



## **Keabsahan Digital Signature/Tanda tangan Elektronik Dinjau Dalam Perspektif Hukum Perdata dan UU ITE**

**Eka Wahyuni<sup>1,2</sup>, Sufirman Rahman<sup>1</sup>& Andi Risma<sup>1</sup>**

<sup>1</sup>Magister Ilmu Hukum, Universitas Muslim Indonesia.

<sup>2</sup>Koresponden Penulis, E-mail: [eka.wahyuni@gmail.com](mailto:eka.wahyuni@gmail.com)

### **ABSTRAK**

*Tujuan Penelitian menganalisis keabsahan digital signature dan kekuatan pembuktian digital signature sebagai alat bukti. Tipe penelitian adalah yuridis normatif. Pendekatan penelitian ini menggunakan pendekatan perundang-undangan (statute approach). Hasil penelitian ini menunjukkan bahwa (1) Kekuatan pembuktian digital signature sebagai alat bukti yakni berdasarkan Pasal 5 UU ITE maka kekuatan penggunaan alat bukti digital signature dalam hukum perdata memiliki kekuatan hukum dan merupakan perluasan dari alat bukti berlaku sesuai dengan hukum acara yang berlaku di Indonesia. (2) keabsahan suatu digital signature yang tercantum dalam suatu dokumen elektronik terkait legalitasnya dalam hukum positif Indonesia dinilai sah dalam perspektif hukum perdata adalah berdasarkan pada syarat-syarat perjanjian sebagaimana yang termuat dalam Pasal 1320 KUH Perdata serta pemberlakuan Undang-Undang Nomor 19 Tahun 2016 Perubahan atas Undang-Undang Nomor 11 Tahun 2008 serta Peraturan Pemerintah No.71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.*

**Kata Kunci:** Digital; Tanda Tangan; Elektronik

### **ABSTRACT**

*This research objective to analyze the validity of digital signatures and the strength of proof of digital signatures as evidence. The type of research is normative juridical. This research approach uses a statutory approach. The results of this study indicate that (1) The strength of digital signature evidence as evidence, namely based on Article 5 of the ITE Law, the power of using digital signature evidence in civil law has legal force and is an extension of valid evidence in accordance with the applicable procedural law in Indonesia. (2) the validity of a digital signature contained in an electronic document related to its legality in Indonesian positive law is considered valid in the perspective of civil law based on the terms of the agreement as contained in Article 1320 of the Civil Code and the enactment of Law Number 19 of 2016 Amendment on Law Number 11 of 2008 and Government Regulation No. 71 of 2019 concerning the Implementation of Electronic Systems and Transactions.*

**Keywords:** Digital; Signature; Electronic

## PENDAHULUAN

Wabah *corona virus disease-2019* (covid-19) menjadi berita utama di berbagai negara pada tiga tahun terakhir ini, sampai saat ini penyebaran wabah yang pertama kali di temukan di Wuhan, China pada Desember 2019 lalu. *World Health Organization (WHO)* pada desember 2019 menginformasikan mengenai kasus virus corona yang pertama kali muncul dan menyerang manusia, berawal dari cluster pneumonia dengan etiologi baru di Kota Wuhan, provinsi Hubei, Cina dan kemudian meluas hingga ke luar China. Selanjutnya COVID-19 dinyatakan sebagai *Public Health Emergency of International Concern (PHEIC)* pada 30 Januari 2020, dan COVID-19 ditetapkan sebagai pandemi pada 11 Maret 2020 (Agustino, 2020).

Berdampingan hidup dimasa pandemi COVID-19 muncul istilah-istilah baru seperti *new normal*, *virtual meeting*, *zoom meeting* dll, sudah tidak menjadi asing lagi, kemudian disamping itu selain pengaruh globalisasi dengan penggunaan sarana teknologi informasi dan komunikasi telah mengubah pola hidup masyarakat dan berkembang dalam tatanan kehidupan baru dan mendorong terjadinya perubahan sosial, ekonomi, budaya, pertahanan, keamanan dan penegakan hukum, dari berbagai dampak positif hingga negatif seperti, perbuatan melawan hukum di dunia maya merupakan fenomena yang sangat mengawatirkan, mengingat tindakan *carding*, *hacking*, penipuan dan penyebaran informasi destruktif telah menjadi bagian dari aktivitas pelaku kejahatan di dunia maya. Kenyataan itu, demikian sangat kontras dengan ketiadaan atau kurangnya regulasi yang mengatur secara spesifik pemanfaatan teknologi informasi dan komunikasi di berbagai sektor. Oleh karena itu, untuk menjamin kepastian hukum, pemerintah berkewajiban melakukan regulasi terhadap berbagai aktivitas terkait dengan pemanfaatan teknologi informasi dan komunikasi tersebut.

Hal ini terkait munculnya berbagai fenomena baru yang merupakan implikasi dari kemajuan teknologi dan informasi. Perkembangan yang saat ini sangat mempengaruhi kehidupan masyarakat global, perkembangan teknologi dan informasi, yang antara lain ditandai dengan era teknologi informatika yang memperkenalkan dunia maya (*cyberspace*) dengan hadirnya *interconnected network* (internet) yang mempergunakan komunikasi tanpa kertas (*paperless document*) (Watie, 2016).

Transaksi elektronik bersifat *non face* (tanpa bertatap muka), dan *non sign* (tidak memakai tanda tangan basah) dan tanpa batas wilayah (seseorang dapat melakukan Transaksi Elektronik dengan pihak lain walaupun mereka berada di Negara yang berbeda) dengan menggunakan teknologi informasi (Slamet & Paliling, 2019). Saat ini perkembangan aspek keamanan dalam informasi sudah mulai diperhatikan, ketika informasi sudah menjadi maju maka akan sejalan akan terdapat resiko-resiko yang harus ditanggung oleh orang-orang, baik yang mengirim, membutuhkan, ataupun sekedar melihatnya, dikarenakan penggunaan informasi elektronik ini menggunakan jaringan publik, dimana setiap orang dapat mengetahui informasi elektronik tersebut, atau apabila salah satu pihak tidak melaksanakan prestasi dari transaksi elektronik yang telah disepakati dari pihak yang lain, hal ini tentu merugikan pihak yang berkepentingan yang menggunakan teknologi informasi untuk penjualan suatu barang atau jasa.

Permasalahan hukum yang sering kali dihadapi adalah ketika terkait dengan penyampaian informasi, komunikasi, dan/atau transaksi secara elektronik, khususnya dalam hal pembuktian dan hal yang terkait dengan perbuatan hukum yang dilaksanakan melalui sistem elektronik (Ersya, 2017). Permasalahan yang lebih luas terjadi pada bidang keperdataan karena transaksi elektronik untuk kegiatan perdagangan melalui sistem elektronik/*electronic commerce* telah menjadi bagian dari perniagaan nasional dan internasional. Kenyataan ini menunjukkan bahwa konvergensi di bidang teknologi informasi, media, dan informatika (telematika) berkembang terus tanpa dapat dibendung, seiring dengan ditemukannya perkembangan baru dibidang teknologi informasi, media, dan komunikasi (Rahmatullah, 2017).

