdasan buatan semakin memperumit pembuktian, karena memungkinkan pelaku mengaburkan peran aktifnya dalam proses manipulasi data. Kondisi ini menyulitkan jaksa penuntut umum untuk menunjukkan hubungan langsung antara kehendak pelaku dan terjadinya pemalsuan data e-KTP.

⁹ Hasibuan, J., & Syam, S. (n.d.). *A legal analysis on online fraud using fake identity. Indonesian Journal of Multidisciplinary Science.*

Secara regulatif, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 mengakui karakter sistem elektronik yang dapat bekerja secara otomatis, sehingga pembuktian niat jahat tidak selalu dapat dilakukan secara langsung. Oleh karena itu, dalam praktik peradilan, pembuktian unsur kesengajaan sering dibangun melalui rangkaian alat bukti tidak langsung (*indirect evidence*), seperti jejak digital, riwayat akses sistem, pola penggunaan KTP palsu, serta keterangan ahli digital forensik. Pendekatan ini sejalan dengan berbagai putusan pengadilan yang menegaskan bahwa kesengajaan dapat disimpulkan dari keseluruhan fakta hukum yang terungkap di persidangan, tanpa harus dibuktikan melalui pengakuan terdakwa.

Menurut tanggapan penulis, kendala pembuktian unsur kesengajaan dalam pemalsuan KTP digital menunjukkan adanya kesenjangan antara konstruksi hukum pidana yang masih berorientasi pada perbuatan konvensional dan realitas kejahatan berbasis teknologi digital cerdas. Meskipun secara normatif unsur kesengajaan telah diatur dengan jelas dalam Pasal 263 KUHP, dalam praktik pembuktiannya diperlukan pendekatan yang lebih adaptif melalui pemanfaatan alat bukti elektronik dan keterangan ahli digital forensik. Penulis berpendapat bahwa hakim tidak seharusnya menilai kesengajaan secara sempit dan formalistik, melainkan menarik kesimpulan dari rangkaian fakta hukum yang saling berkaitan, seperti pola penggunaan identitas palsu, manfaat yang diperoleh pelaku, serta upaya menyembunyikan jejak digital. Dengan demikian, penegakan hukum terhadap pemalsuan KTP digital tetap dapat memberikan kepastian hukum dan rasa keadilan, tanpa mengabaikan prinsip kehati-hatian dan perlindungan terhadap hak-hak terdakwa.

d) Kendala Pembuktian Keterkaitan antara KTP Palsu dan Akibat Hukum

Kendala pembuktian keterkaitan antara penggunaan KTP palsu dan timbulnya akibat hukum perlu dikaitkan dengan kerangka regulasi yang berlaku dalam hukum positif Indonesia. Secara normatif, pemalsuan KTP dapat dijerat dengan

Pasal 263 KUHP karena KTP merupakan dokumen yang menimbulkan hak dan digunakan sebagai alat bukti identitas. Namun, ketika KTP palsu digunakan sebagai sarana untuk melakukan tindak pidana lain seperti penipuan, pembukaan rekening bank, atau pengajuan pinjaman daring penegak hukum juga harus memperhatikan ketentuan pidana lain yang mengatur akibat hukum lanjutan tersebut, seperti Pasal 378 KUHP tentang penipuan serta ketentuan dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016.

Dalam konteks transaksi elektronik, UU ITE mengakui informasi dan dokumen elektronik sebagai alat bukti yang sah sebagaimana diatur dalam Pasal 5 ayat (1) dan ayat (2). Ketentuan ini memberikan dasar hukum bagi penegak hukum untuk menelusuri keterkaitan antara penggunaan KTP palsu dengan akibat hukum yang timbul melalui sistem elektronik. Namun, pembuktian hubungan kausalitas tetap menjadi tantangan, karena sistem elektronik melibatkan berbagai pihak, mulai dari penyelenggara platform, lembaga keuangan, hingga pengguna akhir. Akibatnya, penggunaan KTP palsu sering kali hanya dipandang sebagai salah satu faktor dalam rangkaian proses, sehingga sulit ditentukan sebagai penyebab utama kerugian.

Selain itu, Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan sebagaimana telah diubah dengan Undang-Undang Nomor 24 Tahun 2013 menegaskan bahwa data kependudukan, termasuk KTP elektronik, memiliki kekuatan hukum dan wajib digunakan sebagai dasar dalam pelayanan publik dan transaksi tertentu. Dengan demikian, apabila KTP palsu digunakan dan menimbulkan akibat hukum, secara normatif terdapat hubungan langsung antara dokumen kependudukan yang tidak sah dengan terjadinya kerugian atau peristiwa hukum tertentu. Namun, dalam praktik pembuktian, penegak hukum tetap harus membuktikan bahwa penggunaan KTP palsu tersebut menjadi faktor penentu (*conditio sine qua non*) dalam terjadinya akibat hukum.

