Sibatik Journal
Jurnal Ilmiah Bidang Sosial, Ekonomi, Budaya, Teknologi, dan Pendidikan
E-ISSN: 2809-8544

PERBANDINGAN PERATURAN TANDA TANGAN DIGITAL DI NEGARA JEPANG DAN NEGARA INDONESIA (STUDI PUTUSAN: NOMOR 61/PID/2017/PT YYK)

COMPARISON OF DIGITAL SIGNATURE REGULATIONS IN JAPAN AND INDONESIA (STUDY DECISION: NUMBER 61/PID/2017/PT YYK)

Meisya Millenia[1], Kartina Pakpahan[2], Sri Sulistyawaty[3]
Universitas Prima Indonesia
Email: meisyamillenia20@gmail.com

Abstract

Digital signatures are a substitute for manual signatures that are electronic and have the same function as manual signatures. However, the development of digital signatures has not yet been realized in the world of notarial services, especially in the creation of authentic deeds by notaries. This research uses a Normative Juridical approach. Data was collected through literature research and using qualitative and descriptive analysis. Conclusions from this research, the implementation of electronic digital signatures has been implemented in a number of authentic deeds, but not all are allowed to use digital signatures, some are required to still use hanko or signaturesin the form of stamps made of wood. However, in Indonesia the implementation of digital signatures is still unclear, which is why currently digital signatures have been implemented, however, their use is only in documents in the form of personal identity such as Resident Identification Cards, Driving Licenses, etc and Legal sanctions for criminal acts of misuse of digital signatures in Indonesia include forgery of documents which can be charged under Article 263 paragraph (1) of the Criminal Code. The perpetrator is threatened with imprisonment for six years. In Japan, the crime of misuse of digital signatures is regulated in the Cybercrime Law which was passed in 2011 and the Act on Electronic Signatures and Certification Business Act No. 102. However, the penalties that may be applied depend on various factors, including the severity of the offense, the harm caused. The government's efforts to prevent the misuse of criminal acts of digital signature falsification are by strengthening the digital certification security system, conducting regular audits on services that use digital signatures, implementing effective reporting and following up on cases by providing strict sanctions to provide a deterrent effect at the perpetrator.

Keywords: *Digital Signature, Authentic, Crime, Abuse*

Abstrak

Tanda tangan digital adalah pengganti tanda tangan secara manual yang bersifat elektronik dan mempunyai fungsi sama dengan tanda tangan manual. Namun perkembangan tanda tangan digital ini masih belum dapat terealisasi dalam dunia kenotariatan khususnya dalam pembuatan akta oleh notaris yang sifatnya autentik. Penelitian ini menggunakan pendekatan Yuridis Normatif. Data dikumpulkan melalui penelitian literatur serta menggunakan analisis kualitatif dan deskriptif. Kesimpulan dari penelitian ini, Pelaksanaan tanda tangan digital elektronik telah terlaksana dalam sejumlah pembuatan akta otentik namun tidak semua diperbolehkan untuk menggunakan tanda tangan digital beberapa diharuskan untuk masih menggunakan *hanko* ataupun tanda tangan berbentuk stempel yang terbuat dari kayu. Namun di Indonesia pelaksanaan tanda tangan digital masih abu- abu, karena itulah saat ini tanda tangan digital sudah terlaksana namun, kegunaannya hanya dalam dokumen yang berbentuk identitas pribadi seperti, Kartu Tanda Penduduk, Surat Izin Mengemudi, dll dan Sanksi hukum bagi tindak pidana pennyalahgunaan tanda tangan digital di Indonesia masuk kedalam bentuk pemalsuan surat yang dapat dijerat dengan Pasal 263 ayat (1) KUHP. Pelakunya diancam dengan pidana penjara selama enam tahun. Di negara Jepang, tindak pidana penyalahgunaan tanda tangan digital diatur dalam *Cybercrime Law* yang disahkan pada tahun 2011 dan *Act on Electronic Signatures and Certification Business Act No. 102*. Namun hukuman yang mungkin diterapkan tergantung pada berbagai faktor, termasuk tingkat pelanggaran, kerugian

Meisya Millenia[1], Kartina Pakpahan[2], Sri Sulistyawaty[3]
DOI: https://doi.org/10.54443/sibatik.v2i12.1515

yang diitimbulkan. Upaya pencegahan yang dilakukan pemerintah terhadap terjadinya penyalahgunaan tindak pidana pemalsuan tanda tangan digital adalah dengan mempererat sistem keamanan sertifikasi digital, melakukan audit secara berkala pada layanan yang menggunakan tanda tangan digital, menerapkan pelaporan yang efektif serta menindaklanjuti kasus dengan memberi sanksi yang tegas agar memberi efek jera pada pelaku.

Kata Kunci: Tanda Tangan Digital, Autentik, Tindak Pidana, Penyalahgunaan

PENDAHULUAN

Era rovolusi 4.0 merupakan sebuah era dimana dunia sedang mengalami transformasi menuju era masyarakat transformasi. Sebab itu, negara kita negara Indonesia dituntut untuk mampu mengikuti perkembangan jaman yang ada agar tidak ketinggalan dan mampu menyesuaikan perkembangan tersebut agar tidak masuk kedalam jurang *digital divide.* Karena inilah, banyak pimpinan menginstruksikan kepada seluruh kementrian dan lembaga serta pemerintah daerah untuk mampu ikut serta dalam memanfaatkan segala teknologi informasi dan komunikasi dalam sistem manajemen. Teknologi informasi berkembangan dengan sangat pesat yang menyebabkan seluruh masyarakat mampu mengakses informasi dan data apapun yang diinginkan dalam hitungan detik. Terlebih lagi dalam konteks komunikasi sudah tidak ada hambatan apapun, dikarenakan siapapun mampu berkomunikasi dengan siapapun tanpa mediasi. (Anggel F. Kresna, 2019)