Penggunaan teknologi informasi berbasis sarana elektronik dalam transaksi elektronik diyakini memberikan dampak yang positif bagi pelaku bisnis terutama dalam hal kecepatan dan kemudahan melakukan transaksi dalam interaksi global tanpa batasan tempat dan waktu (Sumadi, 2016). Berkaitan dengan hal tersebut kebutuhan akan kerahasiaan informasi serta penjagaan atas keaslian suatu informasi pun semakin meningkat sehingga Pemerintah Republik Indonesia menerbitkan Undang-Undang Nomor 11 tahun 2008 kemudian diubah menjadi Undang-Undang No 19 Tahun 2016 tentang Transaksi dan Informasi elektronik yang selanjutnya disebut UU ITE (Makarim, 2015).

Salah satu yang perlu diperhatikan dalam transaksi elektronik adalah implementasi *digital signature* yang bertujuan untuk melegalisasi dokumen/hasil dalam suatu transaksi elektronik. Terkait dengan hal tersebut UU ITE No.19 tahun 2016 mengatur autentifikasi hak dan kewajiban dalam sebuah dokumen elektronik yang ditandatangani secara digital (*digital signature*) (Hassanah, 2016). Penggunaan tanda tangan tidak terlepas dari kehidupan kita sehari-hari memngingat cara ini lebih praktis dan efisien. Betapa tidak tanda tangan memiliki berbagai fungsi penting bagi kita semua seperti untuk membuktikan identitas, menjaga keutuhan atau dokumen, atau melakukan koreksi atas surat atau dokumen sebagai bukti persetujuan perubahan dan kebutuhan pengesahaan lainnya (Suwignyo, 2009).

Di zaman sekarang ketika insiden perusakan dan pemalsuan data semakin lazim, telah menjadi keharusan untuk melindungi data apapun yang dikirim secara online. Karena alasan itu tadi *digital signature* semakin populer di kalangan profesional berkat kemampuan mereka untuk memvalidasi keaslian sebuah dokumen, file atau perangkat lunak. Kemudian seiring dengan perkembangan teknologi *digital signature* juga mengalami perkembangan dan transformasi. Transformasi *digital signature* ini hadir dalam bentuk tanda tangan digital atau *digital signature*. Namun tidak semua *digital signature* memiliki kekuatan perlindungan yang sama. Dalam hukum positif Indonesia menentukan bahwa hanya satu cara untuk memberikan kekuatan hukum dan akibat hukum terhadap suatu dokumen yaitu tanda tangan manuskrip. Namun dalam praktek perdagangan khususnya, tanda tangan manuskrip sudah kian tergeser dengan penggunaan tanda tangan elektronik yang melekat pada suatu dokumen atau biasa disebut dengan dokumen elektronik, sehingga muncul perdebatan tentang pengakuan, kekuatan hukum dan akibat hukum dari sebuah tanda tangan elektronik atau *digital signature* (Hudzaifah, 2015).

Dalam kegiatan *e-commerce*, dokumen elektronik dengan sebuah *digital signature* dapat dikategorikan sebagai bukti tertulis. Tetapi terdapat suatu prinsip hukum yang menyebabkan sulitnya pengembangan penggunaan dan dokumen elektronik yang didalamnya terdapat *digital signature* yakni adanya syarat bahwa dokumen tersebut harus dapat dilihat dan disimpan dalam bentuk kertas (Letsoin, 2010). Permasalahan akan muncul ketika seseorang hendak melakukan transaksi misalnya saja pembelian barang, maka para pihak sudah mulai dihadapkan pada berbagai permasalahan hukum seperti keabsahan dokumen yang dibuat, tanda tangan digital (*digital signature*) yang dibuat saat orang tersebut menyatakan sepakat untuk bertransaksi, kekuatan mengikat dari kontrak tersebut serta pembatalan transaksi dan sebagainya. Salah satu isu yang *crucial* dalam transaksi *e-commerce* adalah yang menyangkut keamanan dan mekanisme pembayaran (*payment mechanism*) dan jaminan keamanan dalam bertransaksi (*security risk*) seperti informasi mengenai transfer data dan identitas pribadi konsumen, yang dalam hal ini ada dua permasalahan utama yaitu : pertama mengenai *Identification Integrity* yang menyangkut identitas pengirim yang di kuatkan lewat tanda tangan digital (*digital signature*), kedua mengenai *message integrity* yang menyangkut apakah pesan yang dikirimkan oleh pengirim benar-benar diterima oleh penerima yang dikehendaki (*Intended Recipient*).

Adapun di negara kita selama ini mengenal berbagai *digital signature*/ jenis tanda tangan yaitu ada yang berupa tanda tangan basah cap jempol, tanda tangan elektronik, dan tanda tangan yang dibuat dengan proses *scan* seperti tanda pada umumnya atau tanda tangan konvensional tanda tangan yang dalam penggunaannya diakui dalam hukum pembuktian yang masih perlu pengkajian secara spesifik adalah terkait dengan tanda tangan digital / *digital signature*.

Keabsahan tanda tangan elektronik/*digital signature* dalam suatu perjanjian dalam perspektif hukum perdata adalah dengan mengacu kepada undang undang ITE No.11 Tahun 2008 atas perubahan Undang Undang No.19 Tahun 2016 tentang Informasi dan Transaksi Elektronik serta Peraturan Pemerintah No.71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik sebagai peraturan pelaksana dari transaksi elektronik yang kemudian dikaitkan dengan Pasal Pembuktian serta asas-asas perjanjian dalam Kitab Undang-Undang Hukum Perdata / KUH Perdata yang mana apabila salah satu pihak wanprestasi/cidera janji bagaimana kemudian langkah hukum yang dapat ditempuh.

Selain itu tanda tangan elektronik muncul dalam suatu dokumen elektronik yang pada dasarnya bukan merupakan dokumen tertulis (*non paperless*). Berpijak pada hal tersebut, maka sejatinya konsep tanda elektronik tidak sesuai dengan prinsip hukum yang menyatakan bahwa suatu dokumen harus dapat dilihat, dikirim dan disimpan dalam bentuk kertas. Seiring dengan kemajuan teknologi yang terus berkembang, maka sudah selayaknya apabila di bidang informasi dan teknologi mulai diakomodir kedalam sistem hukum perdata di Indonesia. Sehingga banyak pihak meragukan keabsahan *digital signature* / tanda tangan digital saat ini baik dalam lingkup persidangan maupun dalam proses perjanjian.

