p-ISSN : 0215-3092
e- ISSN : 2443-0013

PERSPEKTIF HUKUM SIBER DI INDONESIA: PENANGANAN KASUS CYBER TERHADAP TANDA TANGAN ELEKTRONIK

Aas Rohmat[1], Ismiyanto[2], Muhammad Muhtarom [3],
[1]Magister Hukum Universitas Islam Batik Surakarta
email: aasrohmat@gmail.com

A B S T R A K

In the era of globalization, society 5.0 technology, followed by the development of information technology in cyber space, is something that cannot be avoided. This is followed by the vulnerability of threats and attacks on data and information traffic that can threaten state sovereignty. The security factor is the main obstacle in line with the increasing level of crime in cyberspace in Indonesia. The purpose of this study is the Perspective of Cyber Law in Indonesia: Handling Cyber Cases Against Electronic Signatures. The research method used in this research is descriptive. The type of research that the author uses is normative legal research or known as doctrinal legal research which is commonly referred to as legal research or legal research instructions. This legal research examines library material obtained through literature review by collecting and studying primary and secondary legal materials in the form of laws and literature that are relevant to the research object. The approaches used in this legal research are statutory and contextual approaches. The analysis used is descriptive, namely to describe or explain the phenomenon under study. The analysis is carried out by linking causes and effects to the emergence of the phenomenon under study. The findings in this study are that the perspective of cyber law in Indonesia in handling cyber cases against data theft or threats related to electronic signatures is very important to be immediately normalized.

A R T I C L E I N F O

Article History:
Accepted 03 okt 2022
Available online 24 Des 2022

Kata kunci: ***Legal perspective, cyber law, handling, cyber cases, electronic signature***.

I. PENDAHULUAN

Di era globalisasi teknologi society 5.0 yang disertai dengan kemajuan ilmu pengetahuan yang semakin pesat dan teknologi keberadaan informasi memiliki arti dan peran penting dalam segala hal aspek kehidupan. Dalam masyarakat modern saat ini, informasi telah berfungsi seperti arus darah yang merupakan sumber kehidupan bagi tubuh manusia. Saat ini, banyak negara memiliki ketergantungan yang tinggi terhadap dunia maya dan internet, baik dalam bidang ekonomi, bisnis, sosial, aspek politik, pemerintahan, pertahanan, dan keamanan. Perkembangan *Information and Communication Technology-ICT* dapat ditandai dengan peningkatan penggunaan internet, meningkatnya penggunaan internet dapat memberikan dampak positif namun dampak negatif akibat kemajuan teknologi. *Cyberspace* adalah ruang di mana

p-ISSN : 0215-3092
e- ISSN : 2443-0013

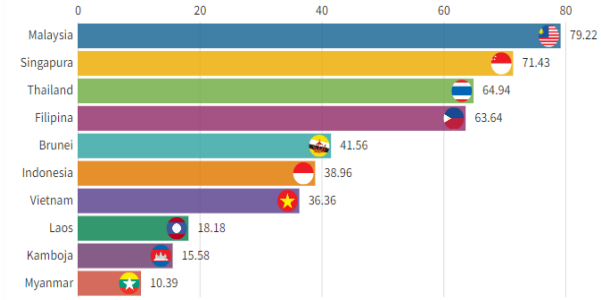
masyarakat terhubung menggunakan jaringan (misalnya internet) untuk melakukan berbagai aktivitas sehari-hari (Kementerian Pertahanan RI, 2014).

Peningkat konektivitas di dunia maya dan ketergantungan pada internet juga menjadi ancaman bagi negara kedaulatan dengan kemungkinan kejahatan transnasional berbasis dunia maya. Seiring dengan perkembangan zaman, kedaulatan dan ketahanan suatu negara tidak hanya itu dinilai dari seberapa besar kekuatan militer atau ekonomi yang dimilikinya, tetapi juga tergantung dari aspek-aspeknya penguasaan, penggunaan, dan pemberdayaan dunia maya.