Perkembangan ini pun akhirnya melahirkan sebuah peraturan Undang-undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang- undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Dinamika perubahan kehidupan manusia telah banyak dibangun menggunakan elektronik atau biasa disebut *online* dimana dalam dunia hukum kenotariatan juga telah memperbarui sistem kebijakan mengenai pendaftaran hukum perusahaan melalui *online.* Namun dalam menjalankan tugas dan wewenang notaris dalam membuat akta otentik, masih belum dapat terealisasi secara *online*. Dikarenakan hal ini masih belum diatursecara keseluruhan dalam peraturan Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik serta juga terdapat kendala dalam peraturan Undang-Undang Jabatan Notaris No 2 tahun 2014 terkait pembuatan akta yang mengharuskan hadirnya saksi-saksi. (Rahmoda Erliyani dan Siti Rosydah, 2020) Namun seiring perkembangan jaman, salah satu bentuk transformasi yang dilakukan adalah penerapan tanda tangan secara digital ataupun elektronik dalam dokumen. Yang dimana hal ini telah diterapkan oleh pemerintah dalam pelaksanaannya dokumen berbentuk identitas pribadi.

Penggunaan tanda tangan elektronik tidak berjalan sebagaimana yang diharapkan karena menghadapi berbagai kendala dan rintangan. Selain tidak mudahnya merubah kebiasaan menggunakan tanda tangan manual, juga adanya ketakutan akan legalitas tanda tangan elektronik maupun keamanan tanda tangan elektronik dari pemalsuan. Namun di beberapa negara maju, perkembangan dunia kenotariatan telah berkembang dengan sangat pesat yang kemudian membawa sebuah gejolak perkembangan baru yang dimana dalam menjalankan kewajiban dan wewenang seorang notaris, ia telah difasilitasi dengan membuat akta secara elektronik. Hal ini biasa kita kenal dengan sebutan *Cyber Notary* ataupun

Meisya Millenia[1], Kartina Pakpahan[2], Sri Sulistyawaty[3]
DOI: https://doi.org/10.54443/sibatik.v2i12.1515

Electric Notary. Dimana konsep ini memiliki pengertian bahwa notaris mampu memanfaatkan kemajuan teknologi dalam membuat akta otentik dalam dunia maya tanpa mengharuskan adanya pertemuan, segala proses pelaksanaan pembuatan akta dilakukan dengan media *online*. Perkembangan ini memicu negara Indonesia untuk mengikuti perkembangan-perkembangan dari negara maju. Terlebih lagi mengamati negara-negara yang menganut sistem *Civil Law* dan sistem *Common Law* bahwa banyak negara yang telah menerapkan sistem *Cyber Notary* ini.

Tidak hanya negara yang menganut sistem *Common Law* seperti Inggris dan Amerika, namun juga negara yang menganut *Civil Law* seperti negara Belanda, Belgia maupun negara Jepang pun telah menerapkan konsep *Cyber Notary*. Negara jepang salah satunya telah mulai mengembangkan konsep ini sejak tahun 2000. (Nippon Koshonin 2023) Negara Jepang juga mengeluarkan Undang-Undang tambahan mengenai otentikasi elektronik untuk perusahaan (K. Yamamoto 2002). Berkembangnya*Cyber Notary* di negara Jepang menunjukkan bahwa hukum harus berkembang mengikuti perkembangan jaman. Penulis membandingkan dengan negara Jepang dikarenakan negara Jepang juga sama dengan negara Indonesia yang merupakan bekas jajahan negara Belanda, serta Indonesia juga ketika hendak melakukan penelitian terkait hal ini, melakukan studi banding ke negara Jepang. Maka berdasarkan uraian latar belakang diatas, penulis mengkaji permasalahan tersebut dalam tugas akhir ini yang berjudul: Perbandingan Peraturan Tanda Tangan Digital di Negara Jepang Dan Negara Indonesia (STUDI PUTUSAN: 61/PID/2017/PT YYK).

TINJAUAN PUSTAKA

Kerangka teori yang digunakan adalah Teori Hukum Perbandingan dan Teori *Good Governance*. Teori tersebut akan digunakan sebagai pisau analisa dalam pembahasan untuk menjawab rumusan masalah yang ada dalam penelitian.

1. Teori Hukum Perbandingan: Teori ini membahas perbandingan sistem hukum antar negara dan fokus pada perbandingan aturan, struktur hukum, dan prinsip hukum yang diterapkan dalam suatu sistem hukum. (Ratno Lukito, 2019)
2. Teori *Good Governance*: *Good governance* merupakan tata kelola yang baik pada suatu usaha yang dilandasi oleh etika profesional dalam berusaha atau berkarya. *Good governance* seringkali diartikan kepemerintah yang baik. *Good Governance* adalah suatu konsep dalam penyelenggaraan manajemen pembangunan yang solid dan bertanggung jawab sejalan dengan demokrasi dan pasar yang efisien, penghindaran salah alokasi dan investasi yang langka dan pencegahan korupsi baik secara politik maupun administratif, menjalankan disiplin anggaran serta penciptaan legal framework bagi tumbuhnya aktivitas kewiraswastaan. (Richard. H Hall, 2002)