## **METODE PENELITIAN**

Metode penelitian yang digunakan dalam proposal penelitian ini adalah yuridis normatif. Dimana penelitian ini dilakukan dengan cara mengkaji, mendeskripsikan

dan menganalisis bahan-bahan kepustakaan yang berupa literatur, peraturan perundang-undangan dan isi dari perjanjian yang berkaitan dengan permasalahan yang akan dibahas. Pendekatan penelitian yang digunakan dalam penulisan ini adalah pendekatan perundang-undangan (*statute approach*) dan pendekatan kasus (*case approach*). Pendekatan perundang-undangan (*statute approach*) dilakukan dengan menelaah semua peraturan perundang-undangan dan regulasi yang bersangkutan paut dengan isu hukum yang sedang diteliti dan Pendekatan doctrinal.

## PEMBAHASAN

### A. Kekuatan Pembuktian *Digital Signature*/Tanda Tangan Elektronik sebagai Alat Bukti

#### 1. Pembuktian Perkara Perdata di Indonesia

Pembuktian adalah penyajian alat-alat bukti yang sah menurut hukum oleh para pihak yang berperkara kepada hakim dalam suatu persidangan dengan tujuan untuk memperkuat kebenaran dalil tentang fakta hukum yang menjadi pokok sengketa, sehingga hakim memperoleh dasar kepastian untuk menjatuhkan putusan. Pembuktian merupakan salah satu aspek yang memegang peranan sentral dalam suatu proses peradilan, dalam kasus perdata selama tahap pembuktian ini para pihak diberikan kesempatan untuk menunjukkan kebenaran terhadap fakta-fakta hukum yang menjadi titik pokok sengketa.

Sampai saat ini hukum pembuktian positif di Indonesia masih berdasarkan pada HIR/RBg dan BW buku ke IV yang merupakan produk pemerintah Hindia Belanda. Hukum pembuktian yang tercantum dalam HIR dan RBg adalah hukum pembuktian formil, sedangkan dalam BW adalah hukum pembuktian materiil. Hukum pembuktian materiil mengatur tentang dapat tidaknya diterima pembuktian dengan alat-alat bukti tertentu di persidangan serta kekuatan pembuktiannya, sedangkan hukum pembuktian formil mengatur tentang caranya mengadakan pembuktian.

Pembuktian merupakan salah satu dari serangkaian proses beracara di pengadilan yang memiliki fungsi penting dalam membantu hakim untuk menemukan hukum dan menjatuhkan putusan. KUH Perdata telah menentukan jenis-jenis alat bukti yang sah dengan kekuatan pembuktiannya masing-masing. Adapun alat-alat bukti yang sah tersebut diatur dalam Pasal 1866 KUH Perdata. Pasal 164 HIR/284 RBg dan Pasal 1866 BW, mengatur mengenai alat-alat bukti yang dapat digunakan dalam penyelesaian sengketa perdata ke pengadilan secara limitatif dan disusun secara berurutan dari mulai alat bukti surat, keterangan saksi, persangkaan-persangkaan, pengakuan dan sumpah.

Dalam kitab Undang-Undang Hukum Perdata pembuktian umumnya diatur dalam Buku Empat (IV) tentang Pembuktian dan Daluarsa. Adapun perihal sistem pembuktiannya, hukum acara perdata menganut prinsip "Mencari Kebenaran Formil" sehingga hakim dalam memeriksa perkara bersifat pasif. Artinya, ia tidak diperkenankan untuk mengambil prakarsa aktif dalam menambah atau mengajukan pembuktian yang diperlukan karena hal tersebut merupakan pilihan hak dari masing-masing pihak.

Salah satu tugas hakim dalam mencari kebenaran formil adalah dengan menyelidiki hubungan hukum yang menjadi dasar gugatan benar-benar ada atau tidak. Adanya

hubungan hukum inilah yang harus terbukti apabila penggugat menginginkan kemenangan dalam suatu perkara. Prinsip lain yang ditemukan dalam pembuktian perkara perdata adalah putusan yang diambil merupakan hasil dari pembuktian fakta yang ada di persidangan. Hakim tidak dibenarkan mengambil putusan tanpa pembuktian. Kunci ditolak atau dikabulkannya gugatan haruslah berdasarkan pembuktian yang bersumber dari fakta-fakta yang diajukan para pihak. Pembuktian hanya dapat ditegakkan berdasarkan dukungan fakta-fakta sehingga pembuktian tidak dapat ditegakkan tanpa adanya fakta yang ada.

Seiring dengan perkembangan kemajuan di bidang teknologi informasi dan telekomunikasi, berkembang pula hal-hal atau cara-cara yang dapat dijadikan sebagai alat bukti dalam hubungan keperdataan yang terjadi di masyarakat modern dewasa ini dengan munculnya berbagai macam transaksi modern. Perkembangan dalam masyarakat yang disertai dengan perkembangan teknologi informasi dan telekomunikasi, timbul pula bermacam alat bukti dalam hubungan hukum keperdataan di luar yang telah diatur dalam peraturan acara perdata (HIR/RBg). Dimulai dengan munculnya fotokopi sampai dengan dikenal dan digunakannya alat bukti elektronik.

Foto (potret) dan hasil rekaman suara atau gambar (dalam perkembangannya termasuk hasil rekaman cctv), berdasarkan literatur tidak dapat dijadikan alat bukti karena dapat saja merupakan hasil rekayasa sehingga tidak dapat membuktikan apa yang sebenarnya terjadi. Namun dalam perkembangan dewasa ini, dengan kemajuan teknologi di bidang informasi dan telekomunikasi, asli atau tidaknya suatu foto dan hasil rekaman suara atau gambar dapat diketahui dengan menggunakan teknik tertentu.

Meski telah diatur secara jelas dan terperinci mengenai alat-alat bukti yang sah dalam hukum pembuktian, namun pada beberapa sengketa perdata khususnya yang menyangkut *e-commerce*, terdapat penggunaan tanda tangan elektronik/*digital signature* sebagai alat bukti di persidangan sehingga pada perkembangannya alat bukti hanya terbatas pada apa yang telah diatur dalam Pasal 1866 KUH Perdata tersebut olehnya itu dengan kehadiran Undang Undang ITE No.19 Tahun 2016 dan PP No.71 Tahun 2019 memberikan payung hukum lebih lanjut mengenai implementasi *Digital Signature*/Tanda Tangan Elektronik yang melekat pada sebuah dokumen elektronik.

## **2. Pembuktian *Digital Signature*/Tanda Tangan Elektronik di Persidangan**

Meningkatnya proses transformasi menuju digital industri berbasis *cyber physical system* atau yang dikenal industri 4.0, telah merubah berbagai bentuk kegiatan fisik (konvensional) menuju industri berbasis digital, tak tertinggal bahkan hambatan yang dihadapi korporasi terkait efisiensi waktu dan biaya mengakibatkan terwujudnya sebuah konsep penandatanganan kontrak berbasis digital (*digital signature*/tanda tangan elektronik).

Implementasi *digital signature*/tanda tangan elektronik merupakan salah satu metode yang dapat digunakan untuk menentukan keaslian atau keabsahan suatu bukti elektronik berupa dokumen atau informasi elektronik. *Digital signature* sendiri adalah informasi elektronik yang dilekatkan pada suatu informasi elektronik, yang dapat digunakan penandatanganan sebagai identitas dan statusnya sebagai subjek hukum.