Indonesia juga menghadapi tantangan global terkait keamanan dan ketahanan nasional di dunia maya. Tantangan ini dapat memiliki implikasi ancaman baru, misalnya berupa serangan siber, kejahatan siber, siber prostitusi, propaganda siber, terorisme siber hingga perang siber. Sifat dan karakteristik dunia maya yang *borderless, spaceless, dan timeless*, membuat *cybercrime* suatu bentuk kejahatan transnasional. Ancaman kejahatan dunia maya merupakan kondisi dan situasi apa pun serta kemampuan yang dianggap mampu melakukan tindakan atau gangguan atau serangan yang mampu merusak atau sesuatu yang merugikan sehingga mengancam kerahasiaan, integritas dan ketersediaan sistem dan informasi.

Sistem keamanan jaringan yang lemah, Seperti kita ketahui bahwa orang-orang dalam menggunakan fasilitas internet kebanyakan lebih mementingkan desain yang di milikinya dengan menyepelekan tingkat keamanannya. Sehingga dengan lemahnya sistem keamanan jaringan tersebut menjadi celah besar sebagian oknum untuk melakukan tindak kejahatan.

Berdasarkan fakta dilapangan bahwa kasus kebocoran data di atas menjadi salah satu pertanda keamanan siber Indonesia yang lemah. Menurut data Cyber Security Index dari NCSI (National Cyber Security Index) Indonesia berada pada posisi 83 dari 160 negara perihal keamanan siber. Indonesia mendapatkan skor 38,96 pada indeks keamanan siber dan skor 46,84 pada tingkat pengembangan digital. Berdasarkan sumber data NCSI (*National Cyber Security Index*) Tahun 2022. Indeks keamanan siber Negara ASEAN disajikan pada Gambar 1 sebagai berikut ini:



Gambar 1. Indeks keamanan siber Negara ASEAN ditahun 2022

Dalam lingkup kawasan Asia Tenggara, Indonesia berada di peringkat 6 dari 10 dalam indeks keamanan siber. Negara tetangga Malaysia berada di posisi pertama dengan skor 79,22. Negara tetangga lainnya, Singapura, berada di posisi kedua perihal keamanan siber dengan skor 71,43.

Kementerian Komunikasi dan Informatika (Kominfo) mencatat, penggunaan tanda tangan digital mengalami peningkatan 350 % selama pandemi Covid-19. Berdasarkan data Kominfo, ada lebih dari 2,58 juta sertifikat elektronik selama 2018-2022. Itu sudah termasuk pihak yang mengadopsi tanda tangan elektonik atau digital. Namun, ahli teknologi informasi (IT) menilai ada risiko pencurian data dengan beragam modus dalam aktivitas tanda tangan elektronik atau digital ini.

Tanda tangan elektronik adalah tanda tangan yang terdiri atas informasi elektronik yang dilekatkan, terasosiasi atau terkait dengan informasi elektronik lainnya yang digunakan berfungsi sebagai alat verifikasi dan autentifikasi identitas

p-ISSN : 0215-3092
e- ISSN : 2443-0013

penandatangganan sekaligus untuk menjamin keutuhan dan keautentikan dokumen. Tanda tangan elektronik mempresentasikan identitas penandatanganan yang diverifikasi berdasarkan data pembuatan tanda tangan elektronik dimana data pembuatan tanda tangan elektronik dibuat secara unik yang hanya merujuk kepada penandatanganan. Sama dengan tanda tangan manual, tanda tangan elektronik bersifat unik yakni tanda tangan elektronik seseorang akan berbeda dengan tanda tangan orang lain. Tanda tangan elektronik merupakan kombinasi dari fungsi hash dan enkripsi dengan metode asimetrik. Fungsi hash merupakan 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 dihasilkan akan berbeda. Nilai hash kemudian di enkripsi menggunakan private key untuk selanjutnya nilai dari hasil enkripsi tersebut adalah nilai signature dari suatu dokumen.

