SKRIPSI

ANALISIS KOMPARASI SISTEM HUKUM DI BIDANG SERTIFIKASI ELEKTRONIK ANTARA INDONESIA DAN SINGAPURA

OLEH:

HUMAERAH HAIRUNNISA

NIM: 2120203874235022

PROGRAM STUDI HUKUM TATA NEGARA

FAKULTAS SYARIAH DAN ILMU HUKUM ISLAM

INSTITUT AGAMA ISLAM NEGERI

PAREPARE

2025

SKRIPSI

ANALISIS KOMPARASI SISTEM HUKUM DI BIDANG SERTIFIKASI ELEKTRONIK ANTARA INDONESIA DAN SINGAPURA

Skripsi sebagai salah satu syarat untuk memperoleh gelar Sarjana Hukum (S.H.) pada Program Studi Hukum Tata Negara Fakultas Syariah dan Ilmu Hukum Islam Institut Agama Islam Negeri Parepare

OLEH:

HUMAERAH HAIRUNNISA

NIM: 2120203874235022

PROGRAM STUDI HUKUM TATA NEGARA

FAKULTAS SYARIAH DAN ILMU HUKUM ISLAM

INSTITUT AGAMA ISLAM NEGERI

PAREPARE

2025

PERSETUJUAN SKRIPSI

Judul Skripsi	: Analisis Komparasi Sistem Hukum Di Bidang Sertifikasi Elektronik Antara Indonesia Dan Singapura
Nama Mahasiswa	: Humaerah Hairunnisa
NIM	: 2120203874235022
Program Studi	: Hukum Tata Negara
Fakultas	: Syariah dan Ilmu Hukum Islam
Dasar Penetapan Pembimbing	: Surat Keputusan Dekan Fakultas Syariah dan Ilmu Hukum Islam Nomor 1108 Tahun 2024.

Disetujui Oleh

Pembimbing	: Dr. H. Syafaat Anugrah Pradana, S.H., M.H. (.....)
NIP	: 19930526 201903 1 008

Mengetahui:

Fakultas Syariah dan Ilmu Hukum Islam

Dekan,

Dr. Rahmawati, S.Ag., M.Ag.

NIP. 19760901 200604 2 001

PENGESAHAN KOMISI PENGUJI

Judul Skripsi	: Analisis Komparasi Sistem Hukum Di Bidang Sertifikasi Elektronik Antara Indonesia Dan Singapura
Nama Mahasiswa	: Humaerah Hairunnisa
NIM	: 2120203874235022
Program Studi	: Hukum Tata Negara
Fakultas	: Syariah dan Ilmu Hukum Islam
Dasar Penetapan Pembimbing	: Surat Keputusan Dekan Fakultas Syariah dan Ilmu Hukum Islam Nomor 1108 Tahun 2024.
Tanggal Kelulusan	: 24 Juni 2025

Disahkan oleh Komisi Penguji

Dr. H. Syafaat Anugrah Pradana, S.H., M.H.	(Ketua)	(.....)
Dr. Zainal Said, M.H.	(Anggota)	(.....)
Hasanuddin Hasim, M.H.	(Anggota)	(.....)

Mengetahui:

Fakultas Syariah dan Ilmu Hukum Islam

Dekan,

Dr. Rahmawati, S.Ag., M.Ag.

NIP. 19760901 200604 2 001

KATA PENGANTAR

بِسْمِ اللهِ الرَّحْمٰنِ الرَّحِيْم

اَلْحَمْدُ لِلّٰهِ رَبِّ الْعَالَمِيْنَ وَالصَّلَاةُ وَالسَّلَامُ عَلَى أَشْرَفِ الْأَنْبِيَاءِ وَالْمُرْسَلِيْنَ وَعَلَى اٰلِهٖ وَصَحْبِهٖ أَجْمَعِيْنَ أَمَّا بَعْد

Puji dan syukur penulis panjatkan ke hadirat Allah swt. karena atas limpahan rahmat dan karunia-Nya penulis dapat menyelesaikan skripsi ini dengan judul "Analisis Komparasi Sistem Hukum Di Bidang Sertifikasi Elektronik Antara Indonesia Dan Singapura" sebagaai salah satu syarat untuk memperoleh gelar Sarjana Hukum (S.H), Program Studi Hukum Tata Negara, Fakutas Syariah Dan Ilmu Hukum Islam, Institut Agama Islam Negeri (IAIN) Parepare.

Penulis menghaturkan banyak terima kasih yang setulus-tulusnya kepada kedua orang tua tercinta yakni Almh. Ibunda Enceng dan Ayahanda Abdul Asis dimana dengan support dan berkah doa tulusnya, penulis mendapatkan kemudahan dalam menyelesaikan tugas akademik tepat pada waktunya.

Penulis telah menerima banyak bimbingan dan bantuan dari Bapak Dr. H. Syafaat Anugrah Pradana, S.H., M.H. selaku dosen pembimbing, sekaligus Ketua Program Studi Hukum Tata Negara. Atas segala bantuan dan bimbingan yang telah diberikan, penulis ucapkan banyak-banyak terima kasih. Atas bimbingan beliau-lah, penulis dapat semangat dalam menyelesaikan tugas akademik ini tepat pada waktunya.

Selanjutnya, penulis juga menyampaikan terima kasih kepada:

1. Bapak Prof. Dr. Hannani, M.Ag. sebagai Rektor IAIN Parepare yang telah bekerja keras mengelola pendidikan di IAIN Parepare.

2. Ibu Dr. Rahmawati, S.Ag., M.Ag. sebagai Dekan Fakultas Syariah dan Ilmu Hukum Islam atas pengabdiannya dalam menciptakan suasana pendidikan yang positif bagi mahasiswa.
3. Dosen Penguji Penulis, Bapak Dr. Zainal Said, M.H. dan Bapak Hasanuddin Hasim, S.H., M.H. yang telah meluangkan waktunya untuk menghadiri seminar proposal dan seminar hasil, serta telah memberikan kritik dan saran untuk penyelesaian skripsi ini.
4. Bapak dan Ibu dosen program studi Hukum Tata Negara yang telah meluangkan waktu mereka dalam mendidik dan membimbing penulis selama masa studi di IAIN Parepare.
5. Bapak dan Ibu staf administrasi Fakultas Syariah Dan Ilmu Hukum Islam yang telah membantu kelancaran proses akademik penulis, baik secara administrasi maupun informasi yang dibutuhkan selama masa studi.
6. Bapak dan Ibu petugas kebersihan dan keamanan kampus yang setia menjaga kebersihan dan kenyamanan lingkungan belajar.
7. Keluarga Besar H. Mada & Larasa' yang mendukung secara materil maupun moril.
8. Sahabat tersayang Najwah Fathi, Sulistiawaty, Arfah Yunus, St. Nur Fatirah, Andi Nanda, dan Risda yang selalu setia menemani penulis dan merupakan teman seperjuangan sejak SMP dan menjadi tempat berbagi segala suka dan duka.
9. Putri Amanda dan Delia teman sperjuangan selama bangku kuliah, yang senantiasa menamani dalam suka dan duka sampai pada titik ini.

10. Teman sekelah HTN A yang sama-sama seperjuangan dari maba sampai titik mahasiswa akhir.
11. Sabilul Muhtadin, S.E. dengan kontribusinya sebagai *support system* dalam menyelesaikan penulisan ini.
12. Diri Sendiri yang telah kuat bertahan dan berjuang sejauh ini, menghadapi rentetang pertanyaan "Kamu Kapan?", mari tetap kuat untuk selamanya.

Penulis tak lupa mengucapkan terima kasih kepada semua pihak yang telah memberikan bantuan, baik moril maupun material hingga tulisan ini dapat diselesaikan. Semoga Allah swt. berkenan menilai segala kebajikan sebagai amal jariyah dan memberikan rahmat dan pahala-Nya.

Akhirnya penulis menyadari bahwa penulisan skripsi ini masih banyak kekurangan. Oleh karena itu, penulis mengharapkan kritik dan saran yang bersifat konstruktif demi kesempurnaan skripsi ini.

Parepare, 28 April 2025

Penulis,

Humaerah Hairunnisa
NIM. 2120203874235022

PERNYATAAN KEASLIAN SKRIPSI

Mahasiswa yang bertanda tangan di bawah ini

Nama	: Humaerah Hairunnisa
NIM	: 2120203874235022
Tempat/Tgl. Lahir	: Pinrang, 02 Juli 2002
Program Studi	: Hukum Tata Negara
Fakultas	: Syariah dan Ilmu Hukum Islam
Judul Skripsi	: Analisis Komparasi Sistem Hukum Di Bidang Sertifikasi Elektronik Antara Indonesia Dan Singapura

Menyatakan dengan sesungguhnya dan penuh kesadaran bahwa skripsi ini benar merupakan hasil karya saya sendiri. Apabila dikemudian hari terbukti bahwa ia merupakan duplikat, tiruan, plagiat, ataun dibuat oleh orang lain, sebagian atau seluruhnya, maka skripsi dan gelar yang diperoleh karenanya batal demi hukum.

