

Keabsahan dan Kekuatan Pembuktian Tanda Tangan Digital dalam Transaksi E-Commerce

Chandra Johan Alen¹, Aturkian Laia²

Ilmu Hukum, Hukum, Universitas Dirgantara Marsekal Suryadarma, Jakarta Timur, Indonesia¹

Ilmu Hukum, Hukum, Universitas Dirgantara Marsekal Suryadarma, Jakarta Timur, Indonesia²

*Email Korespodensi: johanalen01@gmail.com

Sejarah Artikel:

Diterima 04-07-2026
Disetujui 11-07-2026
Diterbitkan 13-07-2026

ABSTRACT

The growth of e-commerce has transformed private law agreements and evidence through electronic signatures (E-signatures). Despite recognition under the UU ITE, classifications of certified and uncertified E-signatures and their evidentiary value still pose normative and practical challenges. This normative juridical research applies statutory, conceptual, and case approaches to analyze the regulation, validity requirements, evidentiary strength, and implementation challenges of E-signatures to ensure legal certainty and party protection. Primary legal sources include the Indonesian Civil Code, UU ITE, PP 71/2019, and Permenkominformo 11/2022. The results show that E-signatures are legally valid if they meet Article 11 of the UU ITE and PP 71/2019. Their evidentiary value equals other electronic evidence, though their weight depends heavily on authentication, system integrity, and Electronic Certification Provider reliability. E-signature effectiveness in court ultimately relies on technical standardization, digital-legal literacy, and consistent evidentiary practices.

Keywords: digital signature; electronic signature; e-commerce; electronic evidence; legal certainty.

ABSTRAK

Perkembangan e-commerce mengubah pola perjanjian dan pembuktian hukum privat melalui instrumen tanda tangan elektronik (TTE). Meskipun diakui UU ITE, klasifikasi TTE tersertifikasi dan tidak tersertifikasi serta kekuatan pembuktiannya masih menyisakan problem normatif dan praktis. Penelitian yuridis normatif dengan pendekatan perundang-undangan, konseptual, dan kasus ini bertujuan menganalisis pengaturan, syarat keabsahan, kekuatan pembuktian, serta tantangan implementasi TTE demi kepastian hukum dan perlindungan para pihak. Bahan hukum primer mencakup KUHPerdara, UU ITE, PP 71/2019, dan Permenkominformo 11/2022. Hasil penelitian menunjukkan TTE sah secara hukum jika memenuhi Pasal 11 UU ITE dan PP 71/2019. Kekuatan pembuktiannya setara alat bukti elektronik lain, tetapi bobotnya sangat dipengaruhi unsur autentikasi, integritas sistem, dan reliabilitas Penyelenggara Sertifikasi Elektronik. Efektivitas TTE di pengadilan masih bergantung pada standardisasi teknis, literasi hukum-digital, dan konsistensi praktik pembuktian.

Katakunci: tanda tangan digital; tanda tangan elektronik; e-commerce; alat bukti elektronik; kepastian hukum

PENDAHULUAN

Transformasi digital telah mendorong perubahan mendasar dalam pola hubungan hukum masyarakat, khususnya pada sektor perdagangan elektronik. *E-commerce* tidak lagi sekadar menjadi alternatif transaksi, melainkan telah berkembang menjadi salah satu arsitektur utama aktivitas ekonomi modern (Makarim, 2020; Ramli, 2022). Dalam transaksi elektronik, para pihak tidak selalu hadir secara fisik, tidak bertemu secara langsung, dan kerap bersepakat melalui platform digital yang memediasi proses penawaran, penerimaan, pembayaran, hingga pengiriman barang atau jasa. Konsekuensinya, persoalan autentikasi identitas, persetujuan kehendak, keutuhan dokumen, dan pembuktian menjadi isu sentral dalam hukum kontrak elektronik.

Pada konteks hukum perjanjian, tanda tangan secara tradisional dipahami sebagai sarana identifikasi penanda tangan sekaligus bentuk persetujuan atas isi dokumen. Dalam transaksi konvensional, tanda tangan basah memiliki fungsi pembuktian yang kuat karena secara fisik dilekatkan pada dokumen yang ditandatangani (Subekti, 2001; Mertokusumo, 2009). Akan tetapi, dalam ekosistem *e-commerce*, mekanisme tersebut tidak selalu dapat dipertahankan. Kehadiran tanda tangan digital atau tanda tangan elektronik kemudian menjadi instrumen substitusi yang memungkinkan proses autentikasi, persetujuan, dan pembuktian dilakukan secara elektronik tanpa meniadakan validitas hukum transaksi. Oleh karena itu, pengakuan hukum terhadap tanda tangan elektronik merupakan prasyarat penting bagi kepastian dan keamanan transaksi digital.

Dalam hukum positif Indonesia, pengakuan terhadap informasi elektronik, dokumen elektronik, dan tanda tangan elektronik telah ditegaskan sejak lahirnya Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yang kemudian diubah melalui Undang-Undang Nomor 19 Tahun 2016 dan terakhir Undang-Undang Nomor 1 Tahun 2024 (Republik Indonesia, 2024). UU ITE menempatkan tanda tangan elektronik sebagai instrumen hukum yang sah sepanjang memenuhi persyaratan tertentu. Lebih lanjut, Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP 71/2019) dan Peraturan Menteri Komunikasi dan Informatika Nomor 11 Tahun 2022 tentang Tata Kelola Penyelenggaraan Sertifikasi Elektronik memberikan kerangka operasional mengenai sertifikat elektronik, Penyelenggara Sertifikasi Elektronik (PSrE), validasi, preservasi, dan tata kelola teknis tanda tangan elektronik tersertifikasi. Secara normatif, rezim ini menunjukkan bahwa hukum Indonesia telah bergerak dari paradigma pembuktian berbasis kertas menuju rezim pembuktian elektronik yang lebih adaptif terhadap kebutuhan ekonomi digital (Republik Indonesia, 2008; Republik Indonesia, 2019; Kementerian Komunikasi dan Informatika, 2022).