Aktivitas tanda tangan elektronik atau digital rentan terhadap pencurian data, karena menyimpan data berharga, seperti perjanjian kerja sama hingga persetujuan pinjaman. Itu kemudian yang menjadi target para pelaku kejahatan siber. Sering terjadi, pelaku kejahatan memperjual belikan data pribadi pengguna. ada sejumlah modus pencurian data layanan tanda tangan elektronik atau digital. Misalnya, pelaku memanfaatkan lengahnya sistem keamanan platform. Dalam proses permintaan dokumen pribadi, kalau tidak diawasi dengan ketat bisa jadi celah. Modus lainnya, pelaku melakukan peretasan terhadap sistem layanan tanda tangan elektronik atau digital. Tentunya akan ada modus lainnya, dan ini akan terus berkembang.

Hukum *cyber* berasal dari *cyberlaw*, yang saat ini secara internasional digunakan untuk istilah hukum yang terkait dengan pemanfaatan Teknologi Informasi. Istilah lain yang juga digunakan adalah Hukum Teknologi Informasi (*Law of Information Technology*), Hukum Dunia Maya (*Virtual World Law*) dan Hukum Mayantara. Secara akademis, *terminology cyber law* belum menjadi terminologi yang umum. Terminologi lain untuk tujuan yang sama seperti *The Law of The Internet, Law and the Information Superhighway, Information Technology Law, The Law of Information, Lex Informatica* dan sebagainya.

Di Indonesia sendiri tampaknya belum ada satu istilah yang disepakati. Istilah yang dimaksudkan sebagai terjemahan dari *cyber law*, misalnya, Hukum Sistem Informasi, Hukum Informasi, dan Hukum Telematika (Telekomunikasi dan Informatika). *Cyber Law* diperlukan karena kegiatan *Cyber* dengan berbasis internet saat ini tidak bisa dibatasi oleh teritori Negara dan dapat dilakukan kapanpun. Meskipun alat buktinya berbentuk virtual (maya) dan bersifat elektronik kegiatan *cyber* adalah kegiatan virtual yang berdampak nyata. Berdasarkan latar belakang diatas tersebut, maka peneliti melakukan penelitian dengan judul " Prespektif Hukum Siber di Indonesia: Penanganan Kasus Siber Terhadap Tanda Tangan Elektronik (Digital Signature)".

II. METODE PENELITIAN

Metode penelitian yang di gunakan dalam penelitian ini adalah diskriptif. Jenis penelitian yang penulis gunakan adalah penelitian hukum normatif atau dikenal dengan penelitian hukum doktrinal yang biasa disebut dengan hukum penelitian atau instruksi penelitian hukum. Penelitian hukum ini mengkaji literatur materi diperoleh melalui studi literatur dengan mengumpulkan dan mempelajari primer dan bahan hukum sekunder berupa peraturan perundang-undangan dan literatur yang relevan dengan obyeknya penelitian. Pendekatan yang digunakan dalam penelitian hukum ini adalah pendekatan undang-undang dan pendekatan konseptual. Pendekatan

p-ISSN : 0215-3092
e- ISSN : 2443-0013

undang-undang dilakukan dengan memeriksa semua undang-undang dan peraturan yang berkaitan dengan masalah hukum yang sedang dipelajari. Pendekatan konseptual adalah dilakukan dengan menganalisis dan menelaah Prespektif Hukum Siber Di Indonesia: Pengangan Kasus Cyber Terhadap Tanda Tangan Elektronik. Analisis yang digunakan adalah deskriptif, yaitu untukmenggambarkan atau menjelaskan fenomena yang diteliti. Analisis dilakukan dengan menghubungkan penyebab dan efek terhadap munculnya fenomena yang diteliti.