Berbeda dengan tanda tangan manuskrip keberadaan *digital signature* yang melekat pada suatu dokumen elektronik, *digital signature* hadir dengan dengan dua kunci kriptografi kunci publik (*public key*) dan kunci privat (*private key*) yang saling mengautentifikasi. Individu yang membuat *digital signature* menggunakan kunci privat untuk mengenkripsi data terkait tanda tangan, sedangkan satu-satunya cara untuk mendeskripsi data tersebut adalah dengan kunci publik penanda tangan.

Tujuan dari suatu *digital signature* dalam suatu dokumen elektronik adalah untuk memastikan otentitas dari dokumen tersebut. Suatu *digital signature* menggunakan cara yang berbeda untuk menandai suatu dokumen, sehingga dokumen atau data tidak hanya mengidentifikasi dari pengirim namun juga memastikan keutuhan dari dokumen tersebut tidak berubah selama proses pengiriman (transmisi). Manfaat dari menggunakan *digital signature* yang diaplikasikan pada pesan atau data elektronik yang dikirimkan, dapat menjamin bahwa pesan atau data elektronik tersebut tidak mengalami suatu perubahan atau modifikasi oleh pihak yang tidak berwenang.

Jaminan *authenticity* ini dapat dilihat adanya *hash function* dalam sistem *digital signature*, *hash function* atau biasa disebut dengan fungsi hash yakni fungsi satu arah dan akan menghasilkan nilai unik untuk setiap data yang dimasukkan, oleh karena itu jika ada perubahan satu bit saja pada konten dokumen maka nilai hash yang akan dihasilkan akan berbeda sehingga penerima data (*recipient*) dapat melakukan perbandingan *hash value*. Apabila *hash value*-sama dan sesuai, maka data tersebut benar-benar otentik, tidak pernah terjadi suatu tindakan yang sifatnya merubah data tersebut pada saat proses pengiriman, sehingga terjamin *authenticity*-nya. Sebaliknya apabila tidak sama atau ada perubahan *hash value*, maka patut dicurigai dan langsung dapat disimpulkan bahwa penerima menerima data yang telah dimodifikasi.

Penggunaan *digital signature* dalam proses pembentukan perjanjian atau kontrak (*e-commerce*), akan memudahkan mekanisme pembuktian dalam kasus perdata. Hal ini karena dengan memberikan *digital signature* pada data elektronik yang dikirimkan, maka akan dapat ditunjukkan dari mana data elektronik tersebut berasal. Terjaminnya integritas pesan tersebut dapat terjadi karena keberadaan *digital certificate* (sertifikat elektronik) yang diperoleh atas dasar aplikasi kepada *certification authority* oleh user (pengguna) atau *subscriber*.

Proses pembuktian baru terjadi apabila ada sengketa diantara para pihak, sengketa itu sendiri biasanya penyelesaiannya ditentukan oleh satu klausula dalam perjanjian. Umumnya penyelesaian tersebut melalui litigasi atau non litigasi. Pembuktian salah satu hal yang sangat penting dalam proses penyelesaian sengketa perdata di pengadilan, dengan adanya tahap pembuktian dapat membuktikan adanya suatu peristiwa dan adanya salah satu pihak yang dinyatakan terbukti atau tidak di muka persidangan. Dengan demikian, dengan adanya pembuktian para pihak berupaya untuk memungkinkan kebenaran adanya suatu peristiwa ataupun dengan menggunakan alat-alat bukti bahwasanya pihak tersebut benar-benar melakukan peristiwa tersebut atau tidaknya. Sehingga pembuktian, hakim dapat memperoleh dasar-dasar untuk menjatuhkan putusan untuk menyelesaikan sengketa dalam persidangan.

Pengakuan akan suatu *digital signature* sebagai alat bukti yang sah dapat terlihat dari ketentuan Undang-Undang No.19 Tahun 2016 tentang Informasi dan Transaksi Elektronik Jo. Undang-Undang No.11 Tahun 2008 tentang ITE Pasal 5 Undang

Undang tersebut menegaskan bahwa “Informasi elektronik dan/atau dokumen elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah dan merupakan perluasan dari alat bukti yang sah sesuai dengan Hukum Acara yang berlaku di Indonesia sesuai dengan ketentuan yang diatur dalam Undang-Undang ini.

Berdasarkan ketentuan diatas memberikan penjelasan bahwa tanda tangan elektronik dapat dijadikan sebagai alat bukti yang sah di persidangan sebagaimana alat-alat bukti lainnya yang diatur dalam KUH Perdata maka Pasal 1869 jo Psal 1874 KUH Perdata dan Pasal 1 Ordonansi 1867 No.29 juga berlaku demikian pada tanda tangan elektronik / *digital signature* yang melekat pada dokumen eletronik tersebut memiliki kekuatan hukum. Dengan menandatangani, menunjukkan persetujuan penandatanganan atas informasi atau dokumen elektronik yang ditandatangani sekaligus menjamin kebenaran isi yang tercantum dalam tulisan tersebut.

Setelah keluarnya Undang-Undang Nomor.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik jo Undang-Undang No.19 Tahun 2016 terdapat perkembangan hukum pembuktian. Yang mana jika sebelumnya bukti elektronik hanya dapat dipakai sebagai bukti persangkaan dalam perkara perdata atau sebagai bukti petunjuk dalam perkara pidana, maka dengan keluarnya Undang-Undang Nomor 11 Tahun 2008 jo Undang-Undang No.19 Tahun 2016 tersebut dokumen elektronik dan hasil cetaknya dengan tegas diakui sebagai alat bukti yang sah di pengadilan asalkan memenuhi syarat tertentu sebagaimana ditentukan undang-undang. Dalam pasal 6 juga disebutkan bahwa informasi elektronik dan dokumen elektronik dapat dijadikan sebagai bukti di persidangan. Namun setiap informasi/dokumen elektronik tersebut baru dianggap sah sebagai alat bukti sepanjang :

1. Dapat diakses;
2. Ditampilkan;
3. Dijamin keutuhannya;
4. Dan dapat dipertanggungjawabkan;

Sebagai alat bukti, dokumen elektronik atau informasi elektronik tersebut haruslah bernilai, yaitu dapat menerangkan suatu keadaan. Hal yang krusial dalam persidangan adalah mengenai tanda tangan basah dalam suatu akte atau surat secara konvensional dengan tanda tangan elektronik/*digital signature* dalam suatu perjanjian (*e-commerce*). Dan berdasarkan Pasal 11 ayat (1) UU Nomor 19 Tahun 2019 tentang perubahan UU Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik menyebutkan bahwa tanda tangan elektronik/*digital signature* memiliki kekuatan hukum dan akibat hukum yang sah.

Berbagai mekanisme penandatanganan dapat digunakan untuk menghasilkan tanda tangan elektronik sebagaimana juga disebutkan dalam (Pasal 59 Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik). Meski demikian tidak semua tanda tangan elektronik tersebut memiliki kekuatan hukum dan akibat hukum yang sah.