Parepare, 24 Mei 2025

Penulis,

Humaerah Hairunnisa
NIM. 2120203874235022

ABSTRAK

Humaerah Hairunnisa, *Analisis Komparasi Sistem Hukum di Bidang Sertifikasi Elektronik Antara Indonesia dan Singapura.* (dibimbing oleh Dr. H. Syafaat Anugrah Pradana,S.H., M.H.)

Sertifikasi elektronik merupakan elemen penting dalam ekosistem transaksi digital untuk menjamin keamanan, keautentikan, dan keandalan sistem elektronik. Penelitian ini bertujuan untuk menganalisis perbandingan hukum di bidang sertifikasi elektronik antara Indonesia dan Singapura dengan merekomendasikan penguatan regulasi dan standarisasi di Indonesia untuk meningkatkan kepercayaan dan penggunaan dalam transaksi elektronik global, dengan mempertimbangkan praktik terbaik dari Singapura.

Penelitian ini menggunakan pendekatan yuridis normatif dengan metode komparatif untuk mengkaji peraturan perundang-undangan, seperti Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik (UU ITE), Peraturan Pemerintah Nomor 71 Tahun 2019 di Indonesia, serta United Nations Commission on International Trade Law (UNCITRAL) & Electronic Transactions Act (ETA) di Singapura.

Hasil penelitian menunjukkan bahwa Indonesia mengatur sertifikasi elektronik melalui pendekatan berbasis otoritas pemerintah, seperti Badan Siber dan Sandi Negara (BSSN), dengan penekanan pada validasi identitas dan keamanan sistem elektronik melalui Balai Sertifikasi Elektronik (BsrE). Sementara itu, Singapura menerapkan pendekatan yang lebih fleksibel dengan melibatkan sektor swasta sebagai Certification Authorities (CA) yang diakui, mendukung ekosistem bisnis yang berorientasi global. Faktor-faktor yang mempengaruhi perbedaan meliputi konteks kelembagaan, budaya, tingkat perkembangan teknologi, standar internasional, dan regulasi yang dipengaruhi oleh sistem hukum masing-masing negara.

Kata Kunci: Sertifikasi Elektronik, Perbandingan, Indonesia, Singapura, Sistem Hukum, Faktor Perbandingan

DAFTAR ISI

TRANSLITERASI DAN SINGKATAN

A. Transliterasi

1. Konsonan

Fonem konsonan bahasa Arab yang dalam sistem tulisan Arab dilambangkan dengan huruf, dalam transliterasi ini sebagian dilambangkan dengan huruf dan sebagian dilambangkan dengan tanda, dan sebagian lain lagi dilambangkan dengan huruf dan tanda.

Daftar huruf bahasa Arab dan transliterasinya kedalam huruf Latin dapat dilihat pada halaman berikut :

Huruf	Nama	Huruf Latin	Keterangan
ا	Alif	tidak dilambangkan	tidak dilambangkan
ب	Ba	B	Be
ت	Ta	T	Te
ث	Tha	T	te dan ha
ج	Jim	J	Je
ح	Ha	ḥ	ha (dengan titik di bawah)
خ	Kha	Kh	ka dan ha
د	Dal	D	De
ذ	Dhal	Dh	de dan ha
ر	Ra	R	Er
ز	Zai	Z	Zet
س	Sin	S	Es
ش	Syin	Sy	es dan ye

ص	Shad	Ṣ	es (dengan titik di bawah)
ض	Dad	ḍ	de (dengan titik di bawah)
ط	Ta	ṭ	te (dengan titik di bawah)
ظ	Za	ẓ	zet (dengan titik di bawah)
ع	‘ain	‘	koma terbalik ke atas
غ	Gain	G	Ge
ف	Fa	F	Ef
ق	Qaf	Q	Q
ك	Kaf	K	Ka
ل	Lam	L	El
م	Mim	M	Em
ن	Nun	N	En
و	Wau	W	We
ه	Ha	H	Ha
ء	Hamzah	‘	Apostrof
ى	Ya	Y	Ye

Hamzah (ء) yang terletak di awal kata mengikuti vokalnya tanpa diberi tanda apapun. Jika ia terletak di tengah atau di akhir, maka ditulis dengan tanda (‘).

2. Vokal

Vokal bahasa Arab, seperti vokal bahasa Indonesia, terdiri atas vokal tunggal atau monoftong dan vokal rangkap atau diftong. Vokal tunggal bahasa

Arab yang lambangnya berupat anda atau harakat, transliterasinya sebagai berikut :

Tanda	Nama	Huruf Latin	Nama
اَ	*Fathah*	A	A
اِ	*Kasrah*	I	I
اُ	*Dammah*	U	U

Vokal rangkap bahasa Arab yang lambangnya berupa gabungan antara harakat dan huruf, transliterasinya berupa gabungan huruf, yaitu :

Tanda	Nama	Huruf Latin	Nama
ـَيْ	*Fathah* dan *yá'*	A	a dan i
ـَوْ	*Fathah* dan *wau*	Au	a dan u

Contoh :

كَيْفَ : k*aifa*

هَوْلَ : hau*la*

3. *Maddah*

Maddah atau vokal panjang yang lambangnya berupa harakat dan huruf, transliterasinya berupa huruf dan tanda, yaitu:

Harakat dan Huruf	Nama	Huruf dan Tanda	Nama
ـَا | ـَى	*Fathah* dan *alif* dan *yá'*	Ā	a dan garis di atas
ـِيْ	*Kasrah* dan *yá'*	Î	i dan garis di atas

ـُوْ	*Dammah* dan *wau*	Û	u dan garis di atas

Contoh :

مَاتَ : māta

رَمَى : ramā

قِيْلَ : qîla

يَمُوْتُ : *yamûtu*

4. *Tā'Marbutah*

Transliterasi untuk *tā' marbutah* ada dua, yaitu:

a) *tā' marbutah* yang hidup atau mendapat harakat *fathah, kasrah,* dan *dammah,* transliterasinya adalah [t].

b) *tāmarbŭtah* yang mati atau mendapat harakat sukun, transliterasinya adalah [h].

Kalau pada kata yang berakhir dengan *tāmarbûtah* diikuti oleh kata yang menggunakan kata sandang *al*-serta bacaan kedua kata itu terpisah, maka *tāmarbûtah* itu ditransliterasikan dengan *ha* (*h*).

Contoh :

رَوْضَةُ الجَنَّةِ : rauḍah al-jannah atau rauḍatul jannah

اَلْمَدِيْنَةُ اَلْفاضِلَةُ : al-madīnah al-fādilahatau al-madīnatul fāḍilah

اَلْحِكْمَةُ : *al-hikmah*

5. *Syaddah* (*Tasydid*)

Syaddah atau *tasydid* yang dalam sistem tulisan Arab dilambangkan dengan sebuah tanda *tasydid*(ـّ), dalam transliterasi ini dilambangkan dengan perulangan huruf (konsonan ganda) yang diberi tanda *syaddah.*

Contoh :

رَبَّنَا : rabbanā

نَجَّيْنَا : najjainā

الْحَقُّ : al-haqq

نُعِّمَ : nu'ima

عَدُوٌّ : 'aduwwun

Jika huruf ber-tasydid di akhir sebuah kata dan didahului oleh huruf kasrah(ـِـيّ), maka ia ditransliterasi seperti huruf maddah menjadi (î).

عَلِيٌّ : 'Ali (bukan 'Aliyyatau 'Aly)

عَرَبِيٌّ : 'Arabi (bukan 'Arabiyyatau 'Araby)

6. Kata Sandang

Kata sandang dalam sistem tulisan Arab dilambangkan dengan huruf لا *(alif lam ma'arifah).* Dalam pedoman transliterasi ini, kata sandang ditransliterasi seperti biasa, al-, baik Ketika ia diikuti oleh huruf *syamsiyah* maupun huruf *qamariyah.* Kata sandang tidak mengikuti bunyi huruf langsung yang mengikutinya. Kata sandang ditulis terpisah dari kata yang mengikutinya dan dihubungkan dengan garis mendatar (-).

Contoh :

اَلشَّمْسُ : al-syamsu (bukanasy-syamsu)

اَلزَّلْزَلَةُ : al-zalzalah (bukanaz-zalzalah)

اَلْفَلْسَفَةُ : al-falsafah

اَلْبِلاَدُ : *al-bilādu*

7. Hamzah

Aturan transliterasi huruf hamzah menjadi apostrof (‘) hanya berlaku bagi hamzah yang terletak di tengah dan akhir kata. Namun, bila hamzah terletak di awal kata, ia tidak dilambangkan, karena dalam tulisan Arab ia berupa alif.

Contoh :

تَأْمُرُوْنَ : ta’muruna

اَلنَّوْعُ : al-nau’

شَيْءٌ : syai’un

أُمِرْتُ : *umirtu*

8. Kata Arab yang lazim digunakan dalam Bahasa Indonesia

Kata, istilah atau kalimat Arab yang ditransliterasi adalah kata, istilah atau kalimat yang belum dilakukan dalam bahasa Indonesia. Kata, istilah atau kalimat yang sudah lazim dan menjadi bagian dari perbendaharaan bahasa Indonesia, atau sering ditulis dalam tulisan bahasa Indonesia, atau lazim digunakan dalam dunia akademik tertentu, tidak lagi ditulis menurut cara transliterasi di atas. Misalnya, kata al-Qur’an (dari*al-Qur’ān)*, alhamdulillah, dan munaqasyah. Namun, bila kata-kata tersebut menjadi bagian dari satu rangkaian kosa kata Arab, maka harus ditransliterasi secara utuh. Contoh :

Fīẓilāl al-qur’an

Al-Sunnah qabl al-tadwin

Al-ibārat bi ‘umum al-lafẓlā bi khusus al-saba

9. *Lafz al-jalalah* (الله)

Kata “Allah” yang didahului partikel seperti huruf jar dan huruf lainnya atau berkedudukan sebagai mudafilaih (frasa nominal), ditransliterasi tanpa huruf hamzah.