III. HASIL PENELITIAN DAN PEMBAHASAN

Kenyataannya kegiatan *cyber* tidak lagi sederhana, karena kegiatannya tidak lagi dibatasi oleh teritorial suatu negara, yang mudah diakses kapanpun dan dari manapun. Kerugian dapat terjadi, baik pada pelaku transaksi maupun pada orang lain yang tidak pernah melakukan transaksi. Di samping itu, pembuktian merupakan faktor yang sangat penting, mengingat informasi elektronik bukan saja belum terakomodasi dalam sistem hukum acara Indonesia secara komprehensif.

Tindak kejahatan *cyber* didunia maya disebabnya kurangnya perhatian masyarakat, Masyarakat dan penegak hukum saat ini masih memberi perhatian yang sangat besar terhadap kejahatan konvensional. Pada kenyataannya para pelaku kejahatan komputer masih terus melakukan aksi kejahatannya. Hal ini disebabkan karena rendahnya faktor pengetahuan tentang penggunaan internet yang lebih dalam pada masyarakat.

Dalam mengatasi rentannya pencurian data yang berharga, data pengguna juga sangat mudah untuk dipalsukan terkait penyalahgunaan tanda tangan elektronik yang menjadi target para pelaku kejahatan siber sehingga dampak yang diakibatkannya pun bisa demikian kompleks dan rumit. Perusahaan/Institusi/Lembaga terntu juga telah menerapkan sejumlah langkah-langkah mencegah risiko keamanan siber, dari layanan tanda tangan elektronik atau digital sesuai aturan yang berlaku. Misalnya, perusahaan/institusi/lembaga menerapkan otentikasi dan otorisasi secara digital. Selain itu, pihaknya juga memanfaatkan asuransi sertifikat elektronik digital harus terus berinovasi menerapkan *life detection*, seperti hasil foto dan video untuk verifikasi lebih otentik. Untuk itu, menyarankan agar penyelenggara layanan tanda tangan elektronik digital membuat sistem keamanan digital yang tersertifikasi. Hal itu termasuk pada peningkatan kompetensi dalam pengamanan data pribadi. Selain itu, perlu adanya pengawasan yang dilakukan regulator.

Tanda tangan elektronik atau digital menjadi opsi yang layak dengan kemampuan enkripsi yang dihasilkan oleh kriptografi asimetris. Enkripsi ini memberi setiap pengguna sepasang kunci, termasuk kunci enkripsi publik dan privat. Penggunaan tanda tangan elektronik atau digital memerlukan dua proses, yaitu tindakan-tindakan dari pihak penandatangan serta dari pihak penerima. Secara singkat kedua proses tersebut dapat dijelaskan sebagai berikut: pertama, pembentukan tanda tangan digital menggunakan nilai hash yang dihasilkan dari dokumen serta kunci privat yang telah didefinisikan sebelumnya. Kedua, verifikasi tanda tangan elektronika atau digital adalah proses pengecekan tanda tangan digital dengan mereferensikan ke dokumen asli dan kunci publik yang telah diberikan, dengan cara demikian dapat ditentukan apakah tanda tangan digital dibuat untuk dokumen yang sama menggunakan kunci privat yang berkorespondensi dengan kunci publik.

Tanda tangan elektronik/ digital merupakan alat untuk menjaga keaslian suatu dokumen yang dikirimkan dengan internet (dokumen elektronik).

p-ISSN : 0215-3092
e- ISSN : 2443-0013

Berdasarkan bunyi Pasal 1 angka (4) UUITE bahwa dokumen elektronik adalah setiap informasi elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektronmagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui komputer atau sistem elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, perta, rancangan , foto atau sejenisnya, huruf, tanda, angka, kode akses, simbol atau perdirasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya. Tahun 2022, kemungkinan juga akan terlihat peningkatan aktivitas di bidang perlindungan data. Negara cenderung menentukan ketentuan hukum untuk mempromosikan penyebab perlindungan data khususnya terkait kasus siber khususnya Tanda Tangan Elektronik.