Hal tersebut didasarkan pada ketentuan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang nomor 11 Tahun 2008 tentang ITE yang menerangkan bahwa tanda tangan elektronik/*digital signature* memiliki kekuatan hukum sehingga dapat dijadikan sebagai alat bukti yang sah di persidangan,

sepanjang memenuhi persyaratan yang berlaku. Yang mana ketentuan lebih lanjut ini dapat kita temukan dalam rumusan Pasal 11 Undang-Undang ITE, yang berbunyi :

“*Digital Signature*/ Tanda Tangan Elektronik memiliki kekuatan hukum dan akibat hukum yang sah selama memenuhi persyaratan sebagai berikut : (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 penanda tangan 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 penandatanganan dapat diketahui; (f) terdapat cara tertentu untuk menunjukkan bahwa penandatanganan telah memberikan persetujuan terhadap informasi elektronik yang terkait.”

Dibanding dengan tanda tangan basah yang kemungkinan dapat ditiru dan pembuktian mengenai identik atau tidak identik suatu tanda tangan basah harus melalui pemeriksaan labfor, keamanan dari tanda tangan elektronik diamankan dengan sistem teknologi yang disebut *asymmetric cryptography* yaitu setiap bit dari sebuah tanda tangan digital dienkripsi oleh lembaga penerbit yang sah. Dengan metode ini, tanda tangan elektronik tersebut telah tersertifikasi keasliannya dan terjamin kemanannya melalui suatu akses yang disebut *hardware security module* (HSM). Dengan sistem tersebut, jika ada pihak lain yang mencoba mengakses tanda tangan tersebut, yang mana tanda tangan telah diamankan oleh penyelenggara dikarenakan tanda tangan elektronik dijaga dengan menggunakan kombinasi *hardware, software* dan prosedur.

Uraian diatas mengemukakan esensi dokumen elektronik yang telah ditandatangani dengan menggunakan *digital signature*, setelah dikeluarkan Undang-Undang No.19 Tahun 2016 tentang Informasi dan Transaksi Elektronik atas perubahan terhadap Undang-Undang No.11 Tahun 2008, ketentuan lebih lanjut mengenai *digital signature*/tanda tangan elektronik juga diatur dalam PP No.71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik maka pengakuan dokumen elektronik yang ditandatangani dengan tanda tangan *digital signature* tersebut merupakan perluasan dari pembuktian hukum acara perdata di Indonesia, sehingga seluruh transaksi elektronik dengan tanda tangan elektronik dapat dianggap sebagai akta, dan kekuatan pembuktiannya sama dengan akta sepanjang dalam penyelenggaraannya *digital signature* merupakan tanda tangan elektronik tersertifikasi yang dibuat dan dikeluarkan oleh Badan Penyelenggara Sertifikat Elektronik (PSrE) yang telah memiliki lisensi oleh Kementrian Kominfo.

Oleh karena itu keabsahan suatu *digital signature*/tanda tangan elektronik ditentukan nilainya apakah tanda tangan elektronik tersebut tersertifikasi atau tidak tersertifikasi. Untuk itu, jika ada pihak yang menyangkal keabsahan suatu tanda tangan elektronik, hakim wajib mendengar keterangan dari lembaga penerbit sertifikat digital untuk mendapatkan keterangan sebagai ahli bahwa tanda tangan elektronik tersebut adalah valid dan diterbitkan oleh lembaga penerbit. Sedangkan jika tanda tangan elektronik yang tidak tersertifikasi, maka validitasnya disamakan dengan tanda tangan basah yang dibantah kebenarannya melalui labfor digital.

## B. Keabsahan *Digital Signature*/Tanda Tangan Elektronik Ditinjau Dalam Perspektif Hukum Perdata dan UU ITE

### 1. Peraturan Mengenai *Digital Signature*/Tanda Tangan Elektronik di Indonesia

*Digital signature* /Tanda tangan elektronik merupakan teknologi yang mulai populer digunakan di Indonesia . Teknologi ini memungkinkan *digital signature*/tanda tangan elektronik untuk dilakukan tanpa tatap muka dan juga tanpa dokumen fisik. Teknologi *digital signature*/tanda tangan elektronik dinilai merevolusi cara menyepakati kontrak menjadi lebih mudah, cepat dan efisien. Namun meski teknologi *digital signature*/tanda tangan elektronik dinilai memberikan banyak manfaat. Teknologi ini masih diliputi banyak keraguan. Salah satunya adalah apakah benar *digital signature*/tanda tangan elektronik bisa diakui secara sah di mata hukum yang berlaku di Indonesia.

Tanda tangan merupakan bagian dari kultur yang sangat mendasar dalam interaksi sebuah masyarakat. Tanda tangan menjadi penting karena tanda tangan merupakan sebuah bentuk dari perwakilan kesepakatan seseorang pada suatu hal. Penerapan tanda tangan sendiri memiliki empat tujuan utama yaitu sebagai alat bukti, tanda persetujuan, pemenuhan formalitas dan juga efisiensi. Itu sebabnya diperlukan adanya undang-undang yang mengatur tentang *digital signature*/tanda tangan elektronik.

Lebih lanjut tanda tangan menurut Tan Thong Kie dalam bukunya berfungsi sebagai suatu pernyataan kemauan pembuat tanda tangan (penandatanganan), bahwa ia menghendaki agar tulisan itu dalam hukum dianggap sebagai tulisannya sendiri (si pembuat tanda tangan), dengan membubuhkan tanda tangannya di bawah suatu tulisan. Pada pasal 1875 KUH Perdata memberikan pengaturan tentang tanda tangan seseorang, yang berbunyi:

“Suatu tulisan di bawah tangan yang diakui kebenarannya oleh orang yang dihadapkan kepadanya atau secara hukum dianggap telah dibenarkan olehnya, menimbulkan bukti lengkap seperti suatu akta otentik bagi mereka yang menandatangkannya, ahli warisnya serta orang-orang yang mendapatkan hak dari mereka ”.

Olehnya itu berdasarkan ketentuan 1875 KUH Perdata keabsahan suatu tanda tangan berasal dari adanya pengakuan dari orang yang membubuhkan tanda tangan tersebut. Sebagai sebuah inovasi baru dalam teknologi di Indonesia *digital signature*/tanda tangan elektronik kehadirannya telah diatur dalam peraturan perundang-undangan, yang mana diterbitkan sejak tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) kemudian di amandemen menjadi Undang-Undang No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik yang mengatur penggunaan *digital signature*/tanda tangan elektronik serta sertifikat elektronik.

Sejak berlakunya UU ITE pada tahun 2008 kemudian diubah menjadi UU No.19 Tahun 2016 merupakan pondasi cikal bakal penerapan teknologi *digital signature*/tanda tangan elektronik di Indonesia. Namun barulah pada tahun 2012 diterbitkan peraturan pemerintah yang kemudian di ubah menjadi PP No. 71 Tahun 2019 tentang Penyelenggaraan sistem dan transaksi elektronik yang menjadi dasar hukum bagi transaksi daring dan implementasi *digital signature*/tanda tangan elektronik di Indonesia.