Meskipun demikian, pengakuan normatif tidak serta-merta menyelesaikan seluruh persoalan. Pertama, masih terdapat kerancuan konseptual di masyarakat maupun praktik bisnis mengenai perbedaan antara “tanda tangan elektronik” dan “tanda tangan digital”. Dalam praktik, kedua istilah sering dipertukarkan, padahal secara teknis tanda tangan digital merupakan salah satu bentuk tanda tangan elektronik yang menggunakan teknik kriptografi asimetris dan umumnya terhubung dengan sertifikat elektronik (Mansur & Gultom, 2014). Kedua, tidak semua bentuk tanda tangan elektronik memiliki bobot pembuktian yang sama. UU ITE memang tidak menutup kemungkinan pengakuan terhadap tanda tangan elektronik non-tersertifikasi, tetapi dalam sengketa, kualitas pembuktiannya dapat berbeda dengan tanda tangan elektronik tersertifikasi yang didukung PSrE dan mekanisme verifikasi formal. Ketiga, sengketa *e-commerce* seringkali melibatkan isu pembuktian yang kompleks: apakah benar para pihak menyetujui kontrak; apakah akun pengguna dibajak; apakah sertifikat elektronik valid; apakah dokumen telah diubah setelah ditandatangani; dan siapa yang menanggung risiko jika sistem elektronik mengalami gangguan.

Permasalahan tersebut menunjukkan bahwa keabsahan tanda tangan digital tidak dapat dipahami hanya sebagai persoalan “diakui atau tidak diakui oleh undang-undang”. Yang jauh lebih penting adalah bagaimana hukum mengonstruksi syarat sah tanda tangan digital, bagaimana posisi tanda tangan tersebut dalam sistem pembuktian perdata Indonesia, dan sejauh mana mekanisme hukum yang ada mampu memberi perlindungan bagi pelaku usaha maupun konsumen dalam sengketa transaksi elektronik. Dalam konteks ini, hukum pembuktian klasik yang selama ini berorientasi pada alat bukti surat, saksi, persangkaan, pengakuan, dan sumpah sebagaimana diatur dalam Pasal 1866 Kitab Undang-Undang Hukum Perdata (KUHPerdata) perlu dibaca secara sistematis bersama perkembangan alat bukti elektronik sebagaimana diakui UU ITE (Budhijanto, 2018).

Sejumlah penelitian terdahulu telah membahas tanda tangan elektronik dari berbagai sudut. Ada penelitian yang menitikberatkan pada aspek keabsahan tanda tangan elektronik berdasarkan Pasal 11 UU ITE; ada pula yang mengkaji fungsi Penyelenggara Sertifikasi Elektronik dalam menjamin validitas tanda tangan elektronik tersertifikasi; sementara penelitian lain menyoroti pembuktian dokumen elektronik dalam sengketa perdata dan pidana. Namun demikian, sebagian kajian masih cenderung berhenti pada uraian normatif bahwa tanda tangan elektronik “sah” menurut UU ITE, tanpa mengurai secara lebih mendalam relasi antara syarat keabsahan, klasifikasi tanda tangan elektronik, kekuatan pembuktian, serta problem implementasinya dalam transaksi *e-commerce* yang bersifat massal, lintas platform, dan rentan penyalahgunaan data. Selain itu, perubahan lanskap regulasi melalui PP 71/2019, penguatan tata kelola PSrE, serta pembaruan materi hukum lewat UU Nomor 1 Tahun 2024 menuntut pembacaan yang lebih mutakhir dan sistematis.

Berdasarkan latar belakang tersebut, artikel ini memfokuskan kajian pada empat rumusan masalah. Pertama, bagaimana pengaturan hukum tanda tangan digital atau tanda tangan elektronik dalam sistem hukum Indonesia? Kedua, bagaimana syarat keabsahan tanda tangan digital dalam transaksi *e-commerce*? Ketiga, bagaimana kekuatan pembuktian tanda tangan digital sebagai alat bukti elektronik dalam sengketa perdata atau transaksi elektronik? Keempat, apa saja tantangan implementasi dan persoalan kepastian hukum dalam penggunaan tanda tangan digital pada transaksi *e-commerce*? Pertanyaan-pertanyaan tersebut penting dijawab karena keberhasilan ekosistem perdagangan digital tidak hanya bergantung pada inovasi teknologi, tetapi juga pada jaminan kepastian hukum, keandalan pembuktian, dan perlindungan hak para pihak yang bertransaksi secara elektronik.

Secara akademik, penelitian ini penting untuk memperkaya diskursus hukum siber, hukum pembuktian, dan hukum perjanjian di Indonesia. Secara praktis, penelitian ini diharapkan memberi kontribusi bagi pelaku usaha, konsumen, penyelenggara platform, praktisi hukum, dan pembentuk kebijakan dalam merumuskan tata kelola transaksi elektronik yang lebih akuntabel. Dengan demikian, penelitian mengenai keabsahan dan kekuatan pembuktian tanda tangan digital dalam transaksi *e-commerce* bukan semata kajian teknis, melainkan bagian dari upaya membangun rezim hukum digital yang menjamin keadilan, keamanan, dan kepastian hukum.

METODE PENELITIAN

Penelitian ini merupakan penelitian hukum yuridis normatif, yaitu penelitian yang menelaah hukum sebagai norma, asas, doktrin, dan putusan yang relevan dengan isu yang diteliti. Fokus penelitian tidak diarahkan pada pengukuran statistik perilaku pelaku usaha atau konsumen, melainkan pada konstruksi normatif mengenai keabsahan dan kekuatan pembuktian tanda tangan digital dalam transaksi *e-commerce*,

serta bagaimana norma tersebut seharusnya diterapkan untuk menjawab problem sengketa elektronik.

Pendekatan yang digunakan meliputi tiga pendekatan. Pertama, pendekatan perundang-undangan (*statute approach*), yakni dengan menelaah UUD NRI 1945, Kitab Undang-Undang Hukum Perdata, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta perubahannya, Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, Peraturan Menteri Komunikasi dan Informatika Nomor 11 Tahun 2022 tentang Tata Kelola Penyelenggaraan Sertifikasi Elektronik, serta ketentuan hukum acara dan pembuktian yang relevan. Kedua, pendekatan konseptual (*conceptual approach*), yang digunakan untuk menelaah konsep tanda tangan elektronik, tanda tangan digital, autentikasi, integritas data, *non-repudiation*, kepastian hukum, pembuktian elektronik, dan perlindungan hukum dalam kontrak elektronik. Ketiga, pendekatan kasus (*case approach*), yakni dengan menelaah praktik sengketa dan persoalan pembuktian elektronik yang relevan dalam konteks transaksi digital dan penggunaan tanda tangan elektronik.

