



**ACTA DIURNAL Jurnal Ilmu Hukum Kenotariatan
Fakultas Hukum Universitas Padjadjaran**

PISSN: 2614-3542 EISSN: 2614-3550

Volume 6, Nomor 2, Juni 2023

Artikel diterbitkan 30 Juni 2023, DOI: <https://doi.org/10.23920/acta.v6i2.1141>

Halaman Publikasi: <http://jurnal.fh.unpad.ac.id/index.php/acta/issue/archive>

KEPASTIAN HUKUM TANDA TANGAN DIGITAL PADA PLATFORM PRIVYID DI INDONESIA

Rahmadi Indra Tektona, Universitas Jember, Jember, email: rahmadiindra@unej.ac.id

Sry Rezeki Laoly, Universitas Jember, Jember, email: srirejekilaoly13@gmail.com

ABSTRAK

Pelaku bisnis ingin sebuah kepastian dari segi hukum maupun keotentikan data yang memiliki peranan penting dalam transaksi bisnis, maka dari situlah peran tanda tangan digital serta sertifikat digital dalam PrivyID sebagai terobosan teknologi untuk mewujudkan keinginan sebagai pelaku bisnis. Dalam transaksi suatu keniscayaan apabila terjadi sengketa, maka diperlukan pengetahuan terkait bagaimana upaya penyelesaian sengketa tanda tangan digital dalam transaksi bisnis apabila terjadi wanprestasi. Tujuan penelitian ini mengetahui serta menganalisis mengenai kepastian hukum tanda tangan digital pada platform privyid di Indonesia, dengan menggunakan metode penelitian hukum normatif dengan pendekatan perundang-Undangan dan pendekatan konseptual, serta menggunakan bahan hukum primer, sekunder, dan non hukum. Hasil menunjukkan bahwa tanda tangan digital pada dokumen elektronik memiliki kepastian hukum sebagai alat bukti menurut hukum acara perdata yang merupakan perluasan dari alat bukti surat serta didukung keberadaan *certifikat authority* (CA).

Kata kunci: pelaku bisnis; tanda tangan digital; wanprestasi.

ABSTRACT

Business actors seek legal certainty and data authenticity, which play important roles in business transactions. Hence, the role of digital signatures and digital certificates within PrivyID serves as a technological breakthrough to fulfill the desires of business actors. In any transaction, disputes may arise, necessitating knowledge of how to resolve disputes related to digital signatures in the event of non-performance. The objective of this research is to understand and analyze the legal certainty of digital signatures on the PrivyID platform in Indonesia. This study utilizes a normative legal research method with legislative and conceptual approaches, along with primary, secondary, and non-legal sources. The analysis reveals that digital signatures on electronic documents possess legal certainty as evidence under civil procedural law, which extends the evidentiary value of written documents and is supported by the existence of a certificate authority (CA).

Keywords: business actor; default; digital signatures.

PENDAHULUAN

Kehadiran kemajuan teknologi secara digital mengakibatkan keterlibatan dalam perkembangan informasi, dimana teknologi komunikasi menjadi sebuah media bagi masyarakat yang dimanfaatkan sebagai sarana untuk berkomunikasi dalam transaksi bisnis yang digunakan untuk lebih mengefisienkan waktu serta biaya.¹ Melihat hal tersebut, maka perlu untuk ditinjau bahwa keamanan suatu untuk melindungi informasi dari orang yang tidak berwenang, ketika seseorang mengirim dokumen elektronik ke si penerima penyusup dapat memodifikasi kemudian mengirim dokumen yang

¹ Carlo A Garungan, *Tanggung Jawab Penyelenggara Sistem Informasi Jika Terjadi Kegagalan Sistem*, Manado Sam Ratulangi University: 2013, hlm.42.

sudah dimodifikasi ke penerima, maka untuk mengatasi hal tersebut diterapkan sebuah tanda tangan digital dalam menandatangani dokumen elektronik.²

Tanda tangan digital dengan aplikasi PrivyID juga memiliki kekuatan hukum yang mengikat yang sama dengan tanda tangan basah sebagaimana diatur dalam Undang-Undang No 11 Tahun 2008 tentang informasi dan transaksi elektronik. Pasal 11 ayat (1) mensyaratkan tanda tangan digital harus terasosiasi atau terkait dengan informasi elektronik lain digunakan sebagai alat verifikasi dan autentikasi, namun aplikasi yang menawarkan teknologi tanda tangan digital belum menjamin keamanan sehingga jika terjadi sengketa kekuatan pembuktiannya lemah. Sebagai salah satu penyedia tanda tangan digital dalam negeri, PrivyID, sudah lebih maju dalam hal keamanan, seperti membatasi NIK atau satu KTP hanya untuk satu ID dan meminimalkan penggunaan tanda tangan digital.