METODE

Jenis Penelitian pada penelitian ini adalah jenis penelitian Antropologis Komparatif, Jenis penelitian ini bertujuan untuk memahami dan membandingkan bagaimana hukum diterapkan dan dipahami dalam budaya dan masyarakat yang berbeda di beberapa negara. Jenis data yang akan digunakan *adalah Electronic Signature and Certification Business Act*

Meisya Millenia[1], Kartina Pakpahan[2], Sri Sulistyawaty[3]
DOI: https://doi.org/10.54443/sibatik.v2i12.1515

tahun 2000 (Jepang), Kitab Undang- Undang Hukum Pidana, Peraturan Pemerintah (Pp) Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem DanTransaksi Elektronik, dan Undang-Undang Informasi dan Transaksi Elektronik sebagai data primer penulis untuk meninjau perbandingan peraturan tanda tangan digital negara Jepang dan negara Indonesia Teknik atau metode perolehan data yang digunakan adalah Yuridis Normatif merupakan studi tentang Undang- Undang dan regulasi yang mengatur penggunaan tanda tangan digital di kedua negara, serta perbedaan dalam kebijakan dan praktik penerapan tanda tangan digital di sektor publik dan swasta. Jenis Pendekatan yang digunakan Kualitatif yaitu kegiatan menganalisis data yang diperoleh dan kemudian disusun dan dirumuskan jawaban pada permasalahan dalam penelitian.

HASIL DAN PEMBAHASAN

Pelaksanaan Peraturan Tanda Tangan Digital di Negara Indonesia dan Negara Jepang

Tanda tangan digital atau elektronik menurut Pasal 1 angka 12 Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU 19/2016) istilah tersebut didefinisikan sebagai berikut:

*"*Tanda Tangan Elektronik adalah *tanda tangan yang terdiri atas Informasi Elektronik* yang dilekatkan, terasosiasi atau terkait dengan Informasi Elektronik lainnya yang digunakan sebagai alat verifikasi dan autentikasi. (Khairil Mahpuz, 2020)

Klasifikasi Jenis tanda tangan elektronik:

a. Tanda tangan elektronik tersertifikasi, yang harus memenuhi persyaratan:
   1. Memenuhi keabsahan kekuatan hukum dan akibat hukum tanda tangan elektronik sebagaimana dimaksud dalam Pasal 59 ayat (3) PP PSTE.
   2. Menggunakan sertifikat elektronik yang dibuat oleh jasa penyelenggara sertifikasi elektronik Indonesia dimana nantinya, penyelenggara sertifikasi elektronik akan membuat tanda tangan digital bersistem kriptografi asimetris (*Asymmetric Cryptography*) dengan menggunakan *Public Key Infrastructure* atau PKI. DalamPKI tersebut, ada yang dinamakan kunci publik (*Public Key*) dan kunci privat (*Private Key*). Kunci privat dibuat secara unik untuk masing-masing individu. Kunci privat ini memiliki pasangan kunci yang terkait secara matematis yang disebut dengan kunci publik. Kunci publik kemudian dilekatkan pada sertifikat elektronik bersama dengan dokumen elektronik yang telah dienkripsi dengan menggunakan kunci privat tersebut. dan;
   3. Dibuat melalui perangkat pembuat tanda tangan elektronik tersertifikasi.
b. Tanda tangan elektronik tidak tersertifikasi, yang dibuat tanpa menggunakan jasa penyelenggara sertifikasi elektronik. Contoh tanda tangan elektronik tidak tersertifikasi adalah tanda tangan yang kita lakukan secara konvensional di kertas kemudian di-*scan.* Tanda tangan elektronik tidak tersertifikasi ini juga lebih mudah untuk ditiru, karena sama sekali tidak melalui proses perangkat khusus dan juga tidak adanya terlibat keterlibatan jasa penyelenggara sertifikasi elektronik. Karena alasan inilah nilai pembuktian nya

Meisya Millenia[1], Kartina Pakpahan[2], Sri Sulistyawaty[3]
DOI: https://doi.org/10.54443/sibatik.v2i12.1515

relatif lebih rendah dibandingkan tanda tanganelektronik tersertifikasi.

Tanda tangan elektronik memiliki fungsi kedudukan yang sama dengan tanda tangan manual ataupun biasa disebut tanda tangan basah sesuai Pasal 52 Ayat 1 yang menerangkan bahwa:

1. Peraturan Pemerintah Penyelenggara Sertifikat Transaksi Elektronik yaitu sebagai alat autentikasi dan verifikasi atas:
2. identitas Penanda Tangan; dan
3. keutuhan dan keautentikan Informasi Elektronik.

Pada umumnya, tanda tangan elektronik ini dilaksanakandalam dokumen yang berbentuk elektronik ataupun transaksi elektronik. Yang dimana pelaksanaannya berbasis digital yang medianya berupa elektronik. Sesuai Pasal 11 Undang-Undang(UU) Nomor 19 Tahun 2016 tentang Perubahan Atas Undang- Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.

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 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 siapapenanda tangannya; dan
f. Terdapat cara tertentu untuk menunjukkan bahwa penanda tangan telah memberikan persetujuan terhadap informasi elektronikyang terkait.