Berdasarkan undang-undang dan peraturan pemerintah yang telah ada, *digital signature*/tanda tangan elektronik harus memiliki kemampuan teknologi pendukung yang menjamin terpenuhinya syarat-syarat yang telah ditetapkan. Yang mana fasilitas tersebut ialah harus memiliki atribut *digital signature*/tanda tangan elektronik dan kemampuannya dalam verifikasi.

Terkait dengan atribut *digital signature*/tanda tangan elektronik yang dimaksud adalah kemampuan otentifikasi yang menjamin keaslian *digital signature*/tanda tangan elektronik dan juga dokumen digital. Mengingat teknologi digital memungkinkan siapapun menyalin dan menggandakan dokumen maupun *digital signature*/tanda tangan elektronik itu sendiri. Itu sebabnya aspek otentikasi *digital signature*/tanda tangan elektronik menjadi penting.

Dimana ada dua aspek yang harus dipenuhi *digital signature*/tanda tangan elektronik :

1. Otentikasi pemilik *digital signature*/tanda tangan elektronik. Artinya tanda tangan elektronik benar-benar dimiliki oleh penandatangan yang tercantum pada dokumen digital
2. Otentikasi dokumen. Dokumen digital juga harus dibuktikan otentik bahwa usai ditandatangani, dokumen tetap sesuai aslinya sehingga dokumen tidak bisa dipalsukan.

Olehnya itu dengan di sahkannya Undang-Undang No.19 Tahun 2016 tentang Perubahan atas Undang-Undang No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik serta PP No.71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, *digital signature*/ tanda tangan elektronik dapat dianggap sah dimata hukum dan memiliki payung hukum.

Dalam perkembangannya Undang-Undang No.71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik Pasal 60 ayat (2) membagi kedalam setidaknya dua jenis *digital signature*/tanda tangan elektronik yaitu (a) tanda tangan elektronik tersertifikasi, yang harus memenuhi keabsahan kekuatan hukum dan akibat hukum tanda tangan elektronik sebagaimana dimaksud dalam Pasal 59 ayat (3); menggunakan sertifikat elektronik yang dibuat oleh jasa penyelenggara Sertifikat Elektronik Indonesia; dan dibuat dengan menggunakan perangkat pembuat tanda tangan elektronik tersertifikasi; (b) tanda tangan elektronik tidak tersertifikasi, yang dibuat tanpa menggunakan jasa penyelenggara sertifikat elektronik.

Lebih lanjut diatur dalam PP No. 80 Tahun 2019 tentang Perdagangan melalui Sistem Elektronik Pasal 49 ayat 3 menyebutkan “ bukti transaksi yang menggunakan tanda tangan elektronik tersertifikasi atau berinduk dapat dianggap sebagai bukti tertulis yang autentik ”. Khusus untuk *digital signature*/tanda tangan elektronik tersertifikasi ini, harus dilakukan oleh Penyelenggara Sertifikat Elektronik Indonesia (PSrE Indonesia) yang telah mendapatkan pengakuan dan telah lulus audit yang mengacu kepada standar yang diterbitkan oleh Kementerian Komunikasi dan Informatika (Kominfo) sesuai dengan Pasal 1 angka 5 Permenkominfo No.11 Tahun 2018 tentang Penyelenggaraan Sertifikasi Elektronik disebutkan jika penyelenggara sertifikat elektronik adalah badan hukum yang berfungsi sebagai pihak yang layak dipercaya, yang memberikan dan mengaudit sertifikat elektronik.

Tersertifikasi dalam *digital signature*/tanda tangan elektronik yang dibuat menggunakan sertifikat elektronik yang diterbitkan oleh PSre Indonesia. Dalam UU

ITE menjabarkan sertifikat elektronik merupakan sertifikat yang bersifat elektronik yang memuat *digital signature*/tanda tangan elektronik dan identitas yang menunjukkan status subjek hukum para pihak dalam transaksi elektronik yang dikeluarkan oleh PSrE Indonesia. Singkatnya, sertifikat elektronik berbentuk file yang dapat membuktikan identitas seseorang dan mampu memvalidasi tanda tangan elektronik, sehingga informasi yang ditandatangani dengan tanda tangan elektronik terjamin dari segi autentitas, integritas dan nirsangkal.

*Digital signature*/tanda tangan elektronik tersertifikasi yang menggunakan sertifikat elektronik memberikan tiga jaminan kepercayaan bagi pemilik yakni berupa autentisitas data, dengan menunjukkan identitas pemilik sertifikat dalam dokumen elektronik, keutuhan agar aktivitas dalam dokumen elektronik yang telah ditandatangani dapat dipantau, serta menjamin adanya nirsangkal, yakni pembuktian kebenaran sehingga penandatanganan tidak bisa menyangkal telah melakukan transaksi elektronik.

Adapun perbedaan mendasar *digital signature*/tanda tangan elektronik yang tersertifikasi dan tidak tersertifikasi terletak pada keabsahan data dan kepastian hukum, yang mana keabsahan data dan kepastian hukum hanya dimiliki oleh melalui badan penyelenggara sertifikat elektronik (PSre) yang telah memiliki lisensi dari pemerintah dalam hal ini Kementerian Komunikasi dan Informatika (KOMINFO). Saat ini di Indonesia setidaknya ada 9 penyelenggara sertifikasi elektronik yang diakui oleh Kementerian Kominfo : (a) PT *Privy Identitas Digital* (PrivyID) ; (b) PT *Indonesia Digital Identity* (VIDA); (c) PT *Djelas Tanda Tangan Bersama*; (d) PT *Tilaka Nusa Teknologi*; (e) PT *Digital Tanda Tangan Asli*; (f) *Perusahaan Umum Percetakan Uang Republik Indonesia* (PERURI); (g) *PT Solusi Net Internusa (Solusi Net)*; (h) *Badan Riset dan Inovasi Nasional* (BRIN); (i) *Balai Sertifikasi Elektronik Badan Siber dan Sandi Negara*.

*Digital Signature*/Tanda Tangan Elektronik yang tersertifikasi ini berdasarkan UU ITE dikatakan sah dimata hukum ketika telah memenuhi beberapa persyaratan yaitu:

1. Data pembuatan tanda tangan elektronik terkait hanya kepada penandatanganan;
2. Data pembuatan tanda tangan elektronik pada saat proses penandatanganan elektronik hanya berada dalam kuasa penandatanganan
3. Segala perubahan terhadap tanda tangan elektronik yang terjadi setelah waktu penandatanganan dapat diketahui
4. Segala perubahan terhadap informasi elektronik yang terkait dengan tanda tangan elektronik tersebut setelah waktu penandatanganan dapat diketahui.
5. Terdapat cara tertentu yang dipakai untuk mengidentifikasi siapa penandatanggannya;
6. Terdapat cara tertentu untuk menunjukkan bahwa penandatanganan telah memberikan persetujuan terhadap informasi elektronik yang terkait.