Pertumbuhan tanda tangan digital ini pun terlihat dari peningkatan jumlah pengguna layanan PrivyID sebagai startup penyedia layanan tanda tangan digital. Jumlah penggunanya dalam enam bulan terakhir naik hampir dua kali lipat, dari satu juta ke 1,9 juta pengguna di Indonesia. Mayoritas pengguna tanda tangan digital PrivyID berlokasi di Pulau Jawa. Berdasarkan catatan, sebanyak 59 persen penggunanya berasal dari Jakarta, Bogor, Tangerang, Depok, dan Bekasi. Sebanyak 70 persen pemakai tanda tangan digital merupakan karyawan swasta dengan rentang usia 25-40 tahun³.

Menurut Tan Thong Kie, tanda tangan adalah suatu pernyataan kemauan pembuat tanda tangan, bahwa ia dengan menuliskan tanda tangannya di bawah suatu tulisan menghendaki agar tulisan itu dalam hukum dianggap sebagai tulisannya sendiri⁴. Tanda tangan digital adalah suatu cara untuk memastikan orisinalitas dokumen elektronik dimana penggunaannya mampu menyampaikan fakta ke penerima untuk dapat yakin atas pesan yang telah dikirimkan benar adanya tanpa dimanipulasi.

Menurut *American Bar Association (ABA)*, pengertian tanda tangan dapat berupa tanda apapun yang dibuat dengan tujuan untuk memberikan persetujuan dan otentifikasi terhadap suatu dokumen tersebut⁵. Penggunaan tanda tangan digital mampu menyampaikan fakta pada penerima untuk dapat yakin atas pesan yang telah dikirimkan benar adanya dan tidak dapat dimanipulasi.⁶ Persoalan hukum yang muncul antara lain berkenaan dengan kekuatan hukum tanda tangan elektronik. Di USA saat ini telah ditetapkan satu undang-undang yang secara formal mengakui keabsahan tanda tangan elektronik. Pengaturan di tingkat internasional diatur dalam Pasal 7 UNICITRAL Model Law (*The United Nations Commissions on International Trade Law*).

Di Indonesia penggunaan tanda tangan digital diatur dalam Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik, namun secara spesifik diatur dalam Peraturan Menteri Komunikasi dan Informatika Nomor 11 tahun 2018 tentang penyelenggaraan sertifikasi

² Roberto Akyuwen, *Lebih Mengenal Digital Banking Manfaat, Peluang, dan Tantangan*, Universitas Gajah Mada Anggota IKAPI, Jakarta: 2020, hlm. 56.

³ Maria Yuniar, "1,9 Juta Orang Indonesia Pakai Tanda Tangan Digital," last modified 2022, <https://www.ekrut.com/media/1-9-juta-orang-indonesia-pakai-tanda-tangan-digital>.

⁴ Tan Thong Kie, *Studi Notariat dan Serba-Serbi Praktek Notaris*, PT. Ichtiar Baru Van Hoeve, Jakarta: 2007, hlm 473.

⁵ Information Security Committee, Section of Science & Technology - American Bar Association, *Digital Signature Guidlines*, American Bar Association, United States:2016, hlm. 4.

⁶ Atmojo, *Penerapan Internet Untuk Bisnis*, Ghalia Indonesia, Yogyakarta: 2020, hlm. 56.

Elektronik.⁷ Tanda tangan digital bersifat unik sehingga hanya terbuka dengan pasangan kuncinya seperti kunci privat dan publik sehingga menjadi metode pengamanan pengiriman informasi itu sendiri dari pihak pengirim ke penerima atau dapat digunakan kriptografi atau enkripsi yang merupakan bentuk pengamanan data atau pesan. Tanda tangan digital keabsahannya sah diterima dengan alasan bahwa tanda tangan digital mampu dibubuhkan orang yang telah di beri kuasa yang diikat secara hukum.