Penandatanganan yang dilakukan seseorang melalui bentuk elektronik, sah secara hukum dan dapat diakui pembuktiannya selama ia memenuhi syarat diatas. Dengan bersedia bertandatangan, artinya seseorang menjamin atas apa yang telah tertera dan dapat dipertanggungjawabkan secara hukum atas kebenarannya. Yang dimana artinya kedudukan tanda tangan elektronik dan tanda tangan basah adalah sama, dimana keduanya memiliki kekuatan dan akibat hukum. Tanda tangan setiap orang tentunya akan berbeda karena hal ini merupakan bentuk paraf dari identitas diri, sama halnya dengan dalam bentuk elektronik tentunya walau ada yang memiliki kemiripan tentu saja akan ada goresan yang berbeda. (Mochamad Januar Rizki , 2023)

Kedua negara Indonesia dan negara Jepang mengakui tanda tangan digital sebagai alat yang sah dalam menandatangani dokumen elektronik. Di negara jepang sendiri, tanda tangan juga basah dikenal juga dengan "*Inkan"* ataupun "*Hanko".* Dimana *hanko* sendiri bentuknya berupa stempel yang berbentuk lingkaran yang bahan pembuatannya merupakan kayu, karet ataupun batu. Penggunaan ini dilakukan untuk menandatangani dokumen yang berbentuk resmi, sertakontrak dan lainnya. Berikut jenis-jenis *Hanko* yang berlaku di jepang: (Iqbal Anshori, 2022)

Meisya Millenia[1], Kartina Pakpahan[2], Sri Sulistyawaty[3]
DOI: https://doi.org/10.54443/sibatik.v2i12.1515

1. *Jitsu In*

   Stempel ini merupakan stempel yang tersertifikasi dan resmi bentuknya karena dapat dipertanggungjawabkan dan telah terdaftar di lembaga pemerintahan. Contoh penggunaan stempel ini digunakan dalam transaksi jual beli rumah, kontrak yang mengikat secara hukum. Dimana *Hanko Jitsu In* ini ada kartu khususnya sebagai bukti legalitas dari pemilik.
2. *Ginko Shirushi*

   Stempel ini bentuknya tulisan nama, dimana contoh fungsi penggunaan ini adalah pembukaan pada rekening bank. Namunsetelah rekening bank telah selesai dibuat, maka akan diwajibkan untuk verifikasi terutama jika adanya transaksi tarikan berbentuk tunai.
3. *Mitome-In*

   Merupakan jenis hanko yang digunakan untuk kepentinganformal, contohnya untuk pengiriman/ penerimaan barang, surat-menyurat, dan pembayaran tagihan.
4. *Gago-In*

   Dimana jenis hanko ini biasa digunakan untuk tanda hakpencipta, seperti lukisan atau ukiran.

Negara jepang menggunakan sistem yang sama dengan negara Indonesia yaitu *Public Key Infranstructure* guna untuk mengidentifikasi keamanan pribadi untuk pertukaran informasi. Dimana biasa warga menyebut sebagai *My Number System* dimana setiap warga jepang diberikan nomor identifikasi unik. PKI telah digunakan untuk berbagai sektor seperti perbankan dan transaksi keuangan guna menjamin kepastian transaksi dan informasi pribadi, pelayanan pemerintah untuk pengajuan pajak online, aplikasi kartu kesehatan dan beberapa layanan publik, dan yang terakhir untuk sertifikasi tanda tangan digital. Dikarenakan tanda tangan digital sangat sering dilakukan untuk memenuhi berbagai proses bisnis dan pemerintahan. PKI memungkinkan pembuatan sertifikat tanda tangan digital yang memastikan otentikasi dan integritas dokumen digital. Dalam teori ini, pemilik tanda tangan diharuskan untuk mengamankan kunci privat mereka sendiri. Di negara Jepang sendiri, tanda tangan digital merupakan hal yang masih belum benar-benar diterapkan, penggunaannya juga masih terbatas bahwa tidak semua bisa digunakan tanda tangan secara digital. Berikut akta notaris yang tidak boleh menggunakan tanda tangan digital di Jepang karena masih memerlukan tanda tangan dan cap jari secara langsung, antara lain:

Tabel 1. Perbandingan Jenis Akta Notaris Yang Memperbolehkan Penggunaan Tanda Tangan Digital Dan Akta Notaris Yang Mengharuskan Stempel Cap Jari Secara Langsung

No.	Akta Notaris Yang Memperbolehkan Penggunaan TandaTangan Digital	Akta Notaris Yang Mengharuskan Stempel/Cap Jari Secara Langsung
1.	Akta Jual Beli Tanah	Akta PendirianPerusahaan
2.	Akta Waris	Akta Perubahan Anggaran DasarPerusahaan

Meisya Millenia[1], Kartina Pakpahan[2], Sri Sulistyawaty[3]
DOI: https://doi.org/10.54443/sibatik.v2i12.1515

3.	Perjanjian KerjaSama	Akta Pendirian Yayasan
4.	Akta Kuasa	Akta Perubahan Anggaran Dasar Yayasan
5.	-	Akta PembukaanWarisan

Di Jepang, penggunaan tanda tangan digital telah diatur oleh Undang-Undang Tanda Tangan Elektronik dan memiliki persyaratan yang harus dipenuhi untuk diakui secara sah. Namun masih adapula beberapa dokumen yang diharuskan untuk menggunakan *hanko* dalam penandatangannya. Berikut jenis dokumen yang diperbolehkan untuk menggunakan *hanko* dan dokumen yang menggunakan tanda tangan digital:

Tabel 2. Perbandingan Dokumen Yang Menggunakan *Hanko* Dan Dokumen Yang Menggunakan Tanda Tangan Digital

No.	Dokumen Yang Menggunakan *Hanko*	Dokumen Yang Menggunakan Tanda Tangan Digital
1.	Dokumen pemerintah, seperti kartu identitas, paspor, dan izin tinggal	Akta Notaris (tertentu)
2.	Kontrak, seperti kontrak sewa dan kontrak kerja	Kontrak(tertentu)
3.	Dokumen perbankan, seperti formulir pembukaan rekening bank	Laporan keuangan(tertentu)
4.	Dokumen perpajakan, sepertiformulir pajak dansurat pemberitahuan pajak	Faktur dan dokumenkeuangan lainnya
5.	Dokumen legal, seperti sertifikat kelahiran, sertifikat kematian, dan akta pernikahan	Izin dan sertifikasi