Selanjutnya adalah terkait dengan kemampuan verifikasi *digital signature*/tanda tangan elektronik. Verifikasi dibutuhkan untuk membuktikan bahwa tanda tangan elektronik yang dicantumkan pada dokumen digital memang benar tanda tangan yang otentik. Kemampuan verifikasi ini penting untuk menjamin *digital signature*/tanda tangan elektronik tidak dipalsukan atau digunakan oleh pihak selain pemilik tanda tangan.

## 2. Mekanisme Atribut Tata Cara Kerja *Digital Signature*/Tanda Tangan Elektronik

*Digital signature*/tanda tangan elektronik membutuhkan sebuah pembuktian identitas yang membuktikan seseorang adalah orang yang benar. Oleh karena itu terdapat fungsi *hash algoritma kriptografi* yang menciptakan tanda tangan elektronik yang unik. Dengan *hash, digital signature*/tanda tangan elektronik akan bisa menyimpan data data pribadi seperti rekam biometrik tanpa bisa disalin oleh pihak lain. Informasi ini hanya bisa diakses dengan menggunakan perangkat token atau sistem verifikasi identitas seperti pindai biometrik yang kemudian akan memberikan kuasa seseorang untuk melakukan tanda tangan.

Kemampuan-kemampuan teknologi menyangkut tanda tangan elektronik seluruhnya harus dimiliki oleh pihak Penyelenggara Sertifikat Elektronik atau PSrE. Pihak PSrE kemudian akan mendapatkan sertifikasi regulator dalam hal ini pemerintah melalui Kementerian Komunikasi dan Informatika untuk bisa menerbitkan sertifikat elektronik untuk *digital signature*/tanda tangan elektronik yang tersertifikasi.

Mengenai tata cara pembuatan *digital signature*/tanda tangan elektronik pemohon harus mendaftarkan diri melalui jasa (PSrE) Indonesia yang telah mendapatkan pengakuan dari Kementerian Kominfo untuk menerbitkan sertifikasi elektronik. Sertifikat elektronik merupakan sertifikat elektronik yang berbentuk elektronik yang kemudian memuat tanda tangan elektronik dan identitas subjek hukum para pihak dalam transaksi elektronik yang dikeluarkan oleh PSrE Indonesia.

*Digital signature*/tanda tangan elektronik dan identitas subjek hukum para pihak dalam transaksi elektronik yang dikeluarkan oleh PSrE Indonesia seperti yang telah dikemukakan sebelumnya. Selain itu Kementerian Kominfo menjabarkan ada tiga tahapan yang harus dilalui pemohon untuk mendapatkan sertifikat elektronik pada *digital signature*/tanda tangan elektronik tersertifikasi.

### 1. Tahap Pengajuan

Pemohon mendaftarkan diri ke PSrE Indonesia dengan ketentuan yang telah dimiliki oleh masing-masing PSrE Indonesia. Syarat tersebut dapat diakses di laman PSrE dan bagi pendaftar dengan profesi Aparatur Sipil Negara (ASN) diwajibkan mendaftar pada PSrE Pemerintah.

### 2. Tahap Verifikasi

PSrE Indonesia akan melakukan verifikasi data pemohon pendaftar, data kependudukan pemohon seperti NIK, nama, tanggal lahir, foto, data biometrik (sidik jari) dibandingkan dengan basis data kementerian yang berwenang mengelola data kependudukan. Apabila data tersebut valid dan benar maka akan dilanjutkan proses penerbitan.

### 3. Tahap Penerbitan

Bagi pemohon yang telah lolos verifikasi, pemohon akan disediakan *account* untuk mengunduh sertifikat elektronik yang telah diterbitkan oleh PSrE Indonesia. *Account* ini sekaligus untuk mengelola layanan *digital signature*/tanda tangan elektronik tersertifikasi, segel elektronik tersertifikasi yang dapat digunakan sebagai pengganti stempel perusahaan, dan layanan lainnya. Setelah memiliki sertifikat elektronik, pemilik dapat langsung menandatangani dokumen elektronik kapanpun dan dimanapun. Pemilik dapat menandatangani dokumen elektronik di berbagai

platform, seperti bisnis digital global, e-banking, layanan pinjam meminjam (peer to peer lending), perjanjian dan lain-lain.

Fitur keamanan yang digunakan dalam *digital signature*/tanda tangan elektronik memastikan bahwa dokumen tidak diubah dan *digital signature*/tanda tangan elektronik tersebut dapat berlaku sah meliputi>

1. PIN, sandi dan kode

Digunakan untuk mengautentifikasi dan memverifikasi identitas penerima dan menyetujui tanda tangan mereka. Email, nama pengguna dan kata sandi adalah yang paling umum.

2. Cap waktu (*Time stamping*)

Memberikan tanggal dan waktu tanda tangan, *time stamping* berguna ketika waktu pada saat melakukan tanda tangan seperti perdagangan saham, penerbitan tiket lotere dan proses hukum.

3. Kriptografi asimetris

Menggunakan algoritma kunci publik yang mencakup enkripsi/otentikasi kunci privat dan publik.

4. *Checksum*

Rangkaian panjang huruf dan angka yang mewakili digit yang benar dalam sebuah data digital, yang dapat digunakan untuk perbandingan untuk mendeteksi kesalahan atau perubahan. *Checksum* bertindak sebagai sidik jari data.

5. *Cyclic redundancy checking (CRC)*

Kode pendeteksi kesalahan dan fitur verifikasi yang digunakan dalam jaringan digital dan perangkat penyimpanan untuk mendeteksi perubahan pada data mentah.

6. Validasi otoritas sertifikat atau *certificate authority (CA)*

CA mengeluarkan tanda tangan elektronik dan bertindak sebagai pihak ketiga terpercaya dengan menerima, mengautentifikasi, menerbitkan, dan memelihara sertifikat digital. Penggunaan CA membantu menghindari pembuatan sertifikat digital palsu.

7. Valisasi *trust service provider (TSP)*

TSP adalah orang atau badan hukum yang melakukan validasi tanda tangan digital atas nama perusahaan dan menawarkan laporan validasi tanda tangan.

Berangkat dari uraian diatas sejatinya kehadiran *digital signature*/tanda tangan elektronik berawal dari adanya sebuah kesepakatan antara kedua belah pihak yang kemudian mengadakan perjanjian, olehnya itu kita berkiblat dengan Kitab-Kitab Undang-Undang Hukum Perdata Pasal 1320 KUH Perdata juga menyebutkan syarat sah dari sebuah perjanjian harus memiliki beberapa unsur yakni :

1. Adanya kata sepakat bagi mereka yang mengikatkan dirinya;
2. Kecapakan para pihak untuk membuat suatu perikatan;
3. Suatu hal tertentu;
4. Suatu sebab (*causa*) yang halal

Perjanjian harus didasarkan pada konsensus atau kesepakatan dari para pihak-pihak yang membuat perjanjian. Dengan asas konsensualisme, perjanjian dikatakan telah lahir jika ada kata sepakat atau persesuaian kehendak diantara para pihak yang membuat perjanjian tersebut. Tidak ada kata sepakat, tidak ada kontrak (*no consent no contract*).