Pengertian kriptografi adalah proses linguistik, matematika, dan representasional yang berbeda dari komputasi, dilihat dari fakta sejarah menyatakan bahwa sebagian besar kriptografi dilakukan dengan kertas, tinta, dan kemudian, telegraf⁸. Kriptografi (*Cryptography*) berasal dari bahasa Yunani, terdiri dari dua suku kata yaitu kript dan graphia. Kripto artinya menyembunyikan, sedangkan graphia artinya tulisan. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data, tetapi tidak semua aspek keamanan informasi dapat diselesaikan dengan kriptografi⁹.

Berkaitan dengan penjelasan di atas, keberadaan tanda tangan digital terbukti mampu memberikan manfaat bagi penyedia barang atau jasa karena diyakini mampu sebagai inovasi dalam layanan keuangan yang mengarah ke berbagai model bisnis yang berbeda.¹⁰ Dalam layanan *Fintech* terdapat peraturan dalam pengembangannya, hal ini terkait dengan bagaimana penggunaan tanda tangan digital dan penggunaan dokumen elektronik sehingga dapat memaksimalkan kemampuan *fintech* di lingkungan bisnis.

Sehubungan dengan itu, pemanfaatan tanda tangan digital akan meningkatkan nilai-nilai dari teknologi finansial dengan memunculkan salah satu produk tanda tangan digital yaitu PrivyID dimana yang dikembangkan oleh PT PrivyID, dimana layanan ini memberikan kewenangan untuk menerima, pendaftaran, verifikasi, dan penerbitan sertifikasi elektronik.¹¹ Meski sudah memiliki kekuatan hukum, namun demikian tetap perlu memperhatikan keamanan dan perlindungan data pribadi bagi para konsumen yang menyalahgunakan data pribadi yang merugikan masyarakat.

Berdasarkan latar belakang di atas, artikel ini mengangkat rumusan masalah yaitu apakah tanda tangan digital pada platform privyid di Indonesia sudah berkepastian hukum, serta berkaitan dengan konsep penyelesaian sengketa. Dengan tujuan dalam penelitian ini, mengetahui, memahami keabsahan penggunaan tanda tangan digital dalam upaya peningkatan perlindungan konsumen dengan menggunakan tanda tangan digital PrivyID di Indonesia serta mengetahui, menganalisis, serta memberikan temuan terkait dengan konsep penyelesaian sengketa transaksi bisnis finansial teknologi apabila terjadi wanprestasi.

⁷ Edmon Makarim, *Notaris dan Transaksi Elektronik*, PT Raja Grafindo Persada, Jakarta: 2013, hlm 5.

⁸ Muhammad Natsir, "Pengembangan Prototype Sistem Kriptografi Untuk Enkripsi Dan Dekripsi Data Office Menggunakan Metode Blowfish Dengan Bahasa Pemrograman Java," *Jurnal Format*, Vol. 6, 2017, No. 1, hlm. 87-105.

⁹ Dony Ariyus, *Kriptografi Keamanan Data dan Kriptografi*, Penerbit Andi Offset, Yogyakarta: 2006, hlm. 56.

¹⁰ Surohman, (et.al.), "Analisa Sentimen Terhadap Review Fintech Dengan Metode Naive Bayes Classifier Dan K-Nearest Neighbor," *Jurnal Sains dan manajemen*, Vol. 8 No. 2, Maret 2020, hlm. 94.

¹¹ Rizki Sulistio, "The Role & Advantages of Digital Signatures for the Fintech Industry, sharing Session PrivyID," 2019. Dalam Affan Muhammad Andalan, "Kedudukan Tanda Tangan Elektronik dalam Transaksi Teknologi Finansial," *Jurist Diction*, Vol. 2 No. 6, November 2019, p.1943.