Bahan hukum yang digunakan terdiri atas bahan hukum primer, sekunder, dan tersier. Bahan hukum primer meliputi peraturan perundang-undangan dan putusan pengadilan yang relevan. Bahan hukum sekunder meliputi buku-buku hukum siber, hukum perjanjian, hukum pembuktian, artikel jurnal, dan penelitian terdahulu yang membahas tanda tangan elektronik, *e-commerce*, serta alat bukti elektronik. Bahan hukum tersier berupa kamus hukum, ensiklopedia, dan sumber penunjang lain untuk memperjelas terminologi.

Teknik pengumpulan bahan hukum dilakukan melalui studi kepustakaan. Bahan-bahan hukum kemudian dianalisis secara kualitatif deskriptif-analitis, yaitu dengan menginventarisasi norma yang berlaku, menafsirkan hubungan antarketentuan, menguji kesesuaian norma dengan praktik *e-commerce*, serta menarik argumentasi hukum atas persoalan keabsahan dan pembuktian tanda tangan digital. Analisis dilakukan secara sistematis dari aspek pengaturan hukum, syarat keabsahan, kekuatan pembuktian, hingga tantangan implementasi. Dengan metode tersebut, penelitian ini diharapkan mampu menghasilkan argumentasi hukum yang komprehensif dan relevan bagi pengembangan hukum transaksi elektronik di Indonesia

HASIL DAN PEMBAHASAN

A. Pengaturan Hukum Tanda Tangan Digital dalam Sistem Hukum Indonesia

1. Pengakuan terhadap Dokumen Elektronik dan Tanda Tangan Elektronik

Fondasi normatif pengakuan tanda tangan digital dalam hukum Indonesia berangkat dari pengakuan terhadap informasi elektronik dan dokumen elektronik sebagai objek hukum yang memiliki akibat hukum. Pasal 5 ayat (1) UU ITE menegaskan bahwa informasi elektronik dan/atau dokumen elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah. Ketentuan ini penting karena menggeser paradigma pembuktian dari yang semula bertumpu pada dokumen kertas menuju pengakuan terhadap dokumen elektronik sebagai alat bukti mandiri. Pasal 5 ayat (2) UU ITE bahkan menegaskan bahwa informasi elektronik dan/atau dokumen elektronik merupakan perluasan dari alat bukti yang sah sesuai hukum acara yang berlaku (Republik Indonesia, 2008).

Pengakuan terhadap alat bukti elektronik tersebut kemudian dilengkapi dengan pengakuan terhadap tanda tangan elektronik. Pasal 1 angka 12 UU ITE mendefinisikan tanda tangan elektronik sebagai tanda tangan yang terdiri atas informasi elektronik yang dilekatkan, terasosiasi, atau terkait dengan informasi elektronik lainnya yang digunakan sebagai alat verifikasi dan autentikasi. Dari

definisi ini terlihat bahwa fungsi utama tanda tangan elektronik bukan semata “pengganti paraf atau coretan tanda tangan”, melainkan sebagai instrumen verifikasi identitas dan autentikasi persetujuan dalam dokumen elektronik (Makarim, 2020).

Secara normatif, keberadaan tanda tangan elektronik juga berkaitan erat dengan Pasal 1320 KUHPerdata mengenai syarat sah perjanjian. Dalam transaksi *e-commerce*, tanda tangan elektronik tidak menggantikan unsur sepakat, cakupan, objek tertentu, dan *causa* yang halal, tetapi berfungsi sebagai medium pembuktian bahwa kesepakatan memang telah diberikan oleh pihak tertentu (Subekti, 2001). Dengan demikian, tanda tangan elektronik tidak boleh dipahami berdiri sendiri; ia bekerja dalam relasi dengan hukum perjanjian, hukum pembuktian, dan hukum teknologi informasi.

2. Syarat Keabsahan Tanda Tangan Elektronik Menurut UU ITE

Pasal 11 ayat (1) UU ITE merupakan norma sentral mengenai keabsahan tanda tangan elektronik. Ketentuan ini menyatakan bahwa tanda tangan elektronik memiliki kekuatan hukum dan akibat hukum yang sah sepanjang memenuhi persyaratan:

- a) data pembuatan tanda tangan elektronik terkait hanya kepada penanda tangan;
- b) data pembuatan tanda tangan elektronik pada saat proses penandatanganan elektronik hanya berada dalam kuasa penanda tangan;
- c) segala perubahan terhadap tanda tangan elektronik yang terjadi setelah waktu penandatanganan dapat diketahui;
- d) segala perubahan terhadap informasi elektronik yang terkait dengan tanda tangan elektronik tersebut setelah waktu penandatanganan dapat diketahui;
- e) terdapat cara tertentu yang dipakai untuk mengidentifikasi siapa penandatanggannya; dan
- f) terdapat cara tertentu untuk menunjukkan bahwa penanda tangan telah memberikan persetujuan terhadap informasi elektronik yang terkait.

Dari ketentuan tersebut dapat ditarik beberapa unsur penting. Pertama, hukum menuntut adanya keterikatan eksklusif antara data pembuat tanda tangan dan penanda tangan. Artinya, sistem tanda tangan elektronik harus mampu menunjukkan bahwa *signature creation data* berada dalam penguasaan penanda tangan dan tidak dapat digunakan sembarang pihak. Kedua, hukum mensyaratkan integritas tanda tangan maupun dokumen elektronik. Setiap perubahan pasca-penandatanganan harus dapat dideteksi. Ketiga, hukum mensyaratkan autentikasi identitas dan indikasi persetujuan. Dua unsur ini sangat penting dalam sengketa *e-commerce*, karena inti sengketa biasanya terletak pada apakah benar pihak tertentu telah menyetujui suatu kontrak atau transaksi.

Apabila dicermati, syarat dalam Pasal 11 UU ITE menunjukkan bahwa pembentuk undang-undang mengadopsi pendekatan *functional equivalence*, yakni tidak menuntut bentuk fisik tanda tangan tertentu, tetapi menuntut agar fungsi hukum tanda tangan tetap terpenuhi: identifikasi, persetujuan, integritas, dan keterkaitan dengan penanda tangan. Dengan pendekatan ini, hukum Indonesia relatif terbuka terhadap berbagai model tanda tangan elektronik, asalkan persyaratan fungsionalnya dapat dibuktikan.