Tanda tangan digital dan hanko adalah dua bentuk penandatanganan dokumen yang berbeda di Jepang. Berikut adalah beberapa perbedaan antara tandatangan digital dan *Hanko* di Jepang:

Tabel 3. Perbandingan Perbedaan *Hanko* dan Tanda Tangan Digital

No.	*Hanko*	Tanda Tangan Digital
1.	Fisik *hanko* berbentuk stempel fisik	Berbentuk dokumen elektronik

Meisya Millenia[1], Kartina Pakpahan[2], Sri Sulistyawaty[3]
DOI: https://doi.org/10.54443/sibatik.v2i12.1515

2.	Keamanan hanko sulit dipalsukan namuntidak menutup kemungkinan	Keamanan tanda tangan digital dianggap lebih aman karena memiliki fitur keamanan seperti sertifikat digital dan enkripsi yang memastikan keaslian danintegritas dokumen
3.	Biaya pembuatan *hanko* lebih murah	Biaya untuk membuat tanda tangan digital lebih mahal dikarenakan, seseorang harus memiliki sertifikat digital yang dikeluarkan oleh pihak yang berwenang, seperti badan sertifikasi digital
4.	Lebih tidak efisien	Lebih efisien karena bisa dilakukan dimanapun dan kapanpun.
5.	Telah melekat dalam budaya dan tradisi	Tidak semua masyarakat mengggunakan, karena masih tergolong baru.

Sanksi Hukum Bagi Tindak Pidana Terhadap Penyalahgunaan Tanda Tangan Digital di Negara Indonesia dan Negara Jepang

Penggunaan tanda tangan elektronik, mendorong terwujudnya tertib hukum (legal order) dalam rangka melindungi kepentingan kepada masyarakat sehingga mampu mengurangi adanya kemungkinan indikasi pemalsuan tanda tangan yang kemudian menimmbulkan kerugian. Dengan demikian dapat terpenuhi efisiensi, kepastian hukum, kemanfaatan dan keadilan dan penggunaan tanda tangan elektronik dan dapat mendukung adanya kepastian hukum untuk kemanfaatan dan keadilan karena sifatnya yang sulit dipalsukan dan memiliki kekuatan hukum tetap yang telah diatur oleh undang-undang. Namun, selain memberi begitu banyaknya dampak positif dikehidupan masyarakat, tanda tangan digital walau sulit untuk dipalsukan tetap saja tidak dapat dipungkiri juga akan ada oknum-oknum tidak bertanggung jawab yang akan terus mencari celah dalam melakukan pemalsuan. Karena penyalahgunaan teknologi memiliki medianya yang ruangnya tidak terbatas, atau bisa dikatakan penggunanya tidak mengenal usia dari kalangan muda hingga yang tua.

Aturan hukum pun dibuat untuk menanggulangi hal tersebut. Tindak pidana penipuan berbasis digital ini pada prinisipnya sama dengan pemalsuan tanda tangan basah pada umumnya namun yang menjadi letak perbedaan adalah pada alat bukti atau sarana perbuatannya yakni menggunakan perangkat elektronik (komputer, internet, perangkat telekomunikasi/*gadget*). (Tony Yuri Rahmanto, 2019) Oleh karenanya penegakan hukum mengenai tindak pemalsuan tanda tangan elektronik ini masih dapat diakomodir oleh Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang- Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Walau sebenarnya penggunaan tanda tangan elektronik diharapkan dapat mengurangi adanya penyalahgunaan. Namun

Meisya Millenia[1], Kartina Pakpahan[2], Sri Sulistyawaty[3]
DOI: https://doi.org/10.54443/sibatik.v2i12.1515

sebenarnya penggunaan tanda tangan elektronik di Indonesia masih sangat minim digunakan.

Pemalsuan tanda tangan masuk dalam bentuk pemalsuan surat yang dapat dijerat dengan Pasal 263 ayat (1) KUHP. Pelakunya diancam dengan pidana penjara selama enam tahun. Lebih jelasnya, Pasal 263 ayat (1) KUHP menyatakan bahwa barangsiapa membuat surat palsu atau memalsukan surat, yang dapat menerbitkan sesuatu hak, sesuatu perjanjian (kewajiban) atau sesuatu pembebasan utang, atau yang boleh dipergunakan sebagai keterangan bagi sesuatu perbuatan, dengan maksud akan menggunakan atau menyuruh orang lain menggunakan surat-surat ituseolah-olah surat itu asli dan tidak dipalsukan, maka kalau mempergunakannya dapat mendatangkan sesuatu kerugian dihukum karena pemalsuan surat, dengan hukuman penjara selama-lamanya enam tahun. studi putusan nomor 61/PID/2017/PT YYK hasil penelitian menunjukkan bahwa terdakwa telah melakukan tindak pidana pemalsuan tanda tangan masuk dalam bentuk pemalsuan surat yang dapat dijerat dengan Pasal 263 ayat (1) KUHP dimana kemudian menghukum terdakwa untuk membayar biaya perkara peradilan

Di negara Jepang, tindak pidana penyalahgunaan tanda tangan digital diatur dalam Undang-Undang Tindak Pidana Komputer (*Cybercrime Law*) yang disahkan pada tahun 2011 dan juga pada Undang-undang tentang Tanda TanganElektronik dan Undang-Undang Bisnis Sertifikasi (*Act on Electronic Signaturesand Certification Business Act No. 102)*. Tindakan kejahatan seperti pemalsuan atau manipulasi tanda tangan digital, penggunaan tanda tangan digital tanpa otorisasi, atau pemalsuan sertifikat digital dapat dikenakan sanksi pidana, termasuk hukuman penjara atau denda. Dalam kedua negara tersebut, tindakan kejahatan terhadap tanda tangan digital dianggap serius dan dapat dikenakan sanksi pidana. Oleh karena itu, penting untuk memperhatikan keamanan dan integritas tanda tangan digital, serta memastikan bahwa penggunaannya sesuai dengan peraturan dan persyaratan yang berlaku.