METODE PENELITIAN

Penelitian ini menggunakan jenis yuridis normatif. Metode pendekatan yang digunakan dalam penelitian ini adalah perundang-undangan dan konseptual. Metode analisis yang digunakan deskriptif analisis yaitu metode yang digunakan untuk menganalisis keadaan atau peristiwa menjelaskan hubungan antara situasi tersebut dengan masalah yang sedang yang diteliti.¹²

PEMBAHASAN

Perkembangan internet telah merevolusi ekonomi, perubahannya terlihat pada prosedur, teknik dan model bisnis. Transaksi secara internet atau *disebut E-commerce* diciptakan transaksi bisnis tanpa kertas yang lebih nyaman, tidak perlu berurusan secara langsung atau tatap muka dengan pihak.¹³ Permasalahan keamanan selalu menjadi tantangan ke depan dalam bertransaksi lewat internet meski dalam website privy.id sudah ada standarisasi kewanaman yang diberikan oleh pihak berwenang nasional maupun internasional yaitu¹⁴ : Kementerian Komunikasi dan Informatika CA Berinduk Kep. MENKOMINFO No. 84 Tahun 2021 Penyedia Sistem Tanda Tangan Elektronik Terdaftar No. 001219.02/DJAI.PSE/08/2021, PrivyID Certification and Acknowledgement: Bank Sentral Indonesia Passed Regulatory Sandbox No.22/266/DKSP/Srt/B, WebTrust Certification for CA PrivyID Certification and Acknowledgement, Kementerian Dalam Negeri Perjanjian Kerja Sama dengan Direktorat Jenderal Kependudukan dan Catatan Sipil No. PKS : 119/2541/DUKCAPIL & 040/PID-BD/PKS/III/2019 No. Addendum: 119/6855/DUKCAPIL & 032/Privy-BD/PKS/IV/2022, PrivyID Certification and Acknowledgement: TUV Rheinland Sertifikasi ISO IEC 27001 2013 Information Security Management System Register.No 01 153 1735164

Setelah proses penandatanganan secara digital selesai dilakukan, maka masalah keamanan atas pertukaran data belum bisa terselesaikan karena masalah utama justru bukan dari teknologinya melainkan pendistribusian kunci publik yang dimana menjamin bahwa kunci publik yang dimaksud merupakan kunci publik yang sebenarnya, untuk dapat mengatasi kewanaman dalam pendistribusian, maka dengan itu sebuah kunci publik direkatkan pada suatu sertifikat digital yang merupakan dokumen yang berisi tentang pernyataan kebenaran sesuatu informasi untuk dapat mengidentifikasi diri kita dimana disertakan dengan kunci publik orang yang bersangkutan atau mengikat nama pengguna ke kunci publiknya dengan tujuan untuk meyakinkan orang lain bahwa kunci tersebut benar-benar sah. Karena demikian maka diterbitkan Lembaga yang dapat dipercaya atau sudah memiliki otorisasi yang disebut dengan CA atau *Certification authority* yaitu sebuah Lembaga yang bertugas untuk mengeluarkan sebuah sertifikat elektronik yang berisi kunci duplikat dari kunci publik pelanggan kemudia CA akan menandatangani digital sertifikat dengan kunci privat miliknya¹⁵

Perjanjian elektronik dalam *E-commerce* memiliki akibat hukum yang dalam acara peradilan dokumen elektronik dapat dianggap sama dengan surat dan memiliki kekuatan hukum sama dengan

¹² Soerjono Soekanto dan Sri Mamudj, *Penelitian Hukum Normatif: Suatu Tinjauan Singkat*, Raja Grafindo Persada, Jakarta: 2001, hlm. 115.

¹³ Barkatullah A. H., *Hukum Transaksi Elektronik. Sebagai Panduan dalam Menghadapi Era Digital Bisnis E-Commerce di Indonesia*, Hikam Media Utama, Bandung: 2018, hlm. 26.

¹⁴ Wita Dewisari Tasya, "Analisis Keamanan Penyelenggara Sertifikasi Elektronik Indonesia: PT Privy Identitas Digital", Makalah II, [diakses pada 12/12/ 2021-2022].

