Al-Zayn: Jurnal Ilmu Sosial & Hukum e-ISSN 3026-2917
https://ejournal.yayasanpendidikandzurriyatulquran.id/index.php/AlZyn p-ISSN 3026-2925
Volume 4 Number 1, 2026
DOI: https://doi.org/10.61104/alz.v4i1. 3715

Penegakan Hukum terhadap Pelaku Pemalsuan Tanda Tangan Elektronik Pada Dokumen PDF dalam Perspektif UU ITE

Putu Ayu Masrini[1], Dewi Iryani[2], Nyoman Tio Rae[3]
Program Studi Magister Hukum, Universitas Bung Karno, Indonesia
Email Korespondens: ayumasrini92@gmail.com

Article received: 01 November 2025, Review process: 11 November 2025
Article Accepted: 25 Desmber 2025, Article published: 10 Januari 2026

ABSTRACT
The rapid development of digital technology has transformed the paradigm of evidentiary law in Indonesia, particularly regarding electronic signatures as substitutes for handwritten ones. On the one hand, electronic signatures enhance efficiency and legal certainty in electronic transactions. On the other hand, the ease of manipulating digital data creates new criminal challenges, notably electronic signature forgery in Portable Document Format (PDF) documents. This study aims to analyze the legal framework concerning perpetrators of electronic signature forgery under Indonesia's Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law) and its amendments, as well as to examine the enforcement mechanisms in such cybercrimes. Using a normative juridical approach, the research analyzes statutory provisions, legal doctrines, and relevant court decisions. The findings reveal that although the ITE Law provides a legal foundation for electronic signatures, law enforcement still encounters difficulties—particularly regarding authentication, digital identity verification, and the validity of electronic evidence. Thus, enhancing digital forensics capacity and regulatory coherence is essential to strengthen the integrity of electronic transactions and legal certainty.
Keywords: *Law Enforcement, Forgery, Electronic Signature, PDF Documents, ITE Law*
ABSTRAK
Perkembangan teknologi digital telah mengubah paradigma hukum pembuktian di Indonesia, terutama dalam konteks tanda tangan elektronik sebagai pengganti tanda tangan manual. Di satu sisi, tanda tangan elektronik memberikan efisiensi dan kepastian hukum dalam transaksi elektronik. Namun di sisi lain, kemudahan manipulasi data digital menimbulkan potensi kejahatan baru berupa pemalsuan tanda tangan elektronik pada dokumen Portable Document Format (PDF). Penelitian ini bertujuan untuk menganalisis bentuk pengaturan hukum terhadap pelaku pemalsuan tanda tangan elektronik dalam perspektif Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) beserta perubahannya, serta menelaah mekanisme penegakan hukum terhadap tindak pidana tersebut. Metode yang digunakan adalah pendekatan yuridis normatif, dengan menganalisis peraturan perundang-undangan, doktrin, dan putusan pengadilan yang relevan. Hasil penelitian menunjukkan bahwa walaupun UU ITE telah memberikan dasar hukum yang sah terhadap tanda tangan elektronik, mekanisme pembuktian dan penegakan hukum masih menghadapi tantangan, terutama dalam aspek keaslian identitas digital dan otentikasi sertifikat elektronik. Oleh karena itu, diperlukan pembaruan sistem verifikasi digital yang lebih kuat serta peningkatan kapasitas aparat penegak hukum dalam memahami forensik digital.
Kata Kunci: *Penegakan Hukum, Pemalsuan, Tanda Tangan Elektronik, Dokumen PDF, UU ITE)*

PENDAHULUAN

Hukum berfungsi sebagai pedoman hidup yang menjaga ketertiban dan keadilan dalam masyarakat. Dalam konteks negara hukum seperti Indonesia, keberadaan hukum tidak hanya menjadi pengatur hubungan sosial, tetapi juga instrumen perlindungan terhadap hak-hak individu. Sebagaimana ditegaskan dalam Pasal 1 ayat (3) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, "Negara Indonesia adalah negara hukum." Prinsip ini menuntut agar seluruh kegiatan sosial dan ekonomi, termasuk aktivitas di ruang digital, dilandasi oleh hukum yang pasti, adil, dan dapat ditegakkan.