Contoh :

دِيْنُاللهِ : dīnullah بِاللهِ : billah

Adapun ta’ marbutah di akhir kata yang disandarkan kepada lafẓ al-jalālah, ditransliterasi dengan huruf [t].

Contoh :

هُم فى رَ حْمَةِ اللهِ : *hum fīrahmatillāh*

10. Huruf Kapital

Walau sistem tulisan Arab tidak mengenal huruf kapital *(All Caps),* dalam transliterasinya huruf-huruf tersebut dikenal ketentuan tentang penggunaan huruf kapital berdasarkan pedoman ejaan Bahasa Indonesia yang berlaku (EYD). Huruf kapital, misalnya, digunakan untuk menuliskan huruf awal namadiri (orang, tempat, bulan) dan huruf pertama pada permulaan kalimat. Bila nama diri didahului oleh kata sandang (*al-*), maka yang ditulis dengan huruf kapital tetap huruf awal nama diri tersebut, bukan huruf awal kata sandangnya. Jika terletak pada awal kalimat, maka huruf A dari kata sandang tersebut menggunakan huruf kapital (*Al-*).

Contoh:

Wamā Muhammadunillārasūl

Inna awwalabaitin wudi’alinnasilalladhī bi Bakkatamubārakan

Syahru Ramadan al-ladhīunzilafih al-Qur’an

Nasir al-Din al-Tusī

Abū Nasr al-Farabi

Al-Gazali

Al-Munqizmin al-Dalal

Jika nama resmi seseorang menggunakan kata Ibnu (anak dari) dan Abu (bapak dari) sebagai nama kedua terakhirnya, maka kedua nama terakhir itu harus disebutkan sebagai nama akhir dalam daftar Pustaka atau daftar referensi. Contoh :

Abu al-Wafid Muhammad ibn Rusyd, ditulis menjadi: Ibnu Rusyd, Abu al-Walid Muhammad (bukan: Rusyd, Abu al-Walid Muhammad Ibnu)

Nasr Hamid Abu Zaid, ditulis menjadi: Abu Zaid, Nasr Hamid (bukan: Zaid, Nasr Hamid Abu)

B. Singkatan

Beberapa singkatan yang dibaku kan adalah :

swt.	: *subḥānahūwata'āla*
saw.	: *ṣhallallāhu 'alaihiwasallam*
a.s.	: *'alaihi al-sallām*
H	: Hijriah
M	: Masehi
SM	: Sebelum Masehi
l.	: Lahir tahun (untuk tahun yang masih hidup saja)
w.	: Wafat tahun
QS./.: 4	: QS al-Baqarah/2:187 atau QS Ibrahim/…, ayat 4
HR	: Hadis Riwayat

Beberapa singkatan dalam bahasa Arab:

ص = صفحه

دم = بدون مكان

صلعم = صلى الله علية وسلم

ط= طبعة

دن = بدون ناشر

الخ = إلى آخرها/آخره

ج= جزء

Beberapa singkatan yang digunakan secara khusus dalam teks referensi perlu dijelaskan kepanjangannya, di antaranya sebagai berikut:

ed. : Editor (atau, eds. [dari kata editors] jika lebih dari satu orang editor). Karena dalam bahasa Indonesia kata "editor" berlaku baik untuk satu atau lebih editor, maka ia bisa saja tetap disingkat ed. (tanpa s).

et al. : "Dan lain-lain" atau "dan kawan-kawan" (singkatan dari *etalia*). Ditulis dengan huruf miring. Alternatifnya, digunakan singkatan dkk. ("dan kawan-kawan") yang ditulis dengan huruf biasa/tegak.

Cet. : Cetakan. Keterangan frekuensi cetakan buku atau literatur sejenis.

Terj. : Terjemahan (oleh). Singkatan ini juga digunakan untuk penulisan karya terjemahan yang tidak menyebutkan nama pengarannya.

Vol. : Volume. Dipakai untuk menunjukkan jumlah jilid sebuah buku atau ensiklopedia dalam bahasa Inggris. Untuk buku-buku berbahasa Arab biasanya digunakan kata juz.

No. : Nomor. Digunakan untuk menunjukkan jumlah nomor karya ilmiah berkala seperti jurnal, majalah, dan sebagainya.

BAB I
PENDAHULUAN

A. Latar Belakang Masalah

Pada era globalisasi, masa interaksi dan konektivitas antarnegara maupun antarindividu meningkat pesat secara signifikan, terutama melalui perkembangan teknologi, komunikasi, dan transaksi pada bisnis elektronik. Melalui proses transformasi, transaksi elektronik dikemas pada bentuk *e-business, e-government, e-commerce, & e-procurement.* Tentunya, hal ini merupakan peluang yang menjanjikan sebab adanya kemudahan bertransaksi dimanapun, kapanpun, dan siapapun.

Namun, dibalik kemudahan penggunaan teknologi, dampak negatif berupa kemanan, ancaman, maupun berita hoaks juga semakin meningkat. Adanya dampak negatif menuntut solusi keamanan berupa langkah maupun strategi yang dirancang oleh pemerintah dalam melindungi data, aset, dan sistem dari ancaman yang dapat membahayakan integritas dan kerahasiaan. [1] Dengan menempatkan keamanan sebagai prioritas utama, individu, organisasi, dan negara dapat menciptakan ekosistem yang lebih aman, mencegah risiko, dan memitigasi dampak dari ancaman potensial. Di era digital, pendekatan proaktif terhadap keamanan adalah kunci untuk menjaga kepercayaan dan stabilitas.

Di Indonesia, aturan tentang Sertifikasi Elektronik diatur di Dalam Undang-Undang Nomor 1 Tahun 2024 Tentang Informasi Dan Transaksi Elektronik yang merupakan perubahan kedua dari Undang-Undang Nomor 11 Tahun 2008, perubahan

[1] Setiawan, "Ekosistem Penyelenggaraan Sertifikat Elektronik Dalam Sistem Perdagangan Elektronik The Ecosystem Of Electronic Certificate Implementation In Electronic Commerce System" 2015

dilakukan guna beberapa ketentuan dalam UU ITE sebelumnya masih menimbulkan kontroversi di Masyarakat, tentunya tujuan atas perubahan ini adalah mewujudkan rasa keadilan dan kepastian hukum di berbagai pihak. Undang-Undang Nomor 1 Tahun 2024 menyempurnakan ketentuan penting seperti alat bukti elektronik yang terdapat pasal 5, mengatur lebih lanjut tentang Penyelenggara Sertifikasi Elektronik yang terdapat pada pasal 13 ayat 1 yang menyatakan bahwa "Setiap orang berhak menggunakan jasa Penyelenggara Sertifikasi Elektronik untuk pembuatan tanda tangan elektronik" Pernyataan tersebut berarti bahwa setiap individu memiliki hak untuk menggunakan layanan yang disediakan oleh **Penyelenggara Sertifikasi Elektronik (PSrE)** untuk membuat tanda tangan elektronik.

Penyelenggara Sertifikasi Elektronik adalah lembaga yang menyediakan layanan terkait penerbitan dan pengelolaan Sertifikat Elektronik yang digunakan untuk Tanda Tangan Elektronik. Lembaga Penyelenggara Sertifikasi Elektronik berperan dalam mendukung keamanan transaksi daring melalui penggunaan Tanda Tangan Digital (*Digital Signature*) dan teknologi Infrastruktur Kunci Publik (*Public Key Infrastructure*). Standar spesifikasi teknis Sertifikat Elektronik umumnya menggunakan standar X.509.v3 yaitu format standar internasional yang digunakan untuk sertifikat elektronik dalam sistem keamanan digital. [2]

Sebagaimana halnya dengan Indonesia, Singapura juga menginisiasi penerapan sertifikasi elektronik melalui penerapan regulasi Tanda Tangan Elektronik *(electronic signature)* yang diakui dalam sistem hukum positif di Singapura serta dalam kerangka hukum internasional. Aturan hukumnya di atur pada UNCITRAL *Model Law on Electronic Signature, The General EU Electronic Commerce Directive*

[2] Mardianto, "Implementasi Keamanan pada Transaksi Data Menggunakan Sertifikat Digital X.509" tahun 2016

– 4 Mei 2000, Electronic Signature Directive - 30 November 1999, Brussels Convention on Online Transactions - 1 Maret 2002 dan GUIDEC (General Usage for International Digitally Electronic Commerce). Dalam hukum positif di Singapura tanda tangan elektronik dalam transaksi elektronik diatur pada *Electronic Transactions Act Cap 88, 2010.* Undang-Undang ini telah diamandemen pada tahun 2021 *(elektronic transactions (amandment) act 2021 cap. 5).*

Pada dasarnya, kebijakan di Indonesia mengenai Sertifikasi Elektronik menunjukkan sejumlah keselarasan dengan prinsip-prinsip yang tertuang pada kebijakan yang ada di Singapura dengan bidang yang sama. Secara normatif, kedua kedua instrument hukum tersebut memiliki tujuan yang sama tapi tak serupa. Contohnya pada *Electronik Transactions Act Singapore* cocok dengan pasal nomor 5 dan 13 di dalam UU ITE tentang alat bukti elektronik, Sertifikasi Elektronik, dan identitas digital. ETA mengakui legalitas dokumen dan tanda tangan elektronik.