¹⁵ Abdul Halim Berkatullah, T. Prasetyo, *Bisnis E-Commerce, Studi Sistem Keamanan Dan Hukum di Indonesia*, Cetakan I,II, Pustaka Pelajar, Yogyakarta: 2006, hlm. 35-36.

kekuatan hukum alat bukti dalam acara perdata. Dalam Undang-Undang No 27 Tahun 2022 Tentang Pelindungan Data Pribadi (UUPDP) Tidak terdapat hal khusus yang mengatur tentang tanda tangan digital sehingga dapat disimpulkan bahwa tanda tangan digital tidak termasuk data pribadi, kecuali tanda tangan tersebut disandingkan dengan data pribadi lain yang dapat mengidentifikasi seseorang, hal tersebut terdapat dalam (3) UUPDP yaitu:

“Informasi adalah keterangan, pernyataan, gagasan, dan tanda-tanda yang mengandung nilai, makna, dan pesan, baik data, fakta, maupun penjelasannya yang dapat dilihat, didengar, dan dibaca yang disajikan dalam berbagai kemasan dan format sesuai dengan perkembangan teknologi informasi dan komunikasi secara elektronik ataupun non elektronik”

Dalam pasal di atas terdapat frase kalimat dilihat, didengar, dibaca, maka suatu jika tanda tangan sebagai bentuk dari informasi harus dapat berlaku seperti frase kalimat tersebut, kemudian terkait perjanjian termasuk dokumen elektronik, terlebih dahulu harus dipahami bahwa data pribadi adalah setiap data tentang seseorang baik teridentifikasi secara tersendiri atau dikombinasikan dan dapat diidentifikasi secara tersendiri atau dikombinasikan dengan informasi lainnya sebagai suatu kesatuan baik secara langsung maupun tidak langsung melalui sistem elektronik ataupun non elektronik. Sejak diundangkannya Undang-undang Nomor 11 Tahun 2008 tentang informasi dan Transaksi Elektronik (UU ITE), maka terdapat penambahan jenis alat bukti di persidangan yakni informasi elektronik/atau dokumen elektronik. Dalam ketentuan umum UUIE dapat diketahui bahwa jenis data elektronik seperti tulisan, foto, suara, gambar, merupakan informasi elektronik sedangkan informasi elektronik seperti tulisan, foto, suara, gambar yang disimpan pada flash disk yang dapat dibuka melalui perangkat komputer merupakan dokumen elektronik.

Dokumen elektronik yang ditandatangani melalui tanda tangan digital di dalam hukum pembuktian di Indonesia, diakui esensinya setelah diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Dokumen elektronik dapat dikatakan sah apabila menggunakan sistem pengamanan yang mampu dipertanggung jawabkan sesuai dengan perkembangan teknologi informasi. Kekuatan pembuktian suatu dokumen elektronik yang ditandatangani dengan tanda tangan digital hanyalah akta di bawah tangan tanpa perantara atau tidak dihadapan pejabat yang berwenang, maka akan memiliki nilai pembuktian asalkan terdapat iktikad baik dari para pihak dan tidak ada pihak yang membantahnya. Tanda tangan digital memiliki eksistensi dalam sebuah dokumen elektronik yang memiliki kekuatan hukum dan akibat hukum yang sama dengan tanda tangan pada dokumen tertulis lainnya, karena terdapat teknik kriptografi asimetris yaitu pasangan kunci kriptografi yang salah satunya digunakan untuk proses enkripsi dan yang satu lagi untuk dekripsi. Semua orang yang mendapatkan kunci publik dapat menggunakannya untuk mengenkripsikan suatu pesan, data ataupun informasi, sedangkan hanya satu orang saja yang memiliki rahasia tertentu dalam hal ini kunci privat untuk melakukan pembongkaran terhadap sandi yang dikirim untuknya.¹⁶ Hal tersebut merupakan suatu bukti sebagaimana dokumen tertulis lainnya.

¹⁶ Arif Amrulloh & Ujianto, E. I. H, “Kriptografi Simetris Menggunakan Algoritma Vigenere Cipher”, *Jurnal CoreIT*, Vol. 5 No. 2, Tahun 2019, hlm. 71–77.