Lebih lanjut, regulasi perlindungan data pribadi sebagaimana diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi juga berpengaruh terhadap pembuktian hubungan kausalitas. Di satu sisi, undang-undang ini melindungi hak subjek data dan membatasi akses terhadap data pribadi. Di sisi lain, keterbatasan akses tersebut dapat memperlambat penelusuran jejak penggunaan KTP palsu dalam sistem elektronik. Oleh karena itu, meskipun kerangka regulasi telah menyediakan dasar hukum untuk menjerat pemalsuan KTP dan akibat hukumnya, efektivitas pembuktian sangat bergantung pada kemampuan penegak hukum dalam mengintegrasikan berbagai ketentuan hukum tersebut secara sistematis, sehingga hubungan antara KTP palsu dan akibat hukum dapat dibuktikan secara sah dan meyakinkan di persidangan.

D. KESIMPULAN

Pengaturan hukum pidana terkait pemalsuan KTP berbasis teknologi digital cerdas pada dasarnya telah memiliki dasar normatif yang memadai melalui Pasal 263 KUHP, UU ITE, dan UU Administrasi Kependudukan. Ketiga regulasi tersebut dapat diterapkan secara alternatif atau kumulatif berdasarkan prinsip *lex specialis derogat legi generali*. Namun, perbedaan dan keterpisahan pengaturan menuntut adanya harmonisasi serta penafsiran yang integratif. Kendala Dalam Pembuktian Tindak Pidana Pemalsuan Dokumen Yang Dilakukan Dengan Memanfaatkan Teknologi Digital Cerdas Berdasarkan Ketentuan Hukum Pidana Positif Di Indonesia, yaitu Kendala Penentuan Kualifikasi KTP sebagai "Surat" dan "Dokumen Elektronik", Kendala Pembuktian Keaslian Data e-KTP, Kendala Pembuktian Unsur Kesengajaan dalam Pemalsuan KTP Digital, serta Kendala Pembuktian Keterkaitan antara KTP Palsu dan Akibat Hukum. disarankan agar aparat penegak hukum meningkatkan kapasitas dan pemahaman terhadap karakteristik dokumen elektronik dan teknologi digital cerdas, khususnya dalam pembuktian pemalsuan KTP digital. Selain itu, diperlukan penguatan koordinasi antar lembaga penegak hukum dan instansi kependudukan, pemanfaatan forensik digital secara optimal, serta penafsiran hukum yang lebih progresif agar kendala pembuktian baik terkait kualifikasi KTP, keaslian data e-KTP,

unsur kesengajaan, maupun hubungan kausal dengan akibat hukum dapat diatasi secara efektif dan tetap menjamin kepastian hukum.

E. REFERENSI

- 1) Al- Qur'an dan terjemahan,(2009), Departemen Agama Republik Indonesia, Bogor, sabiq.
- 2) Andi Hamzah. (2005). Hukum pidana Indonesia: Pokok-pokoknya (ed. revisi). Jakarta: Rineka Cipta.
- 3) ari, D. P., & Hidayat, M. (2020). *Pemalsuan dokumen sebagai tindak pidana dan implikasinya terhadap kepastian hukum. Jurnal RechtsVinding*, 9(3), 421–436.
- 4) Barda Nawawi Arief. (2018). *Bunga rampai kebijakan hukum pidana*. Jakarta: Kencana Prenadamedia Group.
- 5) <https://irmapa.org/teknologi-ai-generatif-dan-ancaman-baru-pemalsuan-dokumen/>, Diakses pada 15 Oktober 2025.
- 6) Hamzah, A. (2008). *Delik-delik tertentu dalam KUHP*. Jakarta: Sinar Grafika
- 7) Hasibuan, J., & Syam, S. (n.d.). *A legal analysis on online fraud using fake identity. Indonesian Journal of Multidisciplinary Science*
- 8) Prasetyo, T., & Sulisty, H. (2021). *Pemalsuan dokumen elektronik dalam perspektif hukum pidana Indonesia. Jurnal Hukum Ius Quia Iustum*, 28(3), 487–505.
- 9) Rahman, F., & Wibowo, A. (2023). *Pertanggungjawaban pidana terhadap pelaku pemalsuan identitas digital. Jurnal Hukum dan Pembangunan*, 53(1), 134–152.
- 10) Setiawan, E., & Hartiwiningsih, H. (2025). *Optimizing the use of digital forensics and information technology in proving criminal acts of electronic document forgery in Indonesia. International Journal of Law, Crime and Justice*, 2(2), 75–86.

- 11) Widhaningroem, S., & Widowaty, Y. (2024). *Digital evidence tracing in the investigation of identity theft in the e-commerce era. Formosa Journal of Social Sciences (FJSS)*.
- 12) Zhang, C. J., Gill, A. Q., Liu, B., & Anwar, M. J. (2025). *AI-based identity fraud detection: A systematic review. arXiv*.