Kemudian, adanya prinsip *Legal Recognition of Electronik Signature* (Pengakuan Hukum terhadap Tanda Tangan Elektronik) dari kebijakan UU ITE yang terdapat pada pasal 11 yaitu penggunaan tanda tangan elektronik diakui sepanjang memenuhi syarat serta kebijakan UNCITRAL yang fokus pada fuctional equivalence antara tanda tangan digital dan tanda tangan basah. Indonesia membedakan Tanda Tangan Elektronik yang tersertifikasi dan belum tersertifikasi, yang tersertifikasi jauh mempunyai kekuatan hukum yang lebih sedangkan Singapura berfokus pada keamanan teknis. Pada Sertifikasi Elektronik, Indonesia mewajibkan akreditasi untuk PSrE dan Singapura lebih bersifat sukarela atau fleksibel karena Singapura mengadopsi UNCITRAL yang bersifat netral dan fleksibel, artinya asalkan Tanda Tangan Elektronik aman dan dapat diverifikasi, dapat diakui sah secara hukum.

Prinsip *Legal Recognition of Electronik Signature* (pengakuan hukum terhadap tanda tangan elektronik) merupakan manifestasi dari *asas kepas*tian hukum dan *asas persamaan* di hadapan hukum dalam konteks hukum digital. Dapat disimpulkan bahwa kebijakan hukum di Indonesia cenderung lebih ketat dan formal dengan penekanan pada legitimasi melalui Penyelenggara Sertifikasi Elektronik yang diatur secara sentralistik. Sebaliknya, Singapura menerapkan pendekatan yang lebih fleksibel dan berbasis pasar, dengan memberikan ruangmyang lebih luas bagi sekor swasta dalam pengembangan dan pemanfaatan infrastruktur identitas serta Sertifikasi Elektronik.

Dalam konteks standar keamanan, standar X.509.v3 memastikan bahwa Sertifikat Elektronik memiliki format yang seragam, aman, dan dapat digunakan di berbagai aplikasi keamanan digital seperti pada web service yang membuat pengguna percaya dan tidak ragu-ragu dalam dalam melakukan transaksi. [3] Fasilitas ini secara signifikan mendukung interoperabilitas antar sistem yang berbeda dalam ekosistem transaksi yang aman. Standardisasi dalam bidang elektronik dan telekomunikasi yang dirumuskan oleh badan pembuat standar *internasional (International Organization for Standardization/International Electrotechnical Commission, 2000)*, baik pada tingkat internasional maupun nasional, dapat disimpulkan sebagai berikut:

[3] Setiawan, "Studi Standardisasi Sertifikat Elektronik dan Keandalan dalam Penyelenggaraan Sistem Transaksi Elektronik The Study of Electronics Certificate and Certificate of Reliability Standarization in The Implementation of Electronic Transaction System" tahun 2014

No.	Internasional	Nasional
1.	**ISO:** *International Organitization For Standardization* (www.iso.ch)	***BSN:*** *Badan Standardisasi Nasional (www.bsn.go.id)*
2.	**IEC:** *International Electrotechnical Commision* (www.iec. ch)	
3.	**ITU-T:** *European Telecommunitications Standards Institute* (http://www.etsi.org/)	
4.	***ETSI:*** *European Telecommunications Standards Institute* (http://www.etsi.org/)	
5.	***ANSI****: American National Standards Institute (www.ansi.org)*	
6.	**IEEE:** *Institute of Electrical and Electronic Engineers (standards.ieee.org)*	
7.	***IETF****: Internet Engineering Task Force (www.ietf.org)*	

Tabel 1.1

Khususnya dalam tingkat nasional selain Badan Standardisasi Nasional (BSN), tidak ada lembaga lain di Indonesia yang memiliki peran langsung sebagai badan resmi untuk mengelola standar internasional seperti ISO atau IEC, sementara itu jika disandingkan dengan Singapura, Negara ini memiliki **ESG:** Enterprise Singapore yang mengelola dan mengembangkan standar nasional serta bekerja sama dengan organisasi standar internasional seperti ISO dan IEC, Enterprise Singapore bertanggung jawab untuk memfasilitasi pengembangan standar nasional melalui Singapore Standards Council (SSC), yang bekerja di bawah naungan ESG.

SSC mengelola berbagai standar teknis dan kualitas untuk industri lokal, sekaligus mengadopsi dan mempromosikan standar internasional. penyelenggara Sertifikat Elektronik *(Certification Authority)* CA dihubungkan dengan menggunakan hirarkis dan lintas-sertifikat *(cross-certified)*. Kedua model ini memiliki karakteristik unik dalam membangun kepercayaan dan mengelola otoritas sertifikat elektronik. [4]

1. Model Hirarkis

   Model hirarkis menggunakan pendekatan berjenjang dengan satu root certificate authority (CA) sebagai entitas pusat yang memiliki kendali penuh atas sertifikat yang dikeluarkan. Dimulai dari satu root CA, yang dapat mendelegasikan wewenang ke (CA bawahan). Di dalam model hirarkis tingkat tertinggi ialah PsrE induk dan tingkat terendah ialah PsrE bawahan yang berarti PsrE Induk memiliki tingkat persyaratan keamanan yang lebih ketat sehingga sulit bagi penyerang untuk mengakses PsrE induk.

   Beberapa tata kelola hierarki seperti tingkatan direktif fokus pada regulasi makro dan berada di level yang tinggi, seperti UU 1/2024 tentang ITE, sementara pada tingkatan bawah menitikberatkan aspek ketersediaan infrastuktur dan dukungan operasional. Tingkatan direktif di level regulasi makro ialah Undang-Undang (UU) nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik (ITE) yang merujuk pada aturan atau kebijakan yang bersifat strategis, memberikan panduan umum, dan berlaku secara nasional dan fokusnya adalah menciptakan kerangka kerja yang mengatur pada skala besar atau makro. Aturan ini berada pada level yang tinggi (contoh: undang-undang) dan memberikan dasar hukum yang luas untuk implementasi kebijakan lebih lanjut. [5]

---

[4] Kakei S, Shiraishi Y, Saito S, "Cross-Certification towards Distributed Authentication Infrastructure: A Case of Hyperledger Fabric" 2020, Research, Japan Society for the Promotion of Science, Hibah Nomor JP19K24342, JP19K11963, dan JP18K04133.

[5] Hermawan Perancangan Manajemen Risiko Keamanan Informasi pada Penyelenggara Sertifikasi Elektronik (PSrE) 2019*)*

Pada regulasi makro yang mengatur berbagai aspek terkait informasi dan transaksi elektronik, seperti keamanan siber, privasi data, dan penggunaan teknologi digital. Akibatnya, model hierarkis dapat menurunkan keandalan seluruh sistem ke tingkat yang lebih besar. Di Internet, sebagian besar CA dibuat menggunakan model hierarkis karena memungkinkan hubungan kepercayaan diperluas dengan mudah.

2. Lintas-sertifikat *(cross-certified)*

Dalam ekosistem Internet of Things, di mana berbagai entitas memperdagangkan data dan hasil analisis data, infrastruktur kunci publik memainkan peran penting dalam membangun hubungan kepercayaan antara entitas ini untuk menentukan siapa yang mempercayai kunci pribadi siapa. Pemilik kunci privat diberikan sertifikat kunci publik yang dikeluarkan oleh otoritas sertifikat (CA) yang mewakili pihak ketiga tepercaya. Pada Januari 2024 diterbitkan pembaharuan sertifikat AlphaSSL dan Alpha SSL Wildcard, sertifikat ini ialah SSL yang digunakan untuk mengamankan situs web dan subdomain, sertifikat ini berguna untuk mengurangi potensi pencurian data, misalnya, pada satu sertifikat Wilcard dapat mengamankan contohnya pada situs *www.dreamtheater.com, blog.meovv.com,* dan *store.blackpink.com.*

Dengan menggunakan enkripsi 256 bit yang layak melindungi situs. infrastruktur otentikasi terdistribusi yang mendesentralisasikan titik kepercayaan CA sehingga mereka didistribusikan di antara beberapa penyedia layanan dan menghubungkannya melalui sertifikasi silang. Lintas sertifikat dalam konteks **CA *(Certificate Authority)*** biasanya mengacu pada mekanisme **cross-certification** dalam sistem keamanan jaringan.

Cross-certification adalah proses di mana dua otoritas sertifikat (CA) saling memvalidasi sertifikat digital mereka untuk menciptakan hubungan kepercayaan antara dua domain atau jaringan yang berbeda. Hal ini sering digunakan dalam sistem Public Key Infrastructure (PKI). Dan memungkinkan dua CA berbeda untuk saling percaya tanpa perlu berada dalam hierarki yang

sama juga berguna dalam integrasi dua organisasi atau jaringan dengan infrastruktur keamanan yang berbeda. CA akan saling menandatangani sertifikat satu sama lain untuk membangun kepercayaan.