Tanda tangan elektronik berfungsi sebagai alat autentikasi dan verifikasi atas identitas penanda tangan dan keutuhan dan keautentikan informasi elektronik. Persetujuan penandatangan terhadap informasi elektronik yang akan ditandatangani dengan tanda tangan elektronik harus menggunakan mekanisme afirmasi dan/atau mekanisme lain yang memperlihatkan maksud dan tujuan penandatangan untuk terikat dalam suatu transaksi elektronik. Jadi tanda tangan elektronik tersebut lazimnya dilakukan pada transaksi elektronik. Transaksi elektronik adalah perbuatan hukum yang dilakukan dengan menggunakan komputer, jaringan komputer, dan/atau media elektronik lainnya.

Mengenai keberadaan tanda tangan digital/elektronik di Indonesia, menurut Pasal 1 angka 12 Undang-Undang Nomor 19 Tahun 2016 (UU No.19/2016) tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, didefinisikan bahwa 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.

Tanda tangan elektronik meliputi:

1. Tanda Tangan Elektronik Tersertifikasi, harus memenuhi persyaratan:
   a) memenuhi keabsahan kekuatan hukum dan akibat hukum tanda tangan elektronik sebagaimana dimaksud dalam Pasal 59 ayat (3) PP PSTE;
   b) menggunakan sertifikat elektronik yang dibuat oleh jasa penyelenggara sertifikasi elektronik Indonesia, dan
   c) dibuat dengan menggunakan perangkat pembuat tanda tangan elektronik tersertifikasi.
2. Tanda Tangan Elektronik Tidak Tersertifikasi, dibuat tanpa menggunakan jasa penyelenggara sertifikasi elektronik.

Undang-undang Informasi dan Transaksi Elektronik (UU ITE) merupakan Hukum Siber Pertama Indonesia dan pembentukannya bertujuan untuk memberikan kepastian hukum bagi masyarakat yang melakukan transaksi secara elektronik, mendorong pertumbuhan ekonomi, mencegah terjadinya kejahatan berbasis teknologi informasi dan komunikasi serta melindungi masyarakat pengguna jasa yang memanfaatkan teknologi informasi dan komunikasi.

UU ITE terdiri dari 54 pasal yang terbagi dalam 13 Bab. Ketentuan-ketentuan yang mengatur kriminalisasi perbuatan yang termasuk kategori tindak pidana siber adalah Bab VII tentang perbuatan yang dilarang pasal 27-pasal 37. Sanksi pidana atas perbuatan-perbuatan tersebut dirumuskan dalam Bab XI tentang ketentuan pidana Pasal 45 -Pasal 52. Dalam perjalanannya, kriminalisasi tinak pidana siber dalam UU ITE yang mengatur penyalahgunaan teknologi informasi dan komunikasi dalam aktifitas di dunia siber belum memadai. Saat ini hukum

p-ISSN : 0215-3092
e- ISSN : 2443-0013

internasional yang banyak digunakan negara-negara di dunia sebagai pedoman dalam pengaturan tindak pidana siber adalah *Convention on Cybercrime 2001*.

Sehubungan dengan itu pemerintah Indonesia bermaksud untuk melakukan aksesi terhadap *Convention on Cybercrine 2001* dan melakukjan harmonisasi hukum nasional indonesia dengan *Convention on Cybercrime 2001*. Berdsaarkan Hasil kajian dan juga hasil *Workshop on Cybercrime Legislation in Indonesia* dengan *Council of Europe Expert*, ketentuan-ketenrtuan UU ITE belum sesuai dengan ketentuan tindak pidana siber dalam konvensi. Untuk itu pemerintah telah menyusun draf RUU Tindak Pidana Teknologi Informasi (RUU TIPITI) yang akan menhgatur beberapa terminologi dan norma-norma dalam konvensi yang belum sesuai atau belum diatur dalam UU ITE. RUU TIPITI yang terdiri dari 10 Bab dan 27 pasal merumuskan beberapa pengertian baru yang dirumuskan adalah sistem komputer, data komputer dan data trafik. Perbuatan-perbuatan yang dikriminalisasi dalam dalam RUU TIPITI pada dasarnya mengatur 5 jenis tindak pidana yaitu : penipuan, pelanggaran hak cipta dan hak-hak terkait, menghambat atau mengahalangi proses peradilan, pembantuan dan penghasutan serta pelanggaran kewajiban oleh penyelenggara sistem.