Kemajuan teknologi informasi dan komunikasi membawa perubahan besar terhadap sistem hukum, khususnya dalam ranah pembuktian dan transaksi elektronik. Tanda tangan elektronik sebagai salah satu inovasi hukum digital hadir untuk menggantikan tanda tangan manual dalam dokumen fisik. Melalui Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dan Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, Indonesia mengakui tanda tangan elektronik sebagai alat autentikasi yang memiliki kekuatan hukum setara dengan tanda tangan konvensional, selama memenuhi unsur keaslian dan integritas data.

Namun, kemudahan ini tidak terlepas dari risiko penyalahgunaan. Salah satu bentuk kejahatan yang muncul seiring berkembangnya teknologi adalah pemalsuan tanda tangan elektronik pada dokumen digital, khususnya berformat Portable Document Format (PDF). Pemalsuan tersebut dilakukan dengan cara meniru, menyalin, atau memodifikasi tanda tangan digital tanpa hak, yang kemudian digunakan seolah-olah sah oleh pihak lain. Tindakan ini bukan hanya melanggar hak individu atas keaslian identitas elektronik, tetapi juga mengancam integritas sistem hukum elektronik dan kepercayaan publik terhadap transaksi digital.

Menurut data Kementerian Komunikasi dan Informatika, kasus pemalsuan dokumen digital dan tanda tangan elektronik meningkat hingga 35% dalam dua tahun terakhir, terutama pada dokumen kontrak bisnis dan surat perjanjian elektronik. Fenomena ini menunjukkan adanya ketimpangan antara norma hukum yang berlaku (das sollen) dengan praktik sosial (das sein) dalam dunia digital. Meskipun UU ITE telah menyediakan dasar hukum untuk penegakan, implementasinya di lapangan masih menghadapi hambatan teknis dan konseptual, terutama terkait pembuktian dan keabsahan sertifikat elektronik.

Lebih jauh, kejahatan pemalsuan tanda tangan elektronik dapat dikategorikan sebagai cybercrime atau tindak pidana siber, karena pelaksanaannya bergantung pada sistem komputer dan jaringan internet. Dalam konteks hukum pidana, tindakan ini berkaitan erat dengan Pasal 263 Kitab Undang-Undang Hukum Pidana (KUHP) yang mengatur pemalsuan surat, serta Pasal 35 dan Pasal 51 ayat (1) UU ITE yang mengatur pemalsuan informasi elektronik dan ancaman pidananya. Kombinasi antara norma klasik (KUHP) dan norma modern (UU ITE) menunjukkan adanya transformasi konsep hukum pidana menuju era digital, di mana objek hukum bukan lagi benda fisik, melainkan data dan identitas elektronik.

Selain itu, fenomena pemalsuan tanda tangan elektronik menimbulkan pertanyaan mendasar mengenai kepastian hukum dalam ranah digital. Gustav Radbruch dalam teori tiga nilai dasar hukum menyebutkan bahwa hukum harus menjamin keadilan, kepastian, dan kemanfaatan secara seimbang. Dalam konteks tanda tangan elektronik, kepastian hukum menjadi penting agar setiap transaksi digital dapat diakui keabsahannya di depan hukum. Tanpa adanya kepastian hukum, masyarakat akan kehilangan kepercayaan terhadap sistem hukum digital, dan potensi penyalahgunaan data akan semakin meningkat.

Secara sosiologis, lemahnya penegakan hukum terhadap kejahatan digital di Indonesia dipengaruhi oleh rendahnya tingkat pemahaman aparat penegak hukum terhadap bukti elektronik (*digital evidence*). Banyak penyidik dan jaksa masih berorientasi pada pola pembuktian konvensional yang menitikberatkan pada dokumen fisik, sementara bukti digital memerlukan metode analisis forensik yang lebih kompleks dan spesifik. Kondisi ini menyebabkan berbagai kasus pemalsuan tanda tangan elektronik tidak dapat dibuktikan secara efektif di pengadilan, sehingga pelaku kerap luput dari pertanggungjawaban hukum.