Tanda tangan digital pada suatu dokumen elektronik dapat mempunyai kekuatan pembuktian di pengadilan harus mendaftarkan tanda tangan digital pada badan CA (*Certification Authority*), maka CA disebut sebagai pejabat umum sehingga dengan memanfaatkan infrastruktur yang telah diberikan CA khususnya kemampuan untuk mengetahui kapan transaksi elektronik yang ditandatangani, maka transaksi elektronik yang ditanda tangani dipersamakan dengan akta otentik yang dibuat yang dibuat di depan pejabat yang berwenang. Apabila syarat-syarat keabsahan suatu perjanjian sebagaimana yang tertuang dalam pasal 1320 BW maka dihubungkan pada proses sertifikat digital yang notabene merupakan bagian dari PKI (*public key infrastructure*).

Dari penjelasan di atas, dapat disimpulkan bahwa tanda tangan yang disertifikasi oleh Lembaga Sertifikasi Otoritas lebih aman dalam mengotentikasi suatu dokumen, dan sangat sulit untuk memalsukan tanda tangan dan menggabungkannya dengan kombinasi unik tanda tangan digital, dokumen dan kunci pribadi, jika dia telah menerapkan ketentuan hukum yang relevan, maka sebenarnya tidak bertentangan dengan hukum. Dokumen yang ditandatangani secara digital merupakan kelanjutan dari alat bukti dalam hukum acara perdata Indonesia, bahwa setiap transaksi elektronik dengan tanda tangan digital dapat dianggap suatu perbuatan, meskipun kekuatan pembuktiannya sama dengan akta otentik yang dibuat oleh pejabat yang berwenang. Dengan pengecualian ketentuan 5 Undang-Undang Nomor 11 Tahun 2008, yang berlaku untuk peraturan tentang informasi elektronik atau dokumen elektronik yang ditentukan dalam ayat (1).

Pasal 164 dan Pasal 1866 Kitab Undang-Undang Hukum Perdata menentukan ada 5 (lima) alat bukti yang terdiri dari bukti tulisan, bukti saksi, persangkaan-persangkaan, pengakuan dan sumpah. Mengenai ketentuan tersebut apakah tanda tangan digital dan sertifikat digital dapat disamakan kedudukannya dengan dokumen elektronik pada umumnya sehingga dianalogikan dengan bukti tulisan atau apakah tanda tangan digital dan sertifikat digital dianalogikan sebagai akta otentik/dibawah tangan.

Melihat ketentuan yang ada, kemungkinan tanda tangan digital digunakan sebagai alat bukti akan ditolak baik oleh hakim, karena pembuktian yang dipersyaratkan adalah pembuktian tertulis, sedangkan tandatangan digital sifatnya tanpa kertas. Berdasarkan penjelasan di atas, maka perlu dibahas kembali terkait suatu dokumen elektronik dapat diterima sebagai alat bukti di persidangan, dikarenakan dalam pasal 164 HIR yang mensyaratkan salah satu bukti itu harus dalam bentuk tertulis/tulisan/surat karena dari kelima syarat yang telah disebutkan diatas, apalagi disebutkan dengan bukti tulisan yang berupa akta otentik. Suatu akta otentik mempunyai kekuatan pembuktian formil, materil dan mengikat artinya alat bukti yang sempurna. Jika ketentuan tersebut dianggap pasti, maka pengakuan dari dokumen elektronik sebagai alat bukti akan menjadi masalah. Dengan itu terobosan hukum, dimana hakim sebagai penegak hukum dan penegak keadilan untuk menggali, dan memahami nilai-nilai hukum yang ada di masyarakat.¹⁷

Pada alat bukti dari transaksi elektronik untuk meyakinkan hakim dalam persidangan dengan cara merubah dokumen elektronik tersebut dalam bentuk analog, digital, elektronik, atau data yang didalam dokumen tersebut di print/di copy, dan juga tanda tangan dari kunci publik atau salinan

¹⁷ Pasal 27 UU Pokok-Pokok Kehakiman

sertifikat digital yang dijadikan dalam satu berkas. Keberadaan sertifikat digital digunakan untuk mengidentifikasi keabsahan pihak-pihak yang bertransaksi dan membubuhkan tanda tangan digital tersebut, sertifikat itu diterbitkan oleh suatu lembaga yang dipercaya untuk mengelola data-data yang terkait dengan sertifikat, untuk mengandalkan kepercayaan. Maka dari kebutuhan pemanfaatan tanda tangan digital memunculkan salah satu produk yaitu sebuah aplikasi yang diberi sebutan PrivyID untuk menandatangani sebuah perjanjian/dokumen di *platform* apapun, teknologi tersebut menyediakan sertifikat elektronik dalam hal penggunaan tanda tangan digital.