Misalnya, jika CA1 mempercayai CA2, maka setiap sertifikat yang diterbitkan oleh CA2 juga dianggap valid oleh CA1, dan sebaliknya. Dalam integrasi sistem keamanan antara perusahaan atau lembaga pemerintahan yang memiliki otoritas sertifikat mereka sendiri. Juga relevan dalam sistem multi-domain atau cloud computing untuk memastikan bahwa pengguna dari dua jaringan dapat berkomunikasi secara aman.

Karakteristik kedua model ini memiliki tujuan yang serupa, yaitu untuk membangun kepercayaan serta melindungi situs-situs yang ada di dunia maya.

Dalam mendukung PSrE, Badan Pengkajian dan Penerapan Teknologi (BPPT) harus memenuhi persyaratan yang tercantum pada Peraturan Menteri Komunikasi dan Informatika NO.4 Tahun 2016 (7) yang mengatur tentang pencegahan, penanggulangan ancaman, dan serangan yang menimbulkan risiko serta memenuhi kepatuhan pada standard ISO/IEC 27001 (kepanjangan ada pada tabel 1.1)6 perkembangan pada penggunaan sistem manajemen telah meningkatkan kebutuhan bahwa BPPT adalah organisasi besar dengan menawarkan jasa dalam memenuhi persayaratan ISO 9001 yang telah direvisi menjadi ISO 9001:2015, pada ISO/IEC 27001 dan ISO 9001:2015 adalah dua standar internasional yang banyak digunakan oleh organisasi di berbagai sektor.

Standar ISO/IEC 27001 ini menyediakan kerangka kerja untuk melindungi informasi yang sensitif, memastikan kerahasiaan, integritas, dan ketersediaan data.[7] Sedangkan pada ISO 90001:2015 adalah standar untuk Sistem Manajemen Mutu (QMS) . Standar ini bertujuan untuk memastikan organisasi memberikan produk atau

[6] Hermawan Perancangan Manajemen Risiko Keamanan Informasi pada Penyelenggara Sertifikasi Elektronik (PSrE) 2019)

[7] Didah Nur Faridah and Dede Erawan 2018)

layanan yang memenuhi kebutuhan pelanggan secara konsisten. Integrasi Kedua Standar menggabungkan ISO/IEC 27001 dan ISO 9001:2015 untuk membangun sistem manajemen terpadu yang mencakup keamanan informasi dan manajemen mutu. Kombinasi ini memberikan jaminan keamanan informasi sekaligus memastikan kepuasan pelanggan.

Penggunaan pada istilah *Good Laboratory Practice* (GLP) pertama kali ditemukan di The New Zealand Testing Laboratory Registration Act of 1972, Undang-Undang ini bertujuan menetapkan kebijakan nasional di bidang pengujian. Hal ini mendorong The United States Environmental Protection Agency (US-EPA), negara-negara lain, serta organisasi internasional seperti Organization for Economic Cooperation and Development (OECD) dan World Health Organization (WHO) untuk mengembangkan dan mengadopsi Good Laboratory Practice (GLP) dalam bentuk regulasi resmi. Pengembangan pada kerangka hukum dan kebijakan penyelenggara CA di Indonesia sesuai pada reformasi hukum, masyarakat tetap saja membutuhkan pengaman informasi dan komunikasi elektronik terlebih dalam bertransaksi. Indonesia mengungkap beberapa peraturan perundang-undangan yang menjadi ketentuan hukum terkait *e-Governmen & e-Commerce*, antara lain: Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), Perubahan pertama Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (ITE), Perubahan kedua Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik (ITE), Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE), Peraturan Menteri Komunikasi dan Informatika (Kominfo), Peraturan Menteri Perdagangan No. 50 Tahun 2020 tentang Perdagangan Melalui Sistem Elektronik (PMSE). Sebagai negara hukum Indonesia merupakan contoh dalam demokrasi penerapan tata kelola dalam segala bidang.

Dengan *internet governance* Indonesia merupakan negara yang tidak otoriter dan harmonisasi kepentingan multi-stakeholders yang terbukti pada forum *Internet Governance* 2013 di Bali.[8]

Ashwin Sasongko, Direktur Jenderal Aplikasi Informatika dari Kementerian Komunikasi dan informatika menyampaikan pada *Internet Governance Forum* bahwa pemerintah Indonesia mengupayakan menyaring pendapat-pendapat dari berbagai pihak agar menilai masukan yang layak, juga meningkatkan pengguna internet secara sehat dan aman. Berlandaskan pada kebijakan sistem hukum pemerintah Indonesia dalam menghadapi penyebaran hoaks yang makin marak terjadi disetiap negara, apalagi berkembangnya teknologi pada era sekarang ini juga memungkinkan individu maupun kelompok mudah berkomunikasi, berkumpul, dan saling berbagi.[9] Hal ini yang membuat hoaks dapat dengan mudah tersebar diberbagai media. Penyeberan Pengaruh negative terhadap kebebasan berpendapat maupun berbicara di internet seperti ujaran kebencian *(hate speech)* yang dikategorikan pada pelaku individu maupun kelompok yang bersifat agresif atau verbal secara tidak langsung, dampak dari perilaku ini juga tidak main-main karena dapat membuat korban trauma pada mental dan kesusahan untuk menjalani hidup.[10]

Penyebaran berita palsu dapat membawa dampak merugikan bagi masyarakat. Di dalam ajaran Islam, Rasulullah Shalallahu alaihi Wassalam menyarankan Ketika mendapat berita harap melakukan *Tabayyun,* Alasan utama pentingnya melakukan tabayyun saat menerima informasi adalah untuk mencegah tindakan menyebarkan berita tanpa dasar yang jelas. Penyebaran berita palsu dapat membawa dampak merugikan bagi masyarakat. penting bagi umat muslim melihat pandangan dari

[8] Makarim, Penyelenggaraan Community Certification Authority Untuk Pengamanan Sumber Daya Internet Oleh Komunitas Untuk Kesiapan Asean Regional E-Commerce tahun 2015

[9] Rahmadhany, Aldila Safitri, dan Irwansyah 2021 "Fenomena Penyebaran Hoax dan Hate Speech pada Media Sosial" hal. 33

[10] Wiwin, H. Syafa'at Anugrah Pradana, and Muhammad Imam Dhiya'ul Haq, 'Regulation of Articles on State Institutional Insults to The Right to Freedom of Expression in Indonesia: A Critical Review', *Mulawarman Law Review* 2023, 2023, pp. 21–31, doi:10.30872/mulrev.v8i1.1122.

Hadits dan Al-Qur'an[11] terhadap bahayanya berita berita hoaks ini, seperti pada sabda Rasulullah Shalallahu alaihi Wassalam:

لَيْسَ الْمُؤْمِنُ بِالطَّعَّانِ وَلَا اللَّعَّانِ وَلَا الْفَاحِشِ وَلَا الْبَذِيءِ

Artinya: Seorang mukmin bukanlah orang yang banyak mencela, bukan orang yang banyak melaknat, bukan orang yang keji, dan bukan pula orang yang kotor omongannya. (HR. Tirmidzi)

Dari hadits di atas kebiasaan mencela dan menyebarkan semua yang didengar adalah perbuatan buruk yang dapat meningkatkan banyak risiko. Memberikan informasi yang salah termasuk dalam tindakan keji, dan menyebarkan hoaks tentunya adalah perbuatan dosa.[12] Maka dari itu, perlu adanya melakukan penanggulangan agar masyarakat tidak langsung percaya terhadap berita berita yang tidak jelas sumbernya.

Dengan memenuhi standar operasi minimum, sertifikat digital atau tanda tangan elektronik yang dikeluarkan oleh suatu domain Certificate Authority (CA) tertentu dapat diakui oleh pihak manapun yang juga mengakui standar tersebut.

Misalnya, dalam pengelolaan sertifikat, CA harus mematuhi standar minimal yang tercantum dalam Certificate Practice Statement (CPS).[13] Singapura masih menggunakan Model Hukum UNCITRAL dalam mengatur prosedur, model hukum ini memberikan kerangka legislatif yang transparan dan diterima secara internasional untuk menangani masalah, selain itu, dengan mengadopsi Model Hukum UNCITRAL, Singapura memperkuat posisinya sebagai pusat utama bagi rekonstruksi dan penyelesaian perdamaian internasional dengan memberikan keunggulan kompetitif dalam menarik lebih banyak investasi asing dan memberikan mekanisme

[11] Sirajuddin *"Berita Hoax Dalam Perspektif Al-Qur'an" hal. 34 tahun 2018*
[12] *Musri dan Putra "Hoax Dalam Tinjauan Hadits Nabawi"Hal. 161 Tahun 2018*
[13] Lestari, Electronic Signature Di Singapura

yang lebih efisien dalam menangani kasus kebangkrutan yang melibatkan berbagai tindakan.Undang-Undang ETA *(Electronic Transactions Act)* menetapkan kerangka hukum mengenai transaksi elektronik di Singapura.