Bedasarkan permasalahan tersebut, penelitian ini berfokus pada dua isu utama. Pertama, bagaimana pengaturan hukum terhadap pelaku pemalsuan tanda tangan elektronik pada dokumen PDF menurut Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) serta peraturan terkait lainnya. Kedua, bagaimana mekanisme penegakan hukum terhadap tindak pidana pemalsuan tanda tangan elektronik, termasuk tantangan yang dihadapi aparat penegak hukum dalam praktik penerapannya.

Adapun tujuan dari penelitian ini adalah untuk menganalisis secara normatif dan konseptual kedudukan tanda tangan elektronik dalam sistem hukum Indonesia, serta merumuskan rekomendasi penguatan aspek regulatif dan institusional guna meningkatkan efektivitas penegakan hukum di era digital. Dengan demikian, hasil penelitian diharapkan dapat memberikan kontribusi terhadap pengembangan kebijakan hukum siber yang lebih responsif terhadap dinamika teknologi dan kebutuhan keadilan di masyarakat.

METODE

Penelitian ini menggunakan pendekatan yuridis normatif (doctrinal research) yang bertumpu pada kajian peraturan perundang-undangan, doktrin, dan asas-asas hukum yang relevan dengan tindak pidana pemalsuan tanda tangan elektronik. Pendekatan ini dipilih karena fokus utama penelitian adalah menelaah konsep, norma, dan penerapan hukum positif terhadap fenomena pemalsuan tanda tangan dalam dokumen PDF yang memanfaatkan sarana elektronik. Dalam konteks ini, peneliti mengkaji sinkronisasi antara das sollen (ketentuan ideal dalam norma UU ITE, UU PDP, dan KUHP) dengan das sein (realitas penerapan hukum dalam praktik penyidikan dan peradilan di Indonesia). Pendekatan yuridis normatif ini juga dilengkapi dengan pendekatan konseptual untuk memahami konstruksi filosofis dari keaslian tanda tangan elektronik dan pendekatan kasus (case approach) melalui analisis beberapa putusan pengadilan terkait pemalsuan

tanda tangan digital. **Jenis dan Sumber Data** Jenis data yang digunakan dalam penelitian ini adalah data sekunder yang terdiri dari tiga jenis bahan hukum. Pertama, bahan hukum primer, yaitu peraturan perundang-undangan yang secara langsung mengatur mengenai tanda tangan elektronik, antara lain: (1) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagaimana diubah dengan UU Nomor 19 Tahun 2016; (2) Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP); (3) Kitab Undang-Undang Hukum Pidana (KUHP); (4) Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Kedua, bahan hukum sekunder, yang mencakup literatur, jurnal hukum, hasil penelitian, pendapat para ahli, dan artikel ilmiah yang relevan dengan topik pemalsuan, identitas digital, serta penegakan hukum siber. Ketiga, bahan hukum tersier, seperti kamus hukum, ensiklopedia, dan indeks peraturan yang berfungsi untuk memperjelas istilah hukum maupun terminologi digital forensik. **Teknik Pengumpulan Data** Teknik pengumpulan data dilakukan melalui dua cara, yaitu: (1) Studi kepustakaan (library research) terhadap buku-buku hukum, artikel jurnal, dan publikasi resmi lembaga penegak hukum (misalnya Bareskrim Polri, Kominfo, dan Mahkamah Agung). (2) Telaah dokumen terhadap putusan pengadilan, laporan penyelidikan siber, serta berita resmi yang berkaitan dengan tindak pidana pemalsuan tanda tangan elektronik.

Tahapan analisis dilakukan secara sistematis melalui proses reduksi data, kategorisasi konsep hukum, serta penerapan analisis normatif deduktif, yaitu dengan menarik kesimpulan dari norma umum menuju penerapan pada kasus konkret. **Analisis Data** Analisis data dilakukan secara *kualitatif deskriptif* dengan menguraikan hasil temuan hukum dalam bentuk narasi argumentatif. Langkah-langkahnya mencakup: (1) Identifikasi norma hukum positif terkait unsur-unsur pemalsuan tanda tangan elektronik. (2) Interpretasi yuridis terhadap pasal-pasal UU ITE dan KUHP untuk menemukan unsur tindak pidana dan tanggung jawab hukum pelaku. (3) Analisis perbandingan antara konsep *electronic signature authenticity* dalam sistem hukum Indonesia dan rezim hukum internasional (misalnya *UNCITRAL Model Law on Electronic Commerce 1996*). (4) Sintesis hasil analisis untuk merumuskan model penegakan hukum yang ideal terhadap pelaku pemalsuan tanda tangan elektronik pada dokumen PDF.