Article 42

Any person who falls under either of the following items is punished by imprisonment with work for not more than one (1) year or a fine of not more than 1,000,000 yen:

(i) a person who violates the provisions of paragraph 2 of Article 13 (The accredited certification business operator may place on an electronic certificate, etc. (*paragraph 2 of article 13 which was electronic or magnetic record prepared for certifying that matters used to confirm that the user has performed the electronic signature are pertaining to the relevant user, and others provided by order of the competent ministry; the same applies in the following paragraph*), amark to the effect that the relevant business has obtained the accreditation, pursuant to the provisions of order of the competent ministry.

(ii) Except for cases prescribed in the preceding paragraph, no person must placethe mark set forth in the preceding paragraph or any mark that can be confused with this mark, on any electronic certificate, et).

Terjemahan:
Pasal 42

Meisya Millenia[1], Kartina Pakpahan[2], Sri Sulistyawaty[3]
DOI: https://doi.org/10.54443/sibatik.v2i12.1515

Barang siapa termasuk salah satu dari yang berikut ini diancam dengan pidana penjara dengan masa kerja paling lama 1 (satu) tahun atau denda paling banyak 1.000.000 yen:

*(i) seseorang yang melanggar ketentuan ayat 2 Pasal 13 (Pelaksana usaha sertifikasi yang terakreditasi dapat membubuhkan pada sertifikat elektronik, dll. (*isi paragraf 2 pasal 13 yang merupakan catatan elektronikatau magnetik yang disiapkan untuk menyatakan hal-hal yang digunakan untuk mengkonfirmasi bahwa pengguna telah melakukan tanda tanganelektronik yang berkaitan dengan pengguna yang relevan, dan lain-lain yang diberikan atas perintah kementerian yang berwenang; hal yang sama berlaku dalam paragraf berikut*), tanda yang menyatakan bahwa bisnis yang bersangkutan telah memperoleh akreditasi, sesuai dengan ketentuan tata tertib kementerian yang berwenang.*

(ii) Kecuali untuk kasus-kasus yang ditentukan dalam paragraf sebelumnya, tidak seorang pun boleh membubuhkan merek yang disebutkan dalam paragraf sebelumnya atau merek apa pun yang dapat dikacaukan dengan merek ini, pada sertifikat elektronik apa pun, dan lain- lain).

Upaya Pencegahan Pemerintah Terhadap Terjadinya Tindak Pidana Penyalahgunaan TandaTangan Digital

Pemerintah sering kali mengambil langkah-langkah untukmencegah penyalahgunaan atau pelaksanaan tanda tangan digital secara tidak sah. Langkah-langkah ini bertujuan untuk menjaga keamanan, integritas, dan validitas dari proses tanda tangan digital serta untuk meminimalkan risiko potensial seperti pemalsuan atau penipuan. Beberapa upaya pencegahan yang umum dilakukan oleh pemerintah meliputi pencegahan yang dapat dilakukan pemerintah antara lain:

1. Undang-Undang dan Regulasi
   Dimana pemerintah dapat mengadopsi undang-undang dan regulasi yang mengatur penggunaan tanda tangan digital. Regulasi ini dapat menguraikan persyaratan yang harus dipenuhi untuk menjalankan tanda tangan digital yang sah, serta sanksi hukum bagi pelanggaran yang terkait dengan penyalahgunaan tanda tangan digital.
2. Sertifikasi Otoritas Tanda Tangan Digital
   Pemerintah bisa mendirikan atau mengakui otoritas sertifikasi tanda tangan digital yang dapat mengeluarkan sertifikat yang sah untuk entitas atau individu yang memenuhi syarat. Otoritas ini dapat melakukan verifikasi identitas dan keabsahan tanda tangan digital.
3. Pengawasan dan Audit
   Pemerintah dapat mengimplementasikan sistem pengawasan dan audit untuk memantau penggunaan tanda tangan digital. Ini bisa melibatkan pemeriksaan berkala dan verifikasi untuk memastikan bahwa tanda tangan digital digunakan sesuai dengan ketentuan yang berlaku dan kontrol internal untuk memantau dan mengidentifikasi kemungkinan adanya penyalahgunaan tanda tangan digital.
4. Pelatihan dan Edukasi
   Pemerintah dapat memberikan pelatihan dan edukasi kepada masyarakat dan sektor

Meisya Millenia[1], Kartina Pakpahan[2], Sri Sulistyawaty[3]
DOI: https://doi.org/10.54443/sibatik.v2i12.1515

bisnis tentang penggunaan yang benar dan aman dari tanda tangandigital. Ini dapat membantu meningkatkan kesadaran akan risiko dan praktik terbaik dalam penggunaan tanda tangan digital dan melakukan kampanye sosial.