Dalam penyelesaian sengketa secara daring diatur dalam pasal 41 UU 11 Tahun 2008 tentang informasi dan transaksi elektronik, dalam hal tersebut masyarakat dapat berperan meningkatkan pemanfaatan teknologi informasi melalui penggunaan dan penyelenggaraan sistem elektronik dan transaksi elektronik sesuai dengan ketentuan UU ITE. Goodman dan Joseph dalam tulisannya yang berjudul "*The Pros and Cons of Online Dispute Resolution: an Assessment of Cyber-Mediation Websites*", menyebutkan bahwa saat ini terdapat tiga jenis Sistem ODR yang berkembang di dunia ini¹⁸.

Negara Tiongkok dimana merupakan salah satu negara yang berminat mendirikan Lembaga Penyelesaian Sengketa Secara Daring yang digunakan untuk menangani kasus internet komersial. Badan penyelesaian sengketa yang didirikan oleh negara Tiongkok berbentuk pengadilan internet, sidang dengan cara melalui video dimana para saksi di periksa lewat keanggotaan dalam sistem pembayaran internet. Penyelesaian sengketa bisnis melalui internet, pada prinsipnya dapat dilakukan secara litigasi dan nonlitigasi atau diluar pengadilan dapat ditempuh dengan menggunakan alternatif penyelesaian sengketa (APS) dengan cara Negoisasi, Arbitrase, Mediasi¹⁹. Dimana dengan negoisasi atau musyawarah diyakini paling sering menghasilkan kesuksesan dan telah menyelesaikan sengketa internasional. Selanjutnya Arbitrase yaitu Perjanjian arbitrase, sebagaimana perjanjian pada umumnya didasarkan pada asas kepastian hukum yang diakomodasi dari Pasal 1338 ayat (1) KUH Perdata yang berbunyi "semua perjanjian yang dibuat secara sah berlaku sebagai Undang-Undang bagi mereka yang membuatnya". Asas itikad baik dalam arbitrase diakomodasi dari bunyi pasal 1338 ayat 3 KUH Perdata yang menyatakan "suatu perjanjian harus dilaksanakan dengan itikad baik". Itikad baik adalah faktor utama dalam pelaksanaan kontrak bisni, jika para pihak mempunyai itikad baik maka kontrak bisnis akan berjalan dengan baik. Dan yang terakhir adalah Mediasi, Mediasi atau penengahan merupakan upaya penyelesaian sengketa secara nonlitigasi yaitu berdasarkan kesepakatan Bersama para pihak melalui pihak penengah atau mediator yang bersikap netral dan tidak membuat keputusan sendiri, tetapi menyediakan dialog antara pihak dalam keterbukaan dan jujur untuk dapat mencapai mufakat.²⁰

¹⁸ Goodman, Joseph W., Dalam Otoritas Jasa Keuangan (Departemen Perlindungan Konsumen), (Kajian Perlindungan Konsumen Sektor Jasa Keuangan: Online Dispute Resolution (ODR), OJK: Jakarta: 2017, hlm. 29.

¹⁹ Hariyani, I., C. Y. Serfiani, dan R. Serfianto. D. Purnomo, *Penyelesaian Sengketa Bisnis*, PT Gramedia Pustaka Utama, Jakarta: 2018, hlm. 153.

²⁰ Ibid., hlm. 62-64.

PENUTUP

Agar tanda tangan di Indonesia berkepastian hukum hendaknya pemerintah mengesahkan peraturan mengenai tanda tangan digital dan sertifikat elektronik, supaya ada aturan hukum lanjutan dari Undang-Undang Nomor 11 tahun 2008 serta Pemerintah segera membuat/mengesahkan serta memberikan ijin dalam peraturan pemakaian aplikasi PrivyID supaya setiap orang yang telah menggunakan aplikasi tersebut lebih percaya dalam proses penandatanganan, serta memberikan ijin kepada CA, baik pemerintah maupun swasta sehingga pelaksanaan transaksi melalui e-commerce dengan menggunakan dokumen elektronik sebagai perjanjian antara pihak mempunyai kekuatan pembuktian dalam persidangan.