HASIL DAN PEMBAHASAN

Analisis Penegakan Hukum terhadap Pelaku Pemalsuan Tanda Tangan Elektronik pada Dokumen PDF

Penegakan hukum terhadap pelaku pemalsuan tanda tangan elektronik pada dokumen PDF merupakan bentuk aktualisasi prinsip *equality before the law* di ranah siber. Pemalsuan tanda tangan elektronik sejatinya tidak hanya merupakan pelanggaran terhadap hak individu atas autentikasi dokumen, tetapi juga merupakan serangan terhadap kepercayaan publik (*public trust*) terhadap sistem transaksi digital. Dalam praktiknya, penegakan hukum atas kasus semacam ini

melibatkan tiga aspek utama: **(1) aspek normatif**, **(2) aspek kelembagaan**, dan **(3) aspek teknis pembuktian**.

1) Aspek Normatif

Secara normatif, dasar hukum yang digunakan adalah Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016. Pasal 5 dan 11 UU ITE menegaskan bahwa tanda tangan elektronik memiliki kekuatan hukum dan akibat hukum yang sah sepanjang memenuhi syarat keaslian dan integritas data.

Dalam konteks pemalsuan, Pasal 35 UU ITE mengatur bahwa setiap orang dengan sengaja dan tanpa hak memanipulasi, mengubah, menambah, mengurangi, melakukan transmisi elektronik dengan tujuan menimbulkan akibat hukum atas data elektronik orang lain dapat dikenai pidana penjara paling lama 12 tahun dan/atau denda paling banyak Rp12 miliar. Ketentuan ini secara substansial paralel dengan delik pemalsuan sebagaimana diatur dalam Pasal 263 KUHP, namun dengan penyesuaian terhadap objek digital.

Dari sisi hukum acara, proses pembuktian tindak pidana ini mengacu pada UU Nomor 8 Tahun 1981 tentang Hukum Acara Pidana (KUHAP), namun dengan tambahan bukti elektronik sebagaimana diakui dalam Pasal 5 ayat (1) UU ITE. Dengan demikian, tanda tangan elektronik yang dipalsukan dapat dijadikan bukti sah bila dapat dibuktikan keterkaitannya secara forensik digital dengan pelaku.

2) Aspek Kelembagaan

Penegakan hukum di bidang ini melibatkan beberapa lembaga, yaitu: Kementerian Komunikasi dan Informatika (Kominfo), Badan Siber dan Sandi Negara (BSSN), Polri (Direktorat Tindak Pidana Siber), serta Kejaksaan dan Pengadilan Negeri. Dalam banyak kasus, koordinasi antarlembaga masih menjadi kendala. Salah satu permasalahan mendasar adalah belum optimalnya peran BSSN sebagai otoritas penyelenggara sertifikasi tanda tangan elektronik (Certification Authority).

Kondisi ini menyebabkan banyak tanda tangan digital yang beredar di masyarakat tidak melalui sistem sertifikasi resmi, sehingga menyulitkan aparat penegak hukum dalam proses autentikasi saat terjadi dugaan pemalsuan. Sebagai contoh, dalam Putusan Pengadilan Negeri Jakarta Selatan No. 807/Pid.Sus/2021/PN Jkt.Sel, aparat penegak hukum mengalami kesulitan dalam membuktikan keterlibatan terdakwa karena tanda tangan elektronik yang digunakan tidak disertifikasi oleh penyelenggara resmi. Kasus ini menggambarkan lemahnya sistem verifikasi dan kebutuhan mendesak untuk memperkuat digital forensic chain of custody.

3) Aspek Teknis Pembuktian

Pembuktian dalam tindak pidana pemalsuan tanda tangan elektronik memerlukan keahlian forensik digital yang tinggi. BSSN telah mengembangkan Digital Signature Verification System (DSVS), namun penggunaannya belum terintegrasi penuh dengan sistem penyidikan Polri dan Kejaksaan. Akibatnya,

validitas tanda tangan elektronik sering kali masih diuji secara manual dengan alat verifikasi pihak ketiga yang tidak terstandar.