5. Teknologi Keamanan
   Pemerintah dapat mendorong pengembangan dan penggunaan teknologi keamanan tinggi untuk melindungi tanda tangan digital dari penyalahgunaan. Ini mungkin termasuk penggunaan enkripsi, sertifikat digital, atau teknologi biometrik untuk memastikan identitas pemilik tanda tangan digital.
6. Kolaborasi Internasional
   Pemerintah dapat bekerja sama dengan negara-negara lain untuk mengembangkan standar internasional terkait dengan penggunaan tanda tangan digital dan mengatasi isu-isu keamanan lintas batas.
7. Penegakan Hukum
   Jika terjadi pelanggaran atau penyalahgunaan tanda tangan digital, pemerintah dapat menggunakan sistem peradilan untuk menegakkan hukum dan memberikan sanksi kepada pelaku yang melanggar.
8. Kebijakan Keamanan Informasi
   Membuat dan menerapkan kebijakan keamanan informasi yang memadai untuk memastikan keamanan tanda tangan digital dan dokumen digital lainnya.
9. Kepastian Penggunaan Sertifikasi Tanda Tangan Digital
   Memastikan bahwa sertifikat digital dan tanda tangan digital hanya digunakan oleh pihak yang berwenang, dengan memperkuat sistem otentikasi dan otorisasi.

Dengan menerapkan upaya-upaya di atas, diharapkan dapat mencegah terjadinya tindak pidana terhadap penyalahgunaan tanda tangan digital dan meningkatkan kepercayaan masyarakat pada teknologi tanda tangan digital sebagai alat yang aman dan sah untuk transaksi bisnis dan legal. Upaya pencegahan ini harus seimbang dengan kebutuhan untuk memfasilitasi transaksi elektronik yang efisien dan berkelanjutan. Keamanan dan integritas tanda tangan digital harus dijaga tanpa menghambat pertumbuhan dan inovasi dalam lingkungan digital.

PENUTUP

Kesimpulan

Studi putusan nomor 61/PID/2017/PT YYK hasil penelitian menunjukkan bahwa terdakwa telah melakukan tindak pidana pemalsuan tanda tangan masuk dalam bentuk pemalsuan surat yang dapat dijerat dengan Pasal 263 ayat (1) KUHP dimana kemudian menghukum terdakwa untuk membayar biaya perkara peradilanPada umumnya, tanda tangan elektronik ini dilaksanakan dalam dokumen yang berbentuk elektronik ataupun transaksi elektronik. Yang dimana pelaksanaannya berbasis digital yang medianya berupa elektronik. Sebuah penyedia layanan tanda tangan digital/elektronik menyatakan bahwa tanda tangan digital dibuat dengan sistem kriptografi asimetris (*Asymmetric Cryptography*) dengan menggunakan infrastruktur kunci publik (*Public Key Infrastructure*/PKI). Dalam PKI tersebut, ada yang dinamakan kunci publik (*Public Key*) dengan kunci privat (*privat*

Meisya Millenia[1], Kartina Pakpahan[2], Sri Sulistyawaty[3]
DOI: https://doi.org/10.54443/sibatik.v2i12.1515

key). Kunci privat, yang dibuat secara unik untuk masing-masing individu, memiliki pasangan kunci yang terkait secara matematis yang disebut dengan kunci publik. Pada tanda tangan elektronik, ada kombinasi fungsi hash dan enkripsi dengan metode asimetrik. Yang dimana fungsi hash adalah untuk menghasilkan nilai unik untuk setiap data yang dimasukkan. Nilai hash inilah yang di kriptografi menggunakan kunci privat yang kemudian nilai darihasil kriptografi tersebutlah nilai *signature* dari sebuah *file* tersebut Sebagaimana namanya, kunci privat hanya diketahui dan dikuasai oleh penanda tangan, sedangkan kunci publik bersifat informasi publik sebagai informasi yang digunakan untuk memvalidasi tanda tangan digital seseorang. Penyelenggara sertifikat elektronik terdiri atas penyelenggara sertifikasi elektronik Indonesia dan penyelenggara sertifikasi elektronik asing. Sistem juga akan memeriksa informasi terkait *hash value*, bila sama maka integritas dokumen terjamin, bila tidak sama maka berarti telah adanya perubahan setelah dokumen tersebut ditanda tangani. Perubahan tersebut dapat dilihat secara otomatis pada pembaca PDF menuturkan bahwa pembuatan tanda tangan digital membutuhkan kombinasipaling sedikit dua faktor autentikasi, sebagai pembuktian identitas penanda tangan secara elektronik. Hal ini untuk memastikan bahwa yang menandatangani dokumen adalah individu yang sama dengan yang identitasnya ada di dalam sertifikat elektronik

Bahwa di negara Indonesia pemalsuan tandatangan masuk dalam bentuk pemalsuan surat yang dapat dijerat dengan Pasal 263 ayat (1) KUHP. Pelakunya diancam dengan pidana penjara selama enam tahun. Lebih jelasnya, Pasal 263 ayat (1) KUHP menyatakan bahwa barangsiapa membuat surat palsu atau memalsukan surat, yang dapat menerbitkan sesuatu hak, sesuatu perjanjian (kewajiban) atau sesuatu pembebasan utang, atau yang boleh dipergunakan sebagai keterangan bagi sesuatu perbuatan, dengan maksud akan menggunakan atau menyuruh orang lain menggunakan surat-surat itu seolah-olah surat itu asli dan tidak dipalsukan, maka kalau mempergunakannya dapat mendatangkan sesuatu kerugian dihukum karena pemalsuan surat, dengan hukuman penjara selama-lamanya enam tahun. Di negara Jepang, tindak pidana penyalahgunaan tanda tangan digital diatur dalam Undang-Undang Tindak Pidana Komputer (*Cybercrime Law*) yang disahkan pada tahun 2011 dan juga pada Undang-undang tentang Tanda Tangan Elektronik dan Undang- Undang Bisnis Sertifikasi (*Act on Electronic Signatures and Certification Business Act No. 102)*. Tindakan kejahatan seperti pemalsuan atau manipulasi tanda tangan digital, penggunaan tanda tangan digital tanpa otorisasi, atau pemalsuan sertifikat digital dapat dikenakan sanksi pidana, termasuk hukuman penjara atau denda. Dalam kedua negara tersebut, tindakan kejahatan terhadap tanda tangan digital dianggap serius dan dapat dikenakan sanksi pidana. Oleh karena itu, penting untuk memperhatikan keamanan dan integritas tanda tangan digital, serta memastikan bahwa penggunaannya sesuai dengan peraturan dan persyaratan yang berlaku.