ETA disahkan pada tahun 1998 dan dilakukan perubahan pada tahun 2021, Singapura menyetujui RUU Transaksi Elektronik di Parlemen pada tanggal 1 Juni 1998. RUU tersebut kemudian disahkan menjadi Undang-Undang Transaksi Elektronik (ETA) pada tanggal 10 Juli 1998. Pengalaman serupa terjadi di Hong Kong, di dimana pemerintah memperkenalkan RUU-nya kepada Dewan Legislatif pada tanggal 14 Juli 1999, dan pada tanggal 5 Januari 2000, Perintah Transaksi Elektronik (ETO) resmi diundangkan. RUU No. 23/98 Merujuk pada "RUU Transaksi Elektronik Tahun 1998" di Singapura. Undang-Undang Transaksi Elektronik (Electronic Transactions Act, ETA) Singapura telah direvisi sejak pengesahannya pada tahun 1998. Revisi signifikan terakhir terjadi pada tahun 2021, ketika Undang-Undang ini dimodifikasi untuk mengadopsi model hukum UNCITRAL.[14]

Baik Indonesia maupun Singapura menunjukkan komitmen yang kuat dalam melindungi masyarakat baik di dunia nyata maupun digital melalui berbagai langkah, termasuk meningkatkan transparansi, memberikan pendidikan kepada masyarakat, dan menerapkan aturan. Namun, Indonesia masih menghadapi tantangan dalam memperkuat upaya tersebut. Kedua negara juga aktif menjalin kerja sama internasional dengan sertifikasi elektronik, misalnya melalui pertukaran informasi dan pelaksanaan investigasi lintas negara.

Dengan demikian, penelitian tentang "Analisis Komparasi Sistem Hukum Di Bidang Sertifikasi Elektronik Antara Indonesia dan Singapura" menjadi sangat penting. penggunaan transaksi elektronik, komunikasi daring, dan pertukaran informasi sangat mendominasi kehidupan sehari-hari.[15] Sertifikasi elektronik

[14] Daniel Seng "The Singapore Electronic Transactions Act And The Hong Kong Electronictransactionsordinance," tahun 2008.*)*

[15] *(*Puji Purnama Sari, Syafaat Pradana, and Abdul Hafid 2025)

berperan sebagai fondasi dalam memastikan keamanan dan integritas data, sehingga risikonya bisa diminimalisir. Penelitian ini akan memberikan wawasan tentang bagaimana dua negara dengan sistem hukum yang berbeda, Indonesia dan Singapura, menangani sertifikasi elektronik. Indonesia dan Singapura memiliki sistem hukum yang berbeda dalam pendekatan terhadap sertifikasi elektronik. Indonesia, dengan undang-undang yang mengatur sertifikasi elektronik seperti UU ITE, dan Singapura dengan regulasi seperti Electronic Transactions Act (ETA), menawarkan dua perspektif yang berbeda mengenai tata cara pengaturan dan penerimaan tanda tangan elektronik serta sertifikasi elektronik. Memahami perbedaan ini penting untuk melihat apakah kedua sistem hukum ini efektif dalam konteks globalisasi dan transaksi lintas negara.

Sertifikasi elektronik menjadi kunci dalam membangun kepercayaan di dunia digital, terutama dalam transaksi e-commerce, pemerintahan elektronik, dan komunikasi digital. Penelitian ini akan memberikan gambaran bagaimana setiap negara mengatur mekanisme pengamanan ini, yang pada gilirannya dapat memengaruhi tingkat kepercayaan masyarakat terhadap transaksi elektronik di masing-masing negara. Mengingat bahwa banyak transaksi elektronik kini bersifat lintas negara, penting untuk mengkaji bagaimana kedua negara ini berkontribusi pada harmonisasi regulasi sertifikasi elektronik di tingkat internasional. Penelitian ini dapat menunjukkan area-area yang perlu diselaraskan atau dikembangkan lebih lanjut untuk mendukung kerjasama internasional dalam hal transaksi elektronik yang aman dan sah secara hukum.

Indonesia dan Singapura memiliki potensi ekonomi digital yang besar. Sertifikasi elektronik yang aman dan diakui secara hukum menjadi faktor penting dalam mengoptimalkan potensi ini. Melalui penelitian ini, bisa ditemukan apakah kebijakan hukum yang diterapkan di kedua negara dapat memfasilitasi pertumbuhan ekonomi digital secara maksimal, ataukah ada hambatan yang perlu diatasi. Penelitian ini akan memberikan masukan penting bagi pembuat kebijakan dan regulator di kedua negara dalam merumuskan kebijakan yang lebih baik dan lebih adaptif

terhadap perkembangan teknologi. Dengan mengetahui kekuatan dan kelemahan sistem yang diterapkan di masing-masing negara, kebijakan baru yang lebih efektif dapat dihasilkan.

Secara keseluruhan, penelitian ini penting untuk memperdalam pemahaman mengenai sistem hukum sertifikasi elektronik, serta untuk memberikan rekomendasi yang dapat meningkatkan efektivitas dan keamanan transaksi elektronik di Indonesia dan Singapura, serta secara global.

B. Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan di atas maka peneliti merumuskan masalah yang akan dijadikan topik pembahasan. Adapun rumusan masalah yang akan diteliti adalah sebagai berikut:

1. Bagaimana kedudukan sistem hukum di bidang Sertifikasi Elektronik antara Indonesia dan Singapura?
2. Apa faktor yang mempengaruhi adanya perbandingan sistem hukum di bidang Sertifikasi Elektronik antara Indonesia dengan Singapura?

C. Tujuan Penelitian

Adapun tujuan dari penelitian ini sebagai berikut:

1. Memahami kedudukan sistem hukum terhadap bidang Sertifikasi Elektronik termasuk relevansi undang-undang dengan standar internasional.
2. Memahami faktor yang mempengaruhi adanya perbedaan sistem hukum di bidang Sertifikasi Elektronik di Indonesia maupun Singapura.

D. Kegunaan Penelitian

Dari hasil penelitian ini diharapkan akan memberikan manfaat sebagai berikut:

1. Kegunaan Teoritis:
   a. Penelitian ini diharapkan dapatmenambah wawasan dan referensi dalam bidang Hukum Tata Negara dan kebijakan internasional, khususnya terkait Sertifikasi Elektronik.
   b. Penelitian ini diharapkan dapat memberikan sumbangan iliah dan pengembangan ilmu pengetahuan, terutama dalam kajian Sertifikasi Elektronik.
2. Kegunaan Praktis:
   a. Penelitian ini diharapkan dapat menjadi masukan bagi pemerintah pusat dalam menyusun kebijakan kebijakan terkait teknologi dan elektronik.
   b. Dapat menjadi model atau contoh bagi masyarakat dalam beraktivitas daring.

E. Definisi Istilah

Mengandung beberapa istilah penting yang perlu dipahami secara mendalam untuk memperjelas ruang lingkup dan fokus penelitian. Istilah pertama adalah *komparasi hukum*, yang mengacu pada metode studi perbandingan yang dilakukan untuk memahami persamaan dan perbedaan sistem hukum di dua negara atau lebih, dalam hal ini Indonesia dan Singapura. Tujuan dari komparasi hukum adalah untuk mengidentifikasi praktik terbaik, mengevaluasi efektivitas kebijakan, serta memberikan masukan terhadap pengembangan hukum nasional.

Selanjutnya, istilah *bidang sertifikasi elektronik* merujuk pada aspek hukum yang mengatur proses verifikasi dan otentikasi dokumen atau transaksi elektronik melalui penggunaan tanda tangan digital dan lembaga penyelenggara sertifikasi elektronik.

Sertifikasi ini menjadi bagian penting dari infrastruktur hukum dalam mendukung keamanan transaksi elektronik, khususnya dalam konteks e-commerce, administrasi pemerintahan digital, dan sistem informasi modern lainnya. Indonesia dan Singapura sebagai subjek komparasi dipilih karena keduanya merupakan negara yang telah memiliki regulasi terkait tanda tangan elektronik, namun dengan latar belakang sistem hukum yang berbeda—Indonesia menganut sistem hukum campuran dengan pengaruh kuat dari hukum Belanda (civil law), sementara Singapura menggunakan sistem hukum common law warisan Inggris. Perbedaan sistem hukum ini berpotensi mempengaruhi pendekatan regulatif, implementasi, dan efektivitas dari sertifikasi elektronik di masing-masing negara.

Adapun beberapa konsep dari masalah yang diteliti yang berguna untuk menghubungkan atau menjelaskan maksud dari judul penelitian ini dengan memberikan gambaran umum tentang istilah penelitian.