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (UU ITE). Undang-Undang ITE merupakan ketentuan yang mengatur bagi setiap orang yang melakukan perbuatan hukum serta memiliki akibat hukum dan merugikan kepentingan negara Indonesia, baik setiap orang yang berada di wilayah hukum negara Indonesia maupun yang berada di luar wilayah hukum Indonesia. Berikut diuraikan pengertiannya dalam UU ITE :

a. Informasi Elektronik
   Undang-undang Informasi dan Transaksi Elektronik (UU ITE) merupakan Hukum Siber Pertama Indonesia dan pembentukannya bertujuan untuk memberikan kepastian hukum bagi masyarakat yang melakukan transaksi secara elektronik, mendorong pertumbuhan ekonomi, mencegah terjadinya kejahatan berbasis teknologi informasi dan komunikasi serta melindungi masyarakat pengguna jasa yang memanfaatkan teknologi informasi dan komunikasi.

Beberapa materi perbuatan yang dilarang (*cybercrimes*) yang diatur dalam UU ITE, antara lain meliputi:

a) Perbuatan yang dikriminalisasi dalam pasal 27 meliputi dengan sengaja dan tanpa hak mendistribusikan, mentransmisikan atau membuat informasi elektronik dan/atau dokumen elektronik yang memiliki muatan yang melanggar kesusilaan dapat diakses, memiliki muatan perudian dapat diakses, memiliki muatan penghinaan dan/atau pencemaran nama baik dapat diakses, memiliki muatan pemerasan atau pengancaman dapat diakses.
b) Pasal 28 Perbuatan yang dikriminalisasi dalam pasal 28 meliputi perbuatan yang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik dan dengan sengaja dan tanpa hak menyebarkan informasi untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyaraat tertentu berdasarkan SARA.
c) Perbuatan yang dikriminalsisasi dalam pasal 29 adalah dengan sengaja serta tanpa hak mengirimkan informasi elektronik dan/atau dokumen elektronik yang didalamnya memuat ancaman berupa kekerasan atau menakuti

p-ISSN : 0215-3092
e- ISSN : 2443-0013

yang ditujukan kepada pribadi atau seseorang.

d) Perbuatan yang dikriminaslisasi dalam pasal 30 meliputi, dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer atau sistem elektronik milik orang lain dengan cara apapun dengan tujuan untuk memperoleh informasi elektronik atau dokumen eektronik, dan dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.
e) Perbuatan yang dikriminalisasi dalam pasal 31 meliputi, yaitu dengan sengaja dan tanpa hak atau melawan hukum yanh melakukan penyadapan atas informasi elektronik dan/atau dokumen elektronik dalam suatu komputer atau sistem elektronik tertentu milik orang lain dan dengan melakukan penyadapan suatu transmisi informasi elektronik atau dokumen elektronik yang tidak bersifat publik dari, ke dan didalam suatu komputer atau sistem elektronik tertentu milik orang lain, baik yang tiak menyebabkan perubahan, penghilangan, atau penghentian informasi elektronik atau dokumen elektronik yang sedang di transmisikan.
f) Perbuatan yang dikriminalisasi dalam pasal 32 sengaja dan tanpa hak atau melawan hukum dengan cara apapunmengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan, suatu informasi elektronik atau dokumen elektronik milik orang lain atau milik publik dan yang tidak berhak.
g) Perbuatan yang dikriminalisasi dalam pasal 33 adalah dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apapun yang berakibat terganggunya sistem elektroni atau mengakibatkan sistem elektronik menjadi tidak bekerja sebagaimana mestinya.
h) Perbuatan yang dikriminalisasi dalam pasal 34 adalah dengan sengaja dan tanpa hak atau melawan hukum memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan, atau meniliki, Perangkat keras atau perangkat lunak komputer yang dirancang atau secara khusu dikembangkan untuk memfasilitasi perbuatan sebagaiman dimaksud dalam pasal 27 sampai dengan pasal 33, Sandi lewat komputer, kode akses, atau hal yang sejenis dengan itu yang ditujukan agar sistem elektronik menjadi dapat diakses dengan tujuan memfasilitasi perbuatan sebagaimana dimaksud dalam pasal 27 sampai dengan pasal 33.
i) Perbuatan yang dikriminalisasi dalam pasal 35 adalah dengan sengaja dan tanpa hak atau melawan hukum, melakukan manipulasi, penciptaan, perubahan, penghilangan, pengeruskan informasi elektronik atau dokumen elektronik dengan tujuan agar informasi elektronik atau dokumen elektronik tersbut dianggap seolah-olah data yang otentik.
j) Perbuatan yang dikriminalisasi dalam pasal 36 adalah dengan senagaja dan tanpa haka tau melawan hukum perbuatan sebagaimana dimaksud dalam Pasal 27 s/d Pasal 34 yang dapat mengakibtkan kerugian bagi orang lain.
k) Ketentuan pasal 37 tidak mengatur perbuatan yang dilarang tetapi mengatur mengenai yurisdiksi atas perbuatan yang dilakuakn di luar wilayah Indonesian terhadap sasaran atau objek yang ada di