*Digital signature* dalam sebuah perjanjian yang berdasarkan asas konsensualisme, perjanjian lahir sejak tercapainya kesepakatan dan dalam ketentuan Pasal 1338 ayat (1) KUH Perdata dinyatakan bahwa “ semua perjanjian yang dibuat secara sah berlaku sebagai undang-undang bagi yang membuatnya”. Dari rumusan ketentuan Pasal tersebut, maka perjanjian berlaku sebagai undang-undang jika telah memenuhi syarat sahnya perjanjian.

Asas konsensuil yang menyatakan bahwa suatu perjanjian telah lahir sejak tercapainya kata sepakat, untuk mencapai kesepakatan harus ada pernyataan kehendak. Olehnya itu sepanjang perjanjian tersebut diakui oleh para pihak yang melakukan *digital signature/* tanda tangan elektroik maka perjanjian tersebut sah namun apabila salah satu pihak menyangkal maka pihak terus harus membuktikannya.

Berdasarkan ketentuan Pasal 1338 ayat (1) KUH Perdata yang menyatakan bahwa “ Semua perjanjian yang dibuat secara sah berlaku sebagai undang-undang bagi mereka yang membuatnya”. Dengan demikian perjanjian yang didalamnya termuat *digital signature/* tanda tangan elektronik tetaplah mengikat selama tidak ada pengingkaran dari pihak yang melakukan perjanjian tersebut. Dengan itu untuk menilai keabsahan suatu perjanjian yang didalamnya termuat *digital signature/*tanda tangan elektronik maka untuk menganalisa keabsahannya adalah berangkat dari ketentuan Pasal 1320 dan Pasal 1338 Kitab Undang-Undang Hukum Perdata tersebut dan Undang Undang No.11 Tahun 2008 jo Undang-Undang No.19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik serta PP NO.71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

## KESIMPULAN

1. *Digital signature* sendiri merupakan suatu pembaharuan dalam sistem hukum positif perdata di Indonesia khususnya dalam hukum pembuktian. Kekuatan pembuktian dari dokumen elektronik yang didalamnya melekat suatu *digital signature/*tanda tangan elektronik di dalam hukum pembuktian di Indonesia, diakui esensinya setelah diatur di dalam UU ITE bahwa informasi elektronik/dokumen elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah dan merupakan perluasan dari alat bukti yang sah sesuai dengan hukum acara yang berlaku di Indonesia.
2. Keabsahan suatu *digital signature* dapat dilihat tentang tata cara pelaksanaannya yang menggunakan teknik *krypthography* dimana *digital signature* tersebut harus memuat informasi-informasi penggunaannya agar lebih aman untuk digunakan dan dalam Pasal 60 ayat (2) PP No 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik terdapat klasifikasi mengenai *digital signature* serta disebutkan pula dalam UU ITE Pasal 11 ayat (1) bahwa *digital signature* memiliki akibat hukum yang sah jika memenuhi 6 (enam) syarat pun juga bertumpu pada KUH Perdata dan Pasal 1320 dalam ketentuannya tidak mensyaratkan bentuk

dan jenis media yang digunakan dalam bertransaksi. Jadi *digital signature* sendiri pada dasarnya dikembalikan dalam KUH Perdata tetap berlaku sah dan mengikat karena dengan adanya perikatan tersebut merupakan undang undang bagi mereka yang membuatnya sebagaimana disebutkan dalam Pasal 1338 KUH Perdata.

## SARAN

1. Olehnya itu seiring dengan tuntutan kebutuhan masyarakat pencari keadilan dalam era perkembangan teknologi informasi dan telekomunikasi dewasa ini, perlu adanya suatu perubahan dalam sistem pembuktian kita saat ini. Dalam arti proses pembuktian di pengadilan tidak terikat pada alat bukti yang ditentukan dalam undang-undang secara terbatas, karenanya dalam undang-undang acara perdata yang akan datang hendaknya alat bukti diatur dalam dalam Kitab Undang-Undang KUHPerdata yang mengikuti perkembangan teknologi modern dewasa ini.
2. Dengan perkembangan zaman yang sudah semakin maju hendaknya pemerintah dalam hal ini sebagai *stakeholder* memfasilitasi infrastruktur dan SDM yang baik dan mendukung perkembangan yang dapat memudahkan implementasi *digital signature*/tanda tangan elektronik khususnya di Indonesia.

## DAFTAR PUSTAKA

- Agustino, L. (2020). Analisis Kebijakan Penanganan Wabah Covid-19: Pengalaman Indonesia. *Jurnal Borneo Administrator*, 16(2), 253-270.
- Ersya, M. P. (2017). Permasalahan Hukum dalam Menanggulangi Cyber Crime di Indonesia. *Journal of Moral and Civic Education*, 1(1), 50-62.
- Hassanah, H. (2016). Analisis Hukum Tentang Perbuatan Melawan Hukum Dalam Transaksi Bisnis Secara Online (E-Commerce) Berdasarkan Burgerlijke Wetboek Dan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. *Jurnal Wawasan Yuridika*, 32(1), 38-51.
- Hudzaifah, H. (2015). Keabsahan Tanda Tangan Elektronik Dalam Pembuktian Hukum Acara Perdata Indonesia. *Katalogis*, 3(5), 194-204.
- Letsoin, F. X. V. R. (2010). Pengakuan tandatangan pada dokumen elektronik dalam pembuktian hukum acara perdata di Indonesia. *SASI*, 16(3), 52-60.
- Makarim, E. (2015). Keautentikan Dokumen Publik Elektronik Dalam Administrasi Pemerintahan Dan Pelayanan Publik. *Jurnal Hukum & Pembangunan*, 45(4), 508-570.
- Rahmatullah, T. (2017). Analisis Permasalahan Hukum E-Commerce dan Pengaturannya di Indonesia. *Jurnal Hukum Media Justitia Nusantara*, 7(2), 10-23.
- Slamet, T. S., & Paliling, M. M. (2019). Kekuatan Hukum Transaksi Dan Tanda Tangan Elektronik Dalam Perjanjian. *Paulus Law Journal*, 1(1), 9-18.
- Sumadi, H. (2016). Kendala dalam menanggulangi tindak pidana penipuan transaksi elektronik di Indonesia. *Jurnal Wawasan Yuridika*, 33(2), 175-203.
- Suwignyo, H. (2009). Keabsahan Cap Jempol sebagai Pengganti Tanda Tangan dalam Pembuatan Akta Otentik. *Notarius*, 1(1), 63-74.

Watie, E. D. S. (2016). Komunikasi dan media sosial (communications and social media). *Jurnal The Messenger*, 3(2), 69-74.

.

.