Analisis hukum dari kondisi ini menunjukkan bahwa penegakan hukum terhadap pemalsuan tanda tangan elektronik belum mencapai efektivitas yang diharapkan. Menurut teori penegakan hukum Lawrence M. Friedman, efektivitas hukum ditentukan oleh tiga subsistem: legal structure, legal substance, dan legal culture. Dalam konteks Indonesia, ketiga subsistem ini belum bekerja secara sinergis—substansi hukum masih lemah dalam detail pengaturan, struktur kelembagaan belum solid, dan budaya hukum masyarakat digital masih rendah.

Perspektif UU ITE terhadap Pemalsuan Tanda Tangan Elektronik dan Perlindungan Hukumnya Secara normatif, UU ITE memang telah mengakui tanda tangan elektronik sebagai instrumen sah dalam transaksi elektronik (Pasal 11), tetapi belum memberikan pengaturan yang spesifik tentang *pemalsuan tanda tangan elektronik* secara tersendiri.

1) Analisis Kecukupan Normatif

Jika dibandingkan dengan konsep tanda tangan konvensional yang dilindungi oleh Pasal 263 KUHP, tanda tangan elektronik memiliki karakteristik yang berbeda. Ia berbasis teknologi kriptografi dan sertifikat digital, sehingga pemalsuannya sering kali tidak bersifat fisik tetapi digital (logical forgery). Namun, UU ITE tidak secara eksplisit mengatur delik pemalsuan digital, melainkan memasukkannya dalam kategori umum manipulasi data elektronik (Pasal 35).

Hal ini menimbulkan kekosongan norma (normative gap) yang berpotensi melemahkan perlindungan hukum bagi korban. Banyak ahli hukum siber, seperti Andri Hamzah dan Ahmad M. Ramli, berpendapat bahwa Indonesia memerlukan pasal khusus yang mengatur pemalsuan tanda tangan elektronik sebagai cyber forgery tersendiri.

2) Perbandingan dengan negara lain

Jika dikomparasikan dengan regulasi di luar negeri, pengaturan Indonesia masih relatif umum.

1) Singapura, melalui Electronic Transactions Act (ETA) 2010, secara tegas menetapkan pemalsuan tanda tangan digital sebagai tindak pidana dengan sanksi pidana hingga 7 tahun penjara.
2) Uni Eropa, melalui eIDAS Regulation (EU) No. 910/2014, mewajibkan negara anggota memiliki sistem sertifikasi tanda tangan digital yang diakui lintas yurisdiksi dan menempatkan tanggung jawab hukum langsung pada penyedia sertifikasi (Qualified Trust Service Providers).

Dari dua model tersebut, terlihat bahwa perlindungan hukum yang kuat terhadap tanda tangan elektronik harus disertai sistem sertifikasi dan tanggung jawab hukum penyelenggara yang ketat.

SIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan mengenai penegakan hukum terhadap pemalsuan tanda tangan elektronik pada dokumen PDF, dapat disimpulkan beberapa hal penting sebagai berikut:

Pertama, penegakan hukum terhadap pemalsuan tanda tangan elektronik pada dokumen PDF masih menghadapi berbagai kendala, terutama dalam aspek pembuktian dan penerapan norma hukum positif. Meskipun Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 telah mengatur keabsahan tanda tangan elektronik, namun praktik di lapangan menunjukkan adanya kekosongan norma teknis terkait mekanisme pembuktian autentisitas tanda tangan digital di pengadilan. Aparat penegak hukum sering mengalami kesulitan dalam menilai integritas dokumen elektronik karena belum adanya standar nasional yang seragam dalam verifikasi digital forensik. Akibatnya, kondisi *das sein* (realitas praktik) belum sepenuhnya mencerminkan *das sollen* (ketentuan normatif) sebagaimana yang diharapkan oleh sistem hukum. Kedua, perlindungan hukum terhadap pemilik tanda tangan elektronik masih bersifat reaktif dan belum mengarah pada upaya preventif. Penegakan hukum cenderung dilakukan setelah terjadinya pelanggaran, sementara sistem pengamanan tanda tangan digital belum diwajibkan secara nasional melalui kebijakan yang tegas. Negara seharusnya tidak hanya hadir dalam bentuk pendekatan represif melalui pemberian sanksi pidana, tetapi juga membangun mekanisme keamanan data dan autentikasi elektronik yang mampu mencegah pemalsuan sejak awal. Tanpa adanya regulasi pelengkap serta kolaborasi yang kuat antara pemerintah, penyelenggara sertifikasi elektronik, dan lembaga penegak hukum, maka ancaman kejahatan siber seperti pemalsuan tanda tangan digital akan semakin meningkat seiring dengan pesatnya digitalisasi dalam administrasi publik maupun privat.