wilayah indonesia.

Berdasarkan rumusan perbuatan yang dikriminalisasi sebagai tindak pidana siber dalam UU ITE terdapat unsur delik yang dirumuskan, yaitu unsur dengan sengaja dan tanpa hak. Dalam beberapa pasal unsur tanpa hak dirumuskan alternatif dengan melawan hukum, yaitu Pasal 30 sampai dengan Pasal 36. Penggunaan kata dengan sengaja mengandung arti bahwa tindak pidana Siber sebagaimana diatur dalam UU ITE diancam dengan pidana apabila dilakukan dengan sengaja. Perbuatan yang dilakukan dengan kelalaian atau kebetulan bukan merupakan tindak pidana dan tidak diancam dengan pidana

V. KESIMPULAN DAN SARAN

Kesimpulan dalam penelitian ini adalah prespektif hukum siber di indonesia: penanganan kasus siber terhadap tanda tangan elektronik. Perusahaan/Institusi/Lembaga terntu juga telah menerapkan sejumlah langkah-langkah mencegah risiko keamanan siber, dari layanan tanda tangan elektronik atau digital sesuai aturan yang berlaku. Untuk itu, menyarankan agar penyelenggara layanan tanda tangan elektronik digital membuat sistem keamanan digital yang tersertifikasi. Hal itu termasuk pada peningkatan kompetensi dalam pengamanan data pribadi. Selain itu, perlu adanya pengawasan yang dilakukan regulator. Cybersecurity menjadi salah satu tren yang menjadi fokus memperkuat dan melindungi setiap negara. Implementasi Cybersecurity di Indonesia masih tersebar berbagai lembaga atau pemangku kepentingan yang masing-masing memiliki pedoman tata kelola. Bermacam-macam peraturan perundang-undangan yang ada, nyatanya tidak mampu mengakomodir dan menjangkau permasalahan yang ada di dunia maya. Karena itu, diperlukan undang-undang khusus untuk mengaturnya. Undang-undang Informasi dan Transaksi Elektronik (UU ITE) merupakan Hukum Siber Pertama Indonesia dan pembentukannya bertujuan untuk memberikan kepastian hukum bagi masyarakat yang melakukan transaksi secara elektronik, mendorong pertumbuhan ekonomi, mencegah terjadinya kejahatan berbasis teknologi informasi dan komunikasi serta melindungi masyarakat pengguna jasa yang memanfaatkan teknologi informasi dan komunikasi khususnya terkait tanda tangan elektonik.