3. Pengaturan Lebih Lanjut dalam PP 71/2019 dan Permen Kominfo 11/2022

PP 71/2019 memperinci rezim hukum tanda tangan elektronik, khususnya terkait klasifikasi, tata kelola sertifikat elektronik, dan penyelenggara sertifikasi elektronik. Pasal 60 PP 71/2019 membedakan tanda tangan elektronik menjadi dua, yaitu tanda tangan elektronik

tersertifikasi dan tanda tangan elektronik tidak tersertifikasi. Tanda tangan elektronik tersertifikasi dibuat dengan menggunakan jasa Penyelenggara Sertifikasi Elektronik (PSrE) Indonesia dan dibuktikan dengan sertifikat elektronik. Sementara itu, tanda tangan elektronik tidak tersertifikasi pada dasarnya tetap dimungkinkan, tetapi tidak memperoleh dukungan verifikasi formal melalui PSrE sebagaimana tanda tangan elektronik tersertifikasi (Republik Indonesia, 2019).

Pembedaan ini sangat penting. Dalam perspektif keabsahan, UU ITE tidak secara eksplisit menyatakan bahwa hanya tanda tangan elektronik tersertifikasi yang sah. Artinya, tanda tangan elektronik tidak tersertifikasi tetap dapat diakui selama memenuhi syarat Pasal 11 UU ITE. Namun, dalam perspektif pembuktian, tanda tangan elektronik tersertifikasi memiliki posisi yang lebih kuat karena didukung sertifikat elektronik, infrastruktur kriptografi, identifikasi pemilik sertifikat, serta jejak audit (*audit trail*) yang lebih dapat diverifikasi.

Permen Kominfo Nomor 11 Tahun 2022 kemudian mengatur tata kelola penyelenggaraan sertifikasi elektronik secara lebih teknis, termasuk kedudukan PSrE Indonesia, penerbitan sertifikat elektronik, pengelolaan data pembuatan tanda tangan elektronik, validasi, preservasi, dan bukti keabsahan tanda tangan elektronik (Kementerian Komunikasi dan Informatika, 2022). Regulasi ini menunjukkan bahwa pembuktian tanda tangan digital tidak hanya berhenti pada teks UU ITE, tetapi bergantung pada infrastruktur kepercayaan (*trust infrastructure*) yang dibangun melalui PSrE. Dengan kata lain, tanda tangan digital yang sah secara normatif membutuhkan ekosistem teknis dan kelembagaan yang mampu menjamin identitas penanda tangan, keutuhan dokumen, serta keberlangsungan validasi di kemudian hari.

4. Relasi dengan Hukum Perdata dan Hukum Pembuktian

Meskipun rezim tanda tangan elektronik berada dalam ranah UU ITE, penilaiannya dalam sengketa *e-commerce* tetap harus dibaca bersama hukum perdata dan hukum pembuktian klasik. Dalam sengketa kontrak elektronik, hakim tidak hanya memeriksa apakah suatu tanda tangan elektronik memenuhi Pasal 11 UU ITE, tetapi juga apakah perjanjian itu memenuhi syarat sah perjanjian, apakah ada wanprestasi, apakah konsumen mengalami kerugian, dan apakah alat bukti yang diajukan cukup untuk membuktikan dalil para pihak (Mertokusumo, 2009).

Di sinilah posisi tanda tangan digital menjadi ganda: ia merupakan instrumen pembentukan kontrak sekaligus alat pembuktian. Sebagai instrumen pembentukan kontrak, tanda tangan digital berfungsi menegaskan adanya persetujuan (*consensus ad idem*). Sebagai alat pembuktian, ia menjadi bagian dari dokumen elektronik yang diajukan di pengadilan untuk menunjukkan bahwa transaksi benar terjadi, dilakukan oleh pihak tertentu, dan isi dokumennya tidak berubah (Ramli, 2022). Dengan demikian, pengaturan hukum tanda tangan digital di Indonesia pada dasarnya telah tersedia, tetapi implementasinya menuntut pembacaan sistematis antara UU ITE, PP 71/2019, peraturan sertifikasi elektronik, dan hukum pembuktian perdata.

B. Syarat Keabsahan Tanda Tangan Digital dalam Transaksi E-Commerce

1. Tanda Tangan Digital Sebagai Sarana Autentikasi Persetujuan

Dalam transaksi *e-commerce*, persoalan paling mendasar adalah bagaimana membuktikan bahwa pihak tertentu benar-benar menyatakan persetujuannya terhadap isi kontrak elektronik. Pada transaksi tatap muka, persetujuan dapat dibuktikan melalui tanda tangan basah, saksi, atau penyerahan dokumen fisik. Sebaliknya, dalam transaksi elektronik, persetujuan kerap diberikan melalui klik, *One-Time Password* (OTP), verifikasi email, penggunaan akun, atau

penandatanganan dokumen digital. Oleh karena itu, keabsahan tanda tangan digital harus dibaca dalam kerangka pembuktian konsensus di lingkungan digital.

Secara normatif, tanda tangan digital dianggap sah jika mampu menunjukkan dua hal: identitas penanda tangan dan adanya persetujuan terhadap informasi elektronik yang ditandatangani. Unsur ini selaras dengan Pasal 11 ayat (1) huruf e dan huruf f UU ITE. Dengan demikian, sekadar adanya gambar tanda tangan yang ditempel pada format PDF belum tentu memenuhi syarat sebagai tanda tangan elektronik yang sah apabila tidak ada mekanisme digital yang dapat membuktikan identitas penanda tangan dan persetujuannya atas dokumen tersebut.

2. Distingsi antara Tanda Tangan Elektronik Biasa dan Tanda Tangan Digital Berbasis Sertifikat

Dalam praktik *e-commerce*, masyarakat sering menyamakan seluruh bentuk persetujuan digital sebagai “tanda tangan digital”. Padahal, dari perspektif hukum dan teknologi, terdapat perbedaan signifikan antara tanda tangan elektronik sederhana (misalnya *scan* tanda tangan, klik “*I agree*”, atau tempelan gambar tanda tangan) dengan tanda tangan digital berbasis sertifikat elektronik. Tanda tangan digital dalam arti teknis umumnya menggunakan sistem kriptografi kunci publik (*public key infrastructure*/PKI) yang menghubungkan identitas penanda tangan dengan kunci privat (*private key*) tertentu, kemudian diverifikasi melalui sertifikat elektronik yang diterbitkan PSrE (Mansur & Gultom, 2014).

Perbedaan ini berdampak langsung pada pembuktian. Tanda tangan elektronik sederhana mungkin cukup untuk menunjukkan adanya interaksi digital, tetapi jika muncul sengketa mengenai identitas, pemalsuan, atau perubahan dokumen, daya buktinya cenderung lemah. Sebaliknya, tanda tangan elektronik tersertifikasi memiliki dukungan teknis yang lebih kuat karena penanda tangan telah melalui proses identifikasi formal, sertifikat elektronik dapat diverifikasi secara *real-time*, dan perubahan dokumen setelah penandatanganan umumnya otomatis merusak segel kriptografinya sehingga dapat langsung terdeteksi.