DAFTAR PUSTAKA

Asshiddiqie, J. (2021). *Hukum tata negara dan pilar-pilar demokrasi*. Jakarta: Sinar Grafika.

Fitriani, D., & Setyaningsih, R. (2023). Perlindungan hukum terhadap pemilik tanda tangan elektronik pada transaksi digital. *Jurnal Hukum dan Pembangunan, 53*(2), 134–150.

Hamzah, A. (2019). *Hukum pidana Indonesia*. Jakarta: Sinar Grafika.

Hidayat, R. (2023). Analisis yuridis pembuktian dokumen elektronik dalam perkara pidana. *Jurnal Rechtsvinding, 12*(1), 45–63.

Kementerian Komunikasi dan Informatika Republik Indonesia. (2025, Oktober 10). *Pedoman penyelenggaraan sistem elektronik dan pengamanan data digital*. https://kominfo.go.id

Lestari, Y. (2023). Kepastian hukum terhadap tanda tangan elektronik dalam perspektif UU ITE. *Jurnal Lex Renaissance, 8*(1), 27–41.

Mahkamah Agung Republik Indonesia. (2024). *Laporan tahunan penegakan hukum bidang ITE tahun 2023*. Jakarta: Mahkamah Agung RI.

Marzuki, P. M. (2021). *Penelitian hukum*. Jakarta: Kencana Prenada Media Group.

Nugraha, B. A. (2023). Penegakan hukum terhadap cybercrime di Indonesia dalam perspektif kepastian hukum. *Jurnal Mimbar Hukum, 35*(2), 201–217.

Organisation for Economic Co-operation and Development (OECD). (2022). *Digital security and the law: Governance challenges in the 21st century*. Paris: OECD Publishing.

Raharjo, S. (2020). *Ilmu hukum*. Bandung: Citra Aditya Bakti.

Republik Indonesia. (2008). *Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58.

Republik Indonesia. (2016). *Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251.

Republik Indonesia. (2019). *Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik*.

Republik Indonesia. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi*. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 182.

Republik Indonesia. (n.d). *Kitab Undang-Undang Hukum Pidana (KUHP)*.

Soekanto, S., & Mamudji, S. (2021). *Penelitian hukum normatif: Suatu tinjauan singkat*. Jakarta: RajaGrafindo Persada.

Suryawan, I. M. (2022). Digital forensics sebagai alat bukti dalam penegakan hukum siber. *Jurnal Hukum dan Teknologi Indonesia, 6*(1), 65–82.

Wahidin, S. (2022). *Cybercrime dan penegakan hukum di Indonesia*. Yogyakarta: Deepublish.

Wardana, B. (2023). Pemalsuan identitas digital dalam sistem elektronik: Analisis kriminologi dan hukum. *Jurnal Hukum IUS QUIA IUSTUM, 30*(1), 113–130.

Risdwiyanto, A. & Kurniyati, Y. (2015). Strategi Pemasaran Perguruan Tinggi Swasta di Kabupaten Sleman Yogyakarta Berbasis Rangsangan Pemasaran. *Jurnal Maksipreneur: Manajemen, Koperasi, dan Entrepreneurship*, *5*(1), 1-23. http://dx.doi.org/10.30588/SOSHUMDIK.v5i1.142.

Bator, R. J., Bryan, A. D., & Schultz, P. W. (2011). Who Gives a Hoot?: Intercept Surveys of Litterers and Disposers. Environment and Behavior, 43*(3), 295–315. https://doi.org/10.1177/0013916509356884*