Keamanan serta ketahanan dalam penanganan kasus siber yaitu menciptakan manajemen keamanan siber yang terintegrasi. Pemerintah Indonesia harus memberlakukan regulasi Cybersecurity dan ketahanan dalam regulasi tertentu. Pengaturan ini merupakan respon untuk mencegah dan menangkal ancaman dan serangan Cyber di masa depan untuk menciptakan perlindungan suatu Negara.

.

DAFTAR PUSTAKA

[1] Adejoke O Oyewunmi, (2012), ‘The ICT Revolution and Commercial Sectors in Nigeria:

Impacts and Legal Intervention', British Journal of Arts and Social Sciences, Vol. 5, No. 2. Council of Europe Convention on Cybercrime 2001.

Anthony J. Diana & David G. Krone, Electronic Signatures : Legal & Practical

Considerations for E-Signing On The Virtual Dotted Line, New York Law Journal, Vol. 1 No. 1, P. 2, (2019).

Aulianisa, S. S., & Indirwan, I. (2020). LESREV (Lex Scientia Law Review),. Lesrev (Lex

Scientia Law Review), 4(1), 33–48.

Dermawan, Rizki, (2021). Pemanfaatan Tanda Tangan Elektronik Tersertifikasi di Era

Pandemi, Jurnal Hukum Lex Generalis, Rewang Rencang, Vol 2 No 8

Edesiri G. Okoro and Promise E. Kigho, (2013)‘The Problem and Prospects of E-

transaction (The Nigerian Perspective), Journal of Research in International Business and Management, Vol. 3 (1)

Electronic Commerce (Provision of Legal Recognition) Bill 2011.
Electronic Transaction Bill 2011.
Evidence Act, 2011, Laws of the Federation of Nigeria.
HIPCAR, (2011) 'Electronic Transaction: Assessment Report', harmonization of ICT
Policies, Legislation and Regulatory Procedures in the Caribbean.
Kalama M. Lui Kwan, Recent Developments in Digital Signature Legislation Electronic
Commerce, Barkeley Technology Law Journal, Vol 14 No. 1, Annual Review of Law and Technology, P. 463-481. (1999).
Kancauskiene, Jolita, (2019) Computer forensics and electronic evidence in criminal legal
proceeding, Digital Evidence & Electronic Signature Law Review Journal, Volume 16, SAS University of London, P.11,
Lawrence Freidman, Legal System, 1975, New York, Russel Sage Foundations, Dalam
Esmi Warassih.
Legal Prisms: Directions in Nigerian Law and Practice, Usmanu Danfodiyo University
Press, Sokoto.
M. L. Ahmadu, (2012) 'Information Technology and Legislative Processes in Nigeria', in
M. L. Ahmadu (ed)
Ministry of Communication and Informatics, (2021). Tanda Tangan Elektronik Menjadi
Solusi Di Era Digital, Direktorat Jenderal Aplikasi Informatika
Mu'azu Abdullahi Saulawa1* Junaidu Bello Marshal 2, (2015) The Relevance of Electronic
Signatures in Electronic Transactions: An Anlysis of Legal Framework. Journal of Law, Policy and Globalization, 34(13), 5-13
National Information Technology Development Agency Act (NITDA) 2007.
Ningrum, I., P., Dalimunthe, S.,N.,I.,S., (2022) The Validity and Power of Proof of
Electronic Signatures That Have Not Been Certified in Indonesian Law Asian Journal of Law and Governance e-ISSN: 2710-5849 | Vol. 4, No. 1, 11-18, 2022
Nityasari, A. (2021). Technology Disruptions in International Relations: The Needs for
Cyber Diplomacy by Indonesia. Global South Review, 2(1), 36. https://doi.org/10.22146/globalsouth.50423
Rehulina, (2022) Keabsahan Digital Signature Dalam Perjanjian E-Commerce, The Journal
of Law, Volume 1, P.45.
Thakare, S. P., & Sarda, S. N. (2015). A Review on Information Technology and Cyber
Laws. Technology and Cyber, 2(5), 10–16.