1. **Konsep Hukum Dalam Sertifikasi Elektronik**

   Aspek hukum pada sertifikasi elektronik meliputi kekuatan hukum untuk pembuktian yang setara. UNCITRAL *(United Nations Commission on International Trade Law)* merupakan salah satu organisasi internasional yang fokus pada perkembangan teknologi informasi terhadap perdagangan elektronik. Hasilnya merupakan *Model Law* yang bersifat tidak mengikat namun dapat menjadi acuan. Pada tanggal 16 Desember 1996 UNCITRAL mengeluarkan *Model Law On Electronic Commerce* yang disahkan oleh ketua PBB.[16] Negara Singapura mengadopsi undang-undang yang dikeluarkan oleh

[16] Ahmad Redi, Aspek Hukum Electronic Signature 4.1. Aspek Hukum Electronic Signature dalam Regulasi Internasional," tahun 2010

UNCITRAL berbeda dengan Indonesia. Di Indonesia, Setiap pelaku usaha yang menggunakan sistem elektronik yang mewajibkan menyediakan informasi lengkap dan akurat terkait syarat-syarat kontrak, identitas produsen, serta rincian produk yang ditawarkan untuk mendukung transaksi elektronik yang terpercaya (*trusted e-transactions*) sesuai dengan Pasal 9 Undang-Undang ITE. Selain itu, penyelenggaraan sistem elektronik oleh pelaku usaha harus disertifikasi oleh Lembaga Sertifikasi Keandalan sebagaimana diatur dalam Pasal 10 Undang-Undang ITE.Transaksi elektronik, baik di sektor publik maupun swasta, yang menggunakan sistem elektronik untuk pelayanan publik juga memerlukan Sertifikat Keandalan dan/atau Sertifikat Elektronik sesuai ketentuan Pasal 41 Peraturan Pemerintah (PP) No. 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE). Agar transaksi elektronik dapat berjalan dengan aman dan terpercaya, penyelenggara sistem elektronik harus memiliki sertifikat keandalan dan sertifikat elektronik, sebagaimana diatur dalam Pasal 41 dan 42 PP PSTE. Dalam peraturan tersebut, aspek seperti proses, kebijakan, manajemen, pendidikan, dan pelatihan juga menjadi perhatian dalam standar keamanan informasi. Namun, standar keamanan informasi yang dimaksud bukan hanya sekadar spesifikasi teknis yang mengatur teknologi atau produk tertentu, tetapi lebih kepada metode yang memungkinkan standar ini dapat diterapkan secara luas di berbagai sektor bisnis sebagai bagian dari perlindungan informasi.[17]

[17] Setiawan, Studi Standardisasi Sertifikat Elektronik dan Keandalan dalam Penyelenggaraan Sistem Transaksi Elektronik tahun 2015

2. Konsep Kepercayaan Digital

Tanggung jawab hukum timbul ketika seseorang melakukan tindakan yang merugikan hak orang lain atau tidak menjalankan kewajibannya dengan semestinya. Asas kepercayaan adalah prinsip yang menyatakan bahwa kepercayaan digital didasarkan pada hubungan saling percaya.[18] suatu perbuatan dapat dianggap sebagai pelanggaran yang harus dipertanggungjawabkan jika terdapat aturan tertulis yang menyatakan bahwa tindakan tersebut bertentangan dengan etika bisnis dan norma yang berlaku dalam masyarakat.[19] Kepercayaan digital dan sertifikasi elektronik adalah dua konsep penting dalam keamanan dan keabsahan interaksi digital, terutama dalam konteks transaksi elektronik, komunikasi daring, dan perlindungan data. Contoh pada Perencanaan strategi juga sangat penting bagi marketing funding dimana seorang marketing funding memiliki tugas dan tanggung jawab yang besar untuk terus meningkatkan jumlah nasabah pada suatu bank dengan melakukan pemasaran produk yaitu kepercayaan sehingga mampu untuk mencapai target yang telah ditentukan dan sebagai seorang pemasar yang kebanyakan waktunya dilakukan dilapangan harus mempunyai perencanaan strategi untuk dapat menunjang keberhasilan dalam mencapai target tujuan tersebut.[20]

---

[18] M.H. Dr. Zainal Said, *Polemik Undang-Undang Perbankan Indonesia Tinjauan Sosio Yuridis), Sustainability (Switzerland)*, 2019, XI <Http://Scioteca.Caf.Com/Bitstream/Handle/123456789/1091/RED2017-Eng-8ene.Pdf?Sequence=12&Isallowed=Y%0Ahttp://Dx.Doi.Org/10.1016/J.Regsciurbeco.2008.06.005%0Ahttps://Www.Researchgate.Net/Publication/305320484_SISTEM_PEMBETUNGAN_TERPUSAT_STRATEGI_MELESTARI>.

[19] Ditha Cindy Agustina, 'Fakultas Ekonomi Dan Bisnis Universitas Muhammadiyah', Riset, No. 02 (2020), Pp. 1–19.

[20] Hardiyanti Tahir, Zainal Said, and Marhani, 'Strategi Marketing Funding Dalam Meningkatkan Jumlah Nasabah Di Bank Bni Syariah Parepare', BANCO: Jurnal Manajemen Dan Perbankan Syariah, 3.2 (2022), pp. 85–100, doi:10.35905/banco.v3i2.2156.

Kepercayaan digital adalah rasa yakin atau keyakinan yang dimiliki seseorang terhadap sistem, layanan, atau pihak yang beroperasi di dunia digital. Ini mencakup keyakinan bahwa data pribadi mereka akan aman, identitas mereka tidak disalahgunakan, transaksi yang dilakukan tidak akan merugikan, serta pihak yang mereka ajak berinteraksi memang benar dan dapat dipercaya.

Kepercayaan ini terbentuk dari beberapa hal, seperti keamanan sistem, transparansi dalam penggunaan data, reputasi penyedia layanan, dan kepatuhan terhadap hukum atau regulasi yang berlaku. Misalnya, ketika seseorang berbelanja online, ia perlu merasa yakin bahwa situs tersebut aman, informasi kartu kreditnya tidak akan bocor, dan barang yang dibeli benar-benar akan dikirim sesuai pesanan. Semua keyakinan itu adalah bagian dari kepercayaan digital. Tanpa kepercayaan digital, orang akan ragu untuk menggunakan layanan online, mengisi data pribadi di formulir digital, atau bahkan sekadar membuka tautan dari email yang tidak dikenal. Maka dari itu, membangun dan menjaga kepercayaan digital menjadi hal yang sangat penting dalam dunia yang semakin terhubung secara daring.

3. Konsep Interoperabilitas (Pengakuan Antar Negara)

Pelaksanaan interoperabilitas menjadi sebuah solusi yang menarik, asalkan didukung oleh terpenuhinya syarat dan kondisi yang dibutuhkan.[21] Interoperabilitas adalah kemampuan dari sistem, aplikasi, atau perangkat yang berbeda untuk saling berkomunikasi, bertukar data, dan menggunakan informasi yang dipertukarkan

[21] Masfi Sya'fiatul Ummah, 'Implementasi Model Interoperabilitas Pada Sistem Informasi Akademik Berbasis Multi Platform Muhammad Faisal Program Studi Teknik Komputer STMIK Profesional Makassar Muh.Faisal.Art@gmail.Com', *Sustainability (Switzerland)*, 11.1 (2019), pp. 1–14 <http://scioteca.caf.com/bitstream/handle/123456789/1091/RED2017-Eng-8ene.pdf?sequence=12&isAllowed=y%0Ahttp://dx.doi.org/10.1016/j.regsciurbeco.2008.06.005%0Ahttps://www.researchgate.net/publication/305320484_Sistem Pembentuka.

secara efektif, meskipun mereka berasal dari pengembang atau platform yang berbeda.

Sertifikasi elektronik yang diterbitkan di Indonesia dapat digunakan di luar negeri, namun pengakuannya bergantung pada perjanjian dan standar yang berlaku di negara tujuan. Secara umum, sertifikat elektronik Indonesia diakui secara nasional dan memiliki kredibilitas tinggi di Indonesia. Namun, untuk pengakuan internasional, tergantung pada perjanjian atau kesepakatan dengan badan sertifikasi di negara lain. Untuk meningkatkan pengakuan internasional, pemerintah Indonesia telah mengambil langkah-langkah seperti bergabung dengan Konvensi Apostille pada tahun 2022. Melalui layanan Apostille, dokumen publik yang diterbitkan di Indonesia, termasuk yang berbentuk elektronik, dapat dilegalisasi dan diakui di 122 negara anggota Konvensi Apostille. Namun, perlu dicatat bahwa layanan Apostille hanya berlaku untuk dokumen publik, dan tidak semua jenis sertifikat elektronik termasuk dalam kategori ini, sama hal-nya dengan Singapura, Sertifikat elektronik yang diterbitkan di Singapura belum otomatis berlaku atau diakui secara sah di Indonesia, kecuali telah ada perjanjian timbal balik (mutual recognition agreement) atau mekanisme pengakuan khusus yang diatur oleh pemerintah Indonesia.