Beberapa upaya pencegahan yang dapat dilakukan pemerintah dalam pelaksanaan Pemalsuan tanda tangan digital antara lain dengan Mempererat peraturan yang mengatur terkait tanda tangan digital agar ada standar keamanan yang harus dipatuhi oleh penyedia layanan, Mengatur tentang sertifkasi digital yang diakui oleh lembaga pemerintah agar mampu mengautentifikassi identitas pemilik tanda tangan elektronik dan keaslian dokumen,

Meisya Millenia[1], Kartina Pakpahan[2], Sri Sulistyawaty[3]
DOI: https://doi.org/10.54443/sibatik.v2i12.1515

Mengatur tentang persyaratan tanda tangan elektronik seperti penggunaan metode otentikasi biometrik agar mengurangi resiko pemalsuan, Mengatur keamanan seperti enkripsi agar mampu melindungi integritas dokumen, Melakukan audit secara berkala pada layanan tanda tangan elektronik untuk memastikan standar keamanan, Memberikan pendidikan dan pelatihan kepada masyarakat agar masyarakat paham akan resiko dan upaya pencegahannya, Memiliki mekanisme pelaporan yang efektif serta menindaklanjuti kasus dengan memberi sanksi yang tegas agar memberi efek jera pada pelaku, Pemerintah bisa kolaborasi dengan sektor swasta agar mengembangkan solusi inovatif dalam pencegahan dan Pemerintah bisa memastikan bahwa seluruh proses penggunaan tanda tangan elektronik termasuk penerbitan sertifikat digital dan validasi tanda tangan, transparan dan dapat dipertanggung jawabkan.

DAFTAR PUSTAKA

Adams, D.: Volunteered geographic information: potential implications for participatory planning. Plan. Pract. Res. 28(4), 464–469 (2013)

Conroy, M.M., Evans-Cowley, J.: Informing and interacting: the use of e-government for citizen participation in planning. J. E-Gov. 1(3), 73–92 (2004)

Horelli, L., Wallin, S.: The future-making assessment approach as a tool for e-planning and community development: the case of ubiquitous Helsinki. In: Silva, C. (ed.) Handbook of Research on E-Planning: ICTs for Urban Development and Monitoring, pp. 58–79. IGI Global, Hershey (2010)

Husnul Hudzaifah, "Keabsahan Tanda Tangan Elektronik Dalam Pembuktian Hukum Acara Perdata Indonesia", 2015, Universitas Tadulako,

K. Yamamoto, "National Report Japan, Notary in Tokyo", 2002, Dalam "Jurnal Notarius International 1-2,

Mohamad Aunurrohim, Keadilan, Kepastian Dan Kemanan Hukum Di Indonesia, 2015, Universitas Negeri Yogjakarta

Rahmida Erliyani Dan Siti Rosydah Hamdan, Akta Notaris Dalam Pembuktian Perkara Perdata & Perkembangan Cyber Notary, Yogyakarta: Dialektika, Juli 2020

Rizki Dermawan, "Pemanfaatan Tanda Tangan Digital Tersertifikasi Di Era Pandemi", 2021, Fakultas Syariah Institut Agama Islam Negeri (IAIN) Kediri

Roman, A.V.: Delineating three dimensions of e-government success: security, functionality and transformation. In: Information Resources Management Association (ed.) Public Affairs and Administration: Concepts, Methodologies, Tools, and Applications, pp. 135–157. IGI Global, Hershey (2015). doi:10.4018/978-1-4666-8358-7.ch007

Santos, B. (2017). E-Government, e-Governance and Urban Planning: Towards a Complete Digital Planning Process. In: Kő, A., Francesconi, E. (eds) Electronic Government and the Information Systems Perspective. EGOVIS 2017. Lecture Notes in Computer Science (), vol 10441. Springer, Cham. https://doi.org/10.1007/978-3-319-64248-2_4

Sulaiman, E., Arifudin, N. ., & Triyana, L. (2021). Kekuatan Hukum Digital Signature Sebagai Alat Bukti Yang Sah Di Tinjau Dari Hukum Acara Perdata. Risalah Hukum, 16(2), 95–105. https://doi.org/10.30872/risalah.v16i2.207

Thamaroni Usman, "Keabsahan Tanda Tangan Elektronik Pada Perjanjian Jual Beli Barang

Dari Perspektif Hukum Perdata", 2020, Universitas Lampung,

Tony Yuri Rahmanto, Penegakan Hukum terhadap Tindak Pidana Penipuan Berbasis Transaksi Elektronik, 2018, Pusat Penelitian dan Pengembangan Hak Asasi Manusia Badan Penelitian dan Pengembangan Hukum dan HAM