3. Unsur Kontrol Eksklusif dan Integritas Dokumen

Salah satu unsur terpenting keabsahan tanda tangan digital adalah kontrol eksklusif penanda tangan atas data pembuatan tanda tangan elektronik. Unsur ini dimaksudkan agar pihak lain tidak dapat menggunakan identitas atau kredensial penanda tangan tanpa izin. Dalam konteks *e-commerce*, unsur ini menimbulkan pertanyaan praktis: bagaimana jika akun pengguna diretas, OTP diketahui pihak ketiga, atau perangkat yang digunakan penanda tangan tidak aman? Apakah tanda tangan elektronik tetap dianggap sah?

Secara normatif, jika data pembuatan tanda tangan elektronik tidak lagi berada dalam kuasa penanda tangan, maka salah satu syarat Pasal 11 UU ITE tidak terpenuhi. Namun dalam praktik sengketa, beban pembuktian atas pembajakan akun atau penyalahgunaan kredensial tidak selalu mudah. Karena itu, keabsahan tanda tangan digital tidak hanya ditentukan oleh ada atau tidaknya sertifikat elektronik, tetapi juga oleh keamanan sistem, prosedur verifikasi identitas, dan kemampuan penyelenggara sistem elektronik menyimpan log aktivitas (*system logs*) secara andal.

Selain itu, integritas dokumen menjadi unsur yang tidak dapat dipisahkan. Tanda tangan digital yang sah harus memungkinkan deteksi terhadap perubahan dokumen pasca-penandatanganan. Fungsi ini krusial dalam sengketa *e-commerce*, sebab pihak yang dirugikan kerap mendalilkan bahwa isi kontrak, *invoice*, atau bukti transaksi telah diubah sepihak. Jika sistem tanda tangan digital mampu menunjukkan nilai acak (*hash*), tanda waktu (*timestamp*), sertifikat,

dan *audit trail*, maka pembuktian integritas dokumen akan jauh lebih kuat.

4. Keabsahan Tanda Tangan Digital dalam Kontrak E-Commerce

Keabsahan tanda tangan digital dalam transaksi *e-commerce* pada dasarnya tidak dapat dipisahkan dari keabsahan kontrak elektronik itu sendiri. Pasal 18 ayat (1) UU ITE menegaskan bahwa transaksi elektronik yang dituangkan ke dalam kontrak elektronik mengikat para pihak. Dengan demikian, ketika kontrak elektronik ditandatangani menggunakan tanda tangan elektronik yang memenuhi syarat Pasal 11 UU ITE, kontrak tersebut pada prinsipnya memiliki kekuatan mengikat sebagaimana kontrak konvensional.

Namun demikian, dalam praktik *e-commerce* terdapat beragam model transaksi. Pada *marketplace* ritel, persetujuan sering kali diberikan melalui klik persetujuan syarat dan ketentuan (*click-wrap agreement*) tanpa penggunaan tanda tangan digital tersertifikasi. Pada transaksi *business-to-business* (B2B), penggunaan dokumen elektronik bertanda tangan digital tersertifikasi jauh lebih lazim. Artinya, bentuk persetujuan elektronik dapat beragam. Dalam konteks sengketa, hakim perlu menilai apakah mekanisme persetujuan yang digunakan benar-benar memenuhi unsur identifikasi, persetujuan, dan reliabilitas sistem. Oleh sebab itu, keabsahan tanda tangan digital dalam *e-commerce* tidak dapat dinilai secara abstrak, tetapi harus dikaitkan dengan jenis transaksi, mekanisme autentikasi yang digunakan, dan kualitas sistem elektronik yang menjadi medium transaksi.

C. Kekuatan Pembuktian Tanda Tangan Digital sebagai Alat Bukti Elektronik

1. Tanda Tangan Digital Sebagai Bagian dari Alat Bukti Elektronik

Dalam hukum acara perdata Indonesia, alat bukti tradisional dikenal melalui surat, saksi, persangkaan, pengakuan, dan sumpah sebagaimana diatur dalam Pasal 1866 KUHPerdata. Kehadiran UU ITE memperluas sistem pembuktian dengan mengakui informasi elektronik dan/atau dokumen elektronik sebagai alat bukti hukum yang sah. Konsekuensinya, dokumen kontrak elektronik, *invoice* digital, rekam jejak transaksi, log sistem, email, dan dokumen bertanda tangan elektronik dapat diajukan sebagai alat bukti di persidangan (Budhijanto, 2018).

Tanda tangan digital pada dasarnya tidak berdiri sendiri sebagai alat bukti yang terpisah dari dokumen elektronik. Ia melekat pada dokumen atau informasi elektronik tertentu dan berfungsi memperkuat autentisitas, integritas, dan atribusi dokumen tersebut kepada penanda tangan. Oleh karena itu, dalam sengketa perdata, hakim umumnya tidak hanya menilai “tanda tangannya” tetapi keseluruhan ekosistem bukti: kontrak elektronik, metadata, sertifikat elektronik, log akses, bukti pembayaran, komunikasi para pihak, dan bukti pendukung lainnya.

2. Nilai Pembuktian Tanda Tangan Elektronik Tersertifikasi

Dari perspektif pembuktian, tanda tangan elektronik tersertifikasi memiliki posisi yang jauh lebih kuat dibandingkan tanda tangan elektronik tidak tersertifikasi. Hal ini disebabkan oleh beberapa faktor. Pertama, tanda tangan elektronik tersertifikasi didukung oleh sertifikat elektronik yang menghubungkan identitas pemilik sertifikat dengan data verifikasi tertentu secara valid. Kedua, PSrE berperan sebagai pihak ketiga terpercaya (*trusted third party*) yang membantu menjamin validitas identitas dan integritas proses penandatanganan. Ketiga, tanda tangan elektronik tersertifikasi umumnya memiliki jejak audit yang lebih baik, termasuk kepastian waktu penandatanganan (*time-stamping*), status sertifikat, dan kemungkinan validasi pasca-penandatanganan.