DAFTAR PUSTAKA

Buku

- Abdul Halim Berkatullah dan Prasetyo, *Bisnis E-Commerce, Studi Sistem Keamanan Dan Hukum di Indonesia*. Cetakan I, II. Yogyakarta: Pustaka Pelajar, Yogyakarta: 2006.
- Atmojo, *Penerapan Internet Untuk Bisnis*. Ghalia Indonesia, Yogyakarta: 2020.
- Barkatullah A. H., *Hukum Transaksi Elektronik. Sebagai Panduan dalam Menghadapi Era Digital Bisnis e-commerce di Indonesia*, Hikam Media Utama, Bandung: 2018.
- Carlo A Garungan, *Tanggung Jawab Penyelenggara Sistem Informasi Jika Terjadi Kegagalan Sistem*, Sam Ratulangi University, Manado: 2013.
- Dony Ariyus, *Kriptografi Keamanan Data dan Kriptografi*, Penerbit Andi Offset, Yogyakarta: 2006.
- Edmon Makarim, *Notaris dan Transaksi Elektrronik*, PT Raja Grafindo Persada, Jakarta: 2013.
- Goodman, Joseph W., *Dalam Otoritas Jasa Keuangan (Departemen Perlindungan Konsumen), (Kajian PerlindunganKonsumen Sektor Jasa Keuangan: Online Dispute Resolution (ODR)*, OJK, Jakarta: 2017.
- Hariyani, I., C. Y. Serfiani, dan R. Serfianto. D. Purnomo, *Penyelesaian Sengketa Bisnis*, PT Gramedia Pustaka Utama, Jakarta: 2018.
- Roberto Akyuwen, *Lebih Menenal Digital Banking Manfaat, Peluang, dan Tantangan*. Universitas Gajah Mada Anggota IKAPI, Jakarta: 2020.
- Soerjono Soekanto dan Sri Mamudj, *Penelitian Hukum Normatif; Suatu Tinjauan Singkat*, Raja Grafindo Persada, Jakarta: 2021.
- Tan Thong Kie, *Studi Notariat dan Serba-Serbi Praktek Notaris*, PT. Ichtiar Baru Van Hoeve, Jakarta: 2007.

Jurnal

- Arif Amrulloh & Ujianto, E. I. H., "Kriptografi Simetris Menggunakan Algoritma Vigenere Cipher", *Jurnal CoreIT*, Vol. 5, No 2.
- Muhammad Natsir, "Pengembangan Prototype Sistem Kriptografi Untuk Enkripsi Dan Dekripsi Data Office Menggunakan Metode Blowfish Dengan Bahasa Pemrograman Java", *Jurnal Format*, 2017, Vol. 6.

Rizki Sulistio, *“The Role & Advantages of Digital Signatures for the Fintech Industry, sharing Session PrivyID,”* 2019. Dalam Affan Muhammad Andalan, *“Kedudukan Tanda Tangan Elektronik dalam Transaksi Teknologi Finansial,”* *Jurist Diction*, 2019, Vol. 2 No. 6.

Surohman, (et.al.), *“Analisa Sentimen Terhadap Review Fintech Dengan Metode Naive Bayes Classifier Dan K-Nearest Neighbor,”* *Jurnal Sains dan manajemen*, 2020, Vol. 8 No. 2.

Peraturan Perundang-Undangan

Undang-Undang Pokok-Pokok Kekuasaan Kehakiman

Undang-Undang Nomor 11 tahun 2018 tentang informasi dan transaksi elektronik (Undang-Undang ITE)

Peraturan pemerintah Nomor. 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik

Sumber lainnya

Information Security Committee, Section of Science & Technology - American Bar Association, Digital Signature Guidlines, American Bar Association, United States: 2016.

Maria Yuniar, *“1,9 Juta Orang Indonesia Pakai Tanda Tangan Digital,”* last modified 2022, <https://www.ekrut.com/media/1-9-juta-orang-indonesia-pakai-tanda-tangan-digital>.

Wita Dewisari Tasya, *“Analisis Keamanan Penyelenggara Sertifikasi Elektronik Indonesia: PT Privy Identitas Digital,”* Makalah II, [diakses pada 12/12/ 2021-2022].