Dalam sengketa *e-commerce*, kondisi tersebut memberi keuntungan pembuktian yang signifikan. Pihak yang mengajukan dokumen bertanda tangan elektronik tersertifikasi dapat menunjukkan bahwa identitas penanda tangan telah diverifikasi secara formal, sertifikat elektronik masih berlaku, dokumen tidak berubah sejak ditandatangani, dan proses penandatanganan dilakukan melalui sistem yang memenuhi standar keamanan operasi. Meskipun demikian, hukum Indonesia belum secara eksplisit menyatakan bahwa tanda tangan elektronik tersertifikasi otomatis memiliki kekuatan pembuktian sempurna seperti akta autentik. Oleh karena itu, penilaiannya tetap berada pada diskresi dan kewenangan hakim berdasarkan keseluruhan alat bukti yang diajukan.

3. Keterbatasan Pembuktian pada Tanda Tangan Elektronik Tidak Tersertifikasi

Berbeda dengan tanda tangan elektronik tersertifikasi, tanda tangan elektronik tidak tersertifikasi menghadapi tantangan pembuktian yang jauh lebih besar. Misalnya, tempelan gambar tanda tangan pada dokumen PDF, persetujuan melalui klik biasa, atau *scan* tanda tangan yang dikirim lewat email pada dasarnya dapat menunjukkan adanya interaksi digital, tetapi belum tentu cukup untuk membuktikan identitas penanda tangan secara meyakinkan. Dalam sengketa, pihak lawan dapat dengan mudah membantah bahwa dokumen dibuat atau ditandatangani olehnya, atau menyatakan bahwa grafik tanda tangan tersebut dicuri dan ditempel tanpa izin.

Dalam kondisi demikian, kekuatan pembuktian tanda tangan elektronik tidak tersertifikasi akan sangat bergantung pada bukti tambahan (*corroborative evidence*), seperti korespondensi pesan instan, bukti pengiriman OTP ke nomor seluler pribadi, rekaman log sistem, keterangan ahli digital forensik, bukti realisasi pembayaran, atau pola perilaku para pihak setelah transaksi berlangsung. Dengan kata lain, tanda tangan elektronik tidak tersertifikasi tidak otomatis tidak sah, tetapi beban pembuktiannya di depan sidang pengadilan jauh lebih berat.

4. Tanda Tangan Digital, Non-Repudiation, dan Beban Pembuktian

Salah satu fungsi penting tanda tangan digital adalah *non-repudiation*, yaitu mencegah penanda tangan menyangkal keterlibatannya dalam suatu transaksi hukum. Secara teoritis, tanda tangan digital yang dibangun dengan infrastruktur kriptografi dan sertifikat elektronik memungkinkan atribusi yang sangat kuat kepada penanda tangan. Namun, dari perspektif hukum acara perdata, asas *non-repudiation* tidak pernah bersifat absolut di ruang sidang. Pihak yang diduga menandatangani tetap dapat mengajukan bantahan, misalnya bahwa kunci privat dicuri, akun diretas, sertifikat digunakan tanpa izin melalui *social engineering*, atau proses identifikasi awal (*know your customer/KYC*) mengandung cacat kehendak.

Karena itu, beban pembuktian dalam sengketa tanda tangan digital tidak sesederhana “ada sertifikat berarti perkara selesai”. Pihak yang mengajukan bukti tetap harus mampu menunjukkan rantai pembuktian (*chain of custody*) yang utuh: identitas penanda tangan, validitas sertifikat elektronik, reliabilitas sistem, keutuhan dokumen, dan relevansi dokumen dengan peristiwa hukum yang disengketakan. Sebaliknya, pihak yang menyangkal juga harus menghadirkan bantahan yang rasional dan dapat diverifikasi secara teknis. Dalam praktik, hakim akan menilai kekuatan pembuktian tanda tangan digital berdasarkan prinsip pembuktian bebas terbatas, yaitu menilai alat bukti menurut kualitas, konsistensi, dan keterkaitannya dengan alat bukti lain.

5. Relevansi dalam Sengketa E-Commerce

Dalam sengketa *e-commerce*, tanda tangan digital dapat muncul pada berbagai jenis dokumen: kontrak kerja sama antara *merchant* dan platform, perjanjian pinjaman digital (*fintech lending*), *invoice* elektronik, *purchase order*, dokumen pembiayaan, atau persetujuan konsumen

terhadap syarat dan ketentuan layanan. Nilai pembuktian tanda tangan digital dalam setiap kasus tidak selalu sama.

Untuk transaksi bernilai tinggi dan berisiko tinggi, penggunaan tanda tangan elektronik tersertifikasi menjadi mutlak karena dapat memperkecil ruang bantahan dari pihak lawan. Sebaliknya, untuk transaksi ritel sederhana, pembuktian sering kali tidak menggunakan tanda tangan digital melainkan bergantung pada kombinasi bukti lain seperti histori pesanan, bukti pembayaran perbankan, notifikasi sistem, dan komunikasi dalam aplikasi. Dengan demikian, kekuatan pembuktian tanda tangan digital tidak dapat dipisahkan dari konteks transaksinya. Semakin besar risiko hukum dan ekonomi suatu transaksi, semakin besar pula kebutuhan akan tanda tangan elektronik yang memenuhi standar autentikasi dan verifikasi tingkat tinggi.

D. Tantangan Implementasi dan Kepastian Hukum Tanda Tangan Digital dalam Transaksi E-Commerce

1. Problem Literasi dan Kesalahpahaman Konseptual

Salah satu hambatan utama implementasi tanda tangan digital di Indonesia adalah masih rendahnya literasi hukum dan teknis mengenai perbedaan antara tanda tangan elektronik biasa, tanda tangan digital, sertifikat elektronik, dan tanda tangan elektronik tersertifikasi. Banyak pelaku usaha maupun konsumen mengira bahwa menempel grafik gambar tanda tangan pada dokumen PDF sudah otomatis setara dengan tanda tangan digital yang aman dan memiliki daya bukti tinggi. Padahal, dari perspektif hukum pembuktian siber, keduanya memiliki derajat keandalan yang berbeda jauh.

Kesalahpahaman konseptual ini menimbulkan risiko hukum yang besar dalam ekosistem *e-commerce*, terutama pada transaksi pinjaman, pembiayaan, kemitraan, dan jual beli bernilai tinggi. Para pihak sering merasa telah “aman secara hukum” hanya karena ada visualisasi tanda tangan dalam dokumen elektronik, padahal mekanisme autentikasi dan integritas dokumennya sangat rapuh. Akibatnya, ketika sengketa muncul, proses pembuktian menjadi buntu dan posisi hukum para pihak tidak sekuat yang diasumsikan semula.

2. Keamanan Sistem dan Penyalahgunaan Identitas

Tantangan berikutnya yang sangat krusial adalah keamanan sistem elektronik itu sendiri. Keabsahan tanda tangan digital bertumpu pada asumsi bahwa data pembuatan tanda tangan berada di bawah kuasa eksklusif penanda tangan dan sistem mampu menjaga integritas dokumen secara penuh. Dalam kenyataannya, ancaman keamanan siber seperti *phishing*, pencurian OTP, pembajakan akun, infiltrasi *malware*, *social engineering*, dan kebocoran data pribadi massal sering kali merusak asumsi eksklusivitas tersebut.

Jika kredensial penanda tangan telah jatuh ke tangan pihak ketiga yang tidak berhak, maka autentikasi formal di atas kertas saja belum tentu cukup untuk menjamin bahwa persetujuan (*consent*) memang diberikan secara sah oleh subjek hukum yang bersangkutan. Persoalan ini menjadi semakin serius ketika dikaitkan dengan perlindungan data pribadi. Penggunaan tanda tangan digital umumnya melibatkan data identitas sensitif, nomor telepon, email, biometrik, hingga dokumen kependudukan (KTP). Dalam konteks ini, keberlakuan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) harus dibaca sebagai instrumen pendukung wajib untuk memastikan bahwa penyelenggara sistem elektronik dan PSrE tidak hanya sah secara kontraktual, tetapi juga akuntabel dalam mengamankan data pengguna (Republik Indonesia, 2022).

3. Fragmentasi Praktik Pembuktian dan Tantangan di Pengadilan

Problem lain yang dihadapi terletak pada praktik pembuktian langsung di ruang sidang pengadilan. Secara normatif, alat bukti elektronik telah diakui secara sah oleh sistem hukum Indonesia. Namun dalam praktik peradilan perdata, kemampuan para pihak litigasi dan aparat penegak hukum untuk memahami karakteristik teknis bukti elektronik tidak selalu seragam.

Tidak semua sengketa *e-commerce* menghadirkan ahli digital forensik karena kendala biaya, tidak semua hakim memiliki pemahaman yang sama mengenai cara memvalidasi sertifikat elektronik via *database* PSrE, dan tidak semua pengacara mampu mengekstraksi log sistem atau metadata secara tepat sebagai alat bukti resmi. Akibatnya, meskipun hukum tertulis telah mengakui tanda tangan digital, efektivitas pembuktiannya di lapangan masih sangat dipengaruhi oleh kapasitas institusional dan pemahaman teknologi dari sistem peradilan kita. Di samping itu, banyak sengketa *e-commerce* diselesaikan melalui mekanisme non-litigasi seperti *customer complaint handling* internal platform yang standarnya jauh lebih pragmatis daripada formal, sehingga berisiko menurunkan kualitas perlindungan hukum konsumen jika platform menentukan validitas transaksi secara sepihak.

4. Kebutuhan Harmonisasi antara Hukum Kontrak, Hukum Pembuktian, dan Regulasi Digital

Keabsahan tanda tangan digital tidak cukup dijamin hanya dengan mengandalkan rumpun norma dalam UU ITE. Diperlukan harmonisasi yang lebih kuat antara hukum kontrak klasik (KUHPperdata), hukum pembuktian (HIR/RBg), hukum perlindungan konsumen, hukum perlindungan data pribadi, dan tata kelola sistem elektronik sektoral. Misalnya, dalam sengketa konsumen *e-commerce*, pertanyaan mengenai keabsahan tanda tangan digital hampir selalu beririsan dengan keabsahan klausula baku (*standard clause*), kewajiban pelaku usaha memberikan informasi yang jujur, mekanisme persetujuan implisit, serta tanggung jawab platform jika terjadi transaksi tidak sah (*unauthorized transaction*).

Karena itu, penguatan kepastian hukum ke depan harus diarahkan setidaknya pada empat pilar:

- **Pertama**, standarisasi kewajiban penggunaan tanda tangan elektronik tersertifikasi untuk jenis transaksi tertentu yang memiliki risiko ekonomi tinggi.
- **Kedua**, penguatan kewajiban hukum bagi penyelenggara sistem elektronik untuk menyimpan *audit trail*, log aktivitas, dan bukti autentikasi secara memadai dengan jangka waktu preservasi yang aman.
- **Ketiga**, peningkatan kapasitas edukasi digital bagi aparat penegak hukum dan hakim dalam menilai keandalan alat bukti elektronik.
- **Keempat**, edukasi publik secara masif mengenai perbedaan esensial antara bentuk-bentuk tanda tangan elektronik dan konsekuensi hukumnya masing-masing.

5. Arah Pembaruan Hukum Pembuktian Elektronik

Secara konseptual, tanda tangan digital merupakan instrumen penting bagi modernisasi hukum pembuktian dan hukum kontrak di era modern. Namun, pembaruan hukum ke depan perlu memastikan bahwa pengakuan normatif di undang-undang harus diikuti oleh penguatan standar pembuktian hukum acara yang operasional. Dalam konteks Indonesia, salah satu agenda penting ialah membangun parameter baku yang lebih jelas mengenai nilai bobot pembuktian tanda tangan elektronik tersertifikasi dan tidak tersertifikasi dalam sengketa perdata.

Perlu didorong adanya pedoman pembuktian elektronik yang lebih operasional bagi lembaga peradilan agar penilaian terhadap sertifikat elektronik, log sistem, metadata, dan jejak

otentikasi memiliki kepastian standar, serta tidak terlalu bergantung pada improvisasi pemahaman masing-masing pihak yang bersengketa. Dengan demikian, tantangan terbesar tanda tangan digital di Indonesia saat ini bukan lagi pada ada atau tidak adanya pengakuan hukum, melainkan pada bagaimana menjadikan pengakuan tertulis itu efektif, aman, dan konsisten dalam praktik transaksi nyata serta penyelesaian sengketa hukum sehari-hari. Tanpa pembenahan aspek implementasi teknis dan hukum acara ini, tanda tangan digital berisiko hanya menjadi simbol modernisasi di atas kertas, tetapi belum sepenuhnya menjelma sebagai instrumen kepastian hukum yang dapat diandalkan oleh masyarakat ekonomi digital.

KESIMPULAN

Berdasarkan hasil penelitian dan pembahasan, dapat disimpulkan beberapa hal sebagai berikut:

Pertama, tanda tangan digital atau tanda tangan elektronik telah memiliki dasar keabsahan yang jelas dalam sistem hukum Indonesia melalui UU ITE beserta perubahan-perubahannya, PP 71/2019, dan Permen Kominfo 11/2022. Rezim hukum tersebut menempatkan tanda tangan elektronik sebagai sarana autentikasi dan verifikasi yang sah sepanjang memenuhi syarat Pasal 11 UU ITE, yakni keterkaitan eksklusif dengan penanda tangan, penguasaan data pembuatan tanda tangan oleh penanda tangan, kemampuan mendeteksi perubahan tanda tangan dan dokumen, mekanisme identifikasi penanda tangan, serta adanya indikasi persetujuan terhadap dokumen elektronik yang ditandatangani.

Kedua, keabsahan tanda tangan digital dalam transaksi *e-commerce* tidak hanya ditentukan oleh ada atau tidaknya tanda tangan pada dokumen elektronik, tetapi oleh terpenuhinya fungsi hukum tanda tangan, yakni identifikasi, persetujuan, autentikasi, dan integritas dokumen. Dalam konteks ini, tanda tangan elektronik tersertifikasi memiliki posisi yang jauh lebih kuat karena didukung sertifikat elektronik, verifikasi identitas, dan infrastruktur Penyelenggara Sertifikasi Elektronik (PSrE). Sebaliknya, tanda tangan elektronik tidak tersertifikasi pada dasarnya tetap sah, namun cenderung memiliki beban pembuktian yang jauh lebih berat ketika timbul sengketa.

Ketiga, dari aspek hukum acara, tanda tangan digital merupakan bagian dari alat bukti elektronik yang sah. Kekuatan pembuktiannya tidak berdiri sendiri, melainkan dinilai bersama dokumen elektronik, metadata, log sistem (*system logs*), bukti pembayaran, korespondensi para pihak, dan bukti pendukung lainnya. Tanda tangan elektronik tersertifikasi pada umumnya memberikan nilai pembuktian yang lebih tinggi karena lebih mudah diverifikasi dan lebih kuat dalam menunjukkan identitas penanda tangan serta keutuhan dokumen. Namun demikian, hukum Indonesia belum menempatkannya secara otomatis setara dengan akta autentik, sehingga penilaian akhirnya tetap berada pada diskresi hakim berdasarkan keseluruhan alat bukti yang diajukan di persidangan.

Keempat, tantangan implementasi tanda tangan digital dalam ekosistem *e-commerce* masih cukup besar. Tantangan tersebut meliputi rendahnya literasi masyarakat, kesalahpahaman antara tanda tangan elektronik biasa dan tanda tangan digital tersertifikasi, ancaman keamanan siber, potensi penyalahgunaan identitas, fragmentasi praktik pembuktian di pengadilan, serta belum meratanya kapasitas penegak hukum dalam menilai alat bukti elektronik. Oleh karena itu, meskipun tanda tangan digital telah memiliki dasar keabsahan dan kekuatan pembuktian yang memadai secara normatif, efektivitasnya dalam memberikan kepastian hukum masih memerlukan penguatan standardisasi teknis, tata kelola data dan sistem elektronik, pedoman pembuktian elektronik yang lebih operasional bagi pengadilan, serta edukasi hukum digital kepada masyarakat dan pelaku usaha.

Dengan demikian, tanda tangan digital dalam transaksi *e-commerce* pada prinsipnya telah sah dan memiliki kekuatan pembuktian yang memadai dalam hukum Indonesia. Akan tetapi, kepastian dan efektivitas perlindungan hukumnya akan sangat bergantung pada kualitas autentikasi, integritas sistem, penggunaan sertifikat elektronik yang andal, serta kemampuan sistem peradilan dalam membaca dan menilai bukti elektronik secara konsisten.

DAFTAR PUSTAKA

- Badan Pemeriksa Keuangan Republik Indonesia. (n.d.). *Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik*. <https://peraturan.bpk.go.id>
- Budhijanto, D. (2018). *Hukum eksistensi siber (cyber existence law) di Indonesia*. Logoz Publishing.
- JDIH Kementerian Komunikasi dan Digital Republik Indonesia. (n.d.). *Peraturan Menteri Komunikasi dan Informatika Nomor 11 Tahun 2022 tentang Tata Kelola Penyelenggaraan Sertifikasi Elektronik*. <https://jdih.komdigi.go.id>
- Kementerian Komunikasi dan Informatika Republik Indonesia. (2022). *Peraturan Menteri Komunikasi dan Informatika Nomor 11 Tahun 2022 tentang Tata Kelola Penyelenggaraan Sertifikasi Elektronik*.
- Kementerian Komunikasi dan Informatika. (2022). *Peraturan Menteri Komunikasi dan Informatika Nomor 11 Tahun 2022 tentang Tata Kelola Penyelenggaraan Sertifikasi Elektronik*. JDIH Kominfo. https://jdih.kominfo.go.id/produk_hukum/view/id/835/t/peraturan+menteri+komunikasi+dan+informatika+nomor+11+tahun+2022+tanggal+13+desember+2022
- Makarim, E. (2020). *Pengantar hukum telematika: Suatu kompilasi kajian*. RajaGrafindo Persada.
- Mansur, D. M., & Gultom, E. (2014). *Cyber law: Aspek hukum teknologi informasi*. Refika Aditama.
- Mertokusumo, S. (2009). *Hukum acara perdata Indonesia*. Liberty.
- Ramli, A. M. (2022). *Cyber law dan hukum hak cipta*. Alumnii.
- Republik Indonesia. (1847). *Kitab Undang-Undang Hukum Perdata [Burgerlijk Wetboek untuk Indonesia]* (Staatsblad Nomor 23 Tahun 1847).
- Republik Indonesia. (1945). *Undang-Undang Dasar Negara Republik Indonesia Tahun 1945*.
- Republik Indonesia. (2008). *Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843. JDIH BPK. <https://peraturan.bpk.go.id/Details/39016/uu-no-11-tahun-2008>
- Republik Indonesia. (2008). *Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*.
- Republik Indonesia. (2016). *Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*.
- Republik Indonesia. (2019). *Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik*. Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185, Tambahan Lembaran Negara Republik Indonesia Nomor 6402. JDIH BPK. <https://peraturan.bpk.go.id/Details/122119/pp-no-71-tahun-2019>
- 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*.
- Republik Indonesia. (2024). *Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas*

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Lembaran Negara Republik Indonesia Tahun 2024 Nomor 7, Tambahan Lembaran Negara Republik Indonesia Nomor 6924. JDIH BPK. <https://peraturan.bpk.go.id/Details/274479/uu-no-1-tahun-2024>

Republik Indonesia. (2024). *Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*.

Subekti. (2001). *Hukum perjanjian*. Intermasa.