4. Konsep Komparasi Sistem Hukum Antara Indonesia dan Singapura

Indonesia dan Singapura perlu dibandingkan dari segi sistem hukum karena keduanya merupakan negara tetangga di kawasan Asia Tenggara yang memiliki latar belakang sejarah, budaya, dan sistem pemerintahan yang berbeda, tetapi memiliki hubungan yang erat secara ekonomi, sosial, dan politik.[22] Dengan melakukan

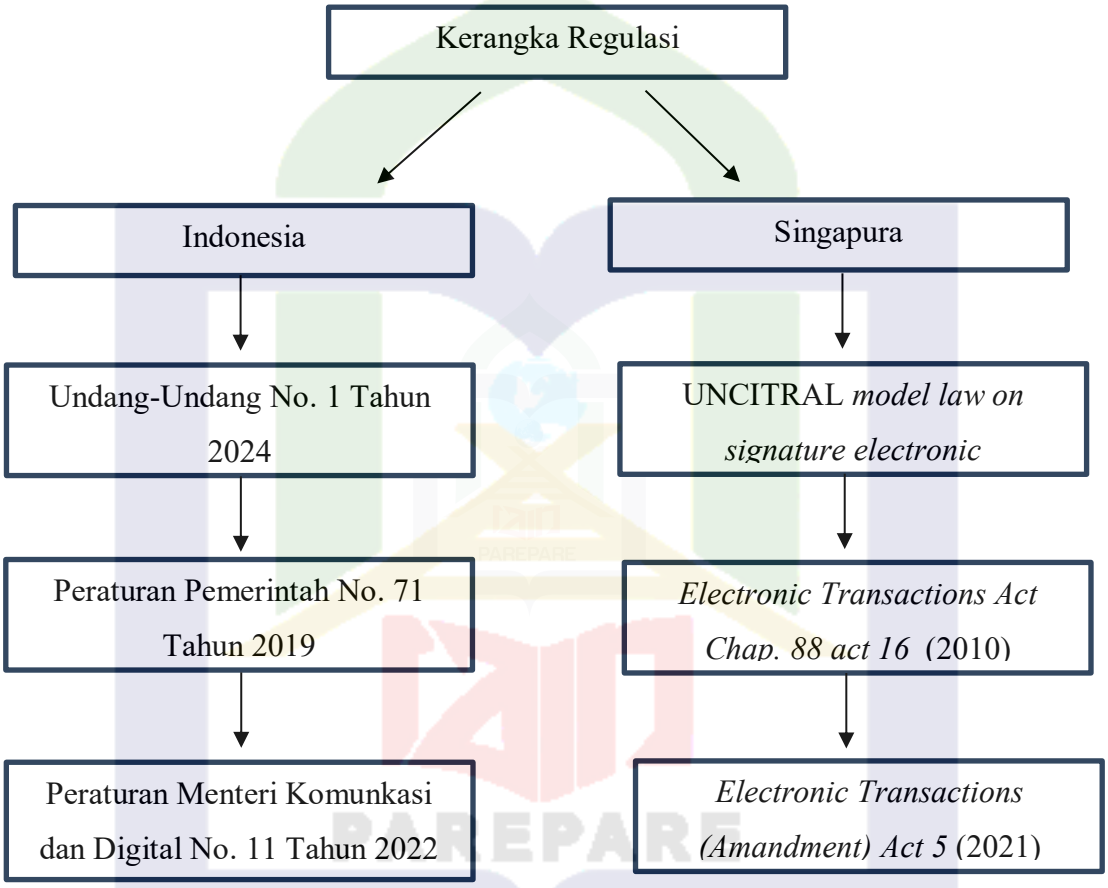
[22] M A Fathurrahman and L Husna, 'Perbandingan Hukum Indonesia Dan India Terhadap Penyelesaian Sengketa Arbitrase Secara Online', *UNES Law Review*, 5.4 (2023), pp. 4478–87 <https://review-unes.com/index.php/law/article/view/758>.

perbandingan sistem hukum antara Indonesia dan Singapura, kita dapat memperoleh berbagai manfaat penting, baik dari sisi akademik maupun praktis. Indonesia menganut sistem hukum civil law (berbasis hukum tertulis, dipengaruhi Belanda). Singapura menganut sistem hukum common law (berbasis preseden dan yurisprudensi, dipengaruhi Inggris). Letak geografis yang dekat juga menjadi alternatif, dan adanya pemicu semangat agar menjadi motivasi bagi penulis dikarena Singapura dianggap sebagai negara mau. Singapura juga termasuk dalam hukum internasional karena ia adalah negara berdaulat yang terlibat aktif dalam hubungan antarnegara, organisasi internasional, dan perjanjian global. Keikutsertaannya memperlihatkan bahwa hukum internasional tidak hanya berlaku untuk negara-negara besar, tetapi juga untuk negara manapun yang menjalin kerja sama global. Hukum internasional publik merupakan kumpulan norma dan prinsip hukum yang mengatur hubungan atau persoalan yang melampaui batas negara, namun tidak berkaitan dengan aspek perdata.[23]

[23] Hasanuddin Hasim, 'Hubungan Hukum Internasional Dan Hukum Nasional Perspektif Teori Monisme Dan Teori Dualisme', Mazahibuna Jurnal Perbandingan Mazhab, 1.2 (2019), pp. 166–79.

5. Kerangka Regulasi Sertifikasi Elektronik

Regulasi kerangka sertfikasi elektronik memberikan aturan, prosedur, dan standar teknik yang menjamin keabsahan dan kendala sertifikasi elektronik, Kerangka ini merupakan konseptual dari masalah yang ditelitii



Dengan demikian, secara keseluruhan, judul ini menunjukkan bahwa penelitian akan membandingkan secara hukum bagaimana Indonesia dan Singapura mengatur, mengimplementasikan, dan mengawasi sertifikasi elektronik sebagai bagian dari tata kelola digital mereka.

F. Tinjauan Penelitian Relevan

Penelitian terdahulu dimasukkan untuk menghindari kemiripan dengan penelitian ini, penelitian sebelumnya dimasukkan sebagai bahan perbandingan dan rujukan. Maka calon peneliti mencantumkan penilitian terkaait sebagai berikut:

Penelitian pertama karya skripsi Dadik Parifudin Universitas Muhammadiyah Yogyakarta 2009, dengan judul "Pembuktian Terhadap Tindak Pidana Pemalsuan Data Dalam Informasi Dan Transaksi Elektronik *(E-Commerce)*" terhadap proses pembelian barang, para pihak sering menghadapi berbagai masalah hukum, seperti validitas dokumen yang dihasilkan, tanda tangan digital yang digunakan untuk menyetujui transaksi, kekuatan mengikat kontrak, hingga Pembatalan transaksi. Salah satu isu utama dalam transaksi e-commerce adalah keamanan pembayaran dan risiko keamanan yang muncul selama proses transaksi. Permasalahan ini mencakup jaminan keabsahan dan perlindungan data dalam transaksi digital, yang menjadi perhatian penting untuk menciptakan kepercayaan antara pihak-pihak yang terlibat.

Persamaan pada penelitian ini dengan penelitian penulis sama-sama membahas tentang Sertifikasi Elektronik dan mengulik Undang-Undang No. 1 Tahun 2024 Tentang Informasi dan Transaksi Elektronik, adapun yang menjadi perbedaan ialah penelitian Dadik Parifudin seputar transaksi elektronik dengan menganalisis pembuktian tindak pidana dalam *(e-commarce)* sedangkan penelitian ini membahas lebih luas dengan Sertifikasi Elektronik yang mencakup keamanan bertransaksi, *digital signature*, dan juga kepercayaan terhadap situs Penyelenggara Sertifikasi Elektronik.

Penelitian Dadik Parifudin juga menyinggung *digital signature* yang berarti Tanda tangan digital sangat penting dalam dunia digital saat ini karena beberapa

faktor penting yang meningkatkan keamanan, integritas, dan kepercayaan transaksi dan komunikasi elektronik, tanda tangan digital memverifikasi identitas pengirim. Karena hanya pemegang kunci pribadi yang dapat membuat tanda tangan digital, tanda tangan digital memastikan bahwa orang atau entitas yang mengirim pesan atau dokumen benar-benar orang yang mereka klaim. Hal ini penting dalam transaksi e-commerce.

Penelitian kedua karya Skripsi oleh Ratno Tri Handoko Universitas Jember, tahun 2010, dengan judul Kekuatan Pembuktian Alat Bukti Elektronik Penelitian (Dokumen Dan Tanda Tangan Elektronik) Dalam Sengketa E-Commarce ini berusaha menganalisah mengenai masalah yang muncul dalam memastikan keaslian atau keotentikan informasi, mengingat kemudahan dalam menggandakan dokumen elektronik. Selain itu, timbul pertanyaan juga mengenai apakah hukum acara perdata di Indonesia masih relevan dengan perkembangan teknologi baru yang berkaitan dengan pembuktian dalam perkara hukum. Dengan pesatnya perkembangan teknologi, ada kebutuhan untuk menyesuaikan regulasi agar tetap dapat menjamin integritas dan keabsahan bukti-buktinya. Oleh karena itu, sangat penting untuk meneliti sejauh mana kekuatan pembuktian alat bukti elektronik dalam perlindungan *e-commerce.* Pertanyaan yang perlu dikaji dalam penelitian Ratno Tri Handoko ialah Lembaga Penyelenggara Sertifikasi Elektronik, sebagai pihak yang berwenang mengeluarkan Sertifikat Digital, memiliki tanggung jawab terhadap pihak ketiga yang merasa dirugikan dalam mengatur e-commerce.

Selain itu, penting juga untuk mengetahui apakah alat bukti elektronik memiliki kekuatan yang mengikat bagi hakim dalam memutuskan perlindungan e-commerce. Hal ini terkait dengan penerimaan dan pengakuan terhadap bukti

elektronik dalam proses hukum yang terus berkembang, serta perlunya regulasi yang jelas terkait dengan tanggung jawab lembaga sertifikasi dan penguatan alat bukti elektronik dalam penyelesaian.

Persamaan pada penelitian ini dengan penelitian Ratno Tri Handoko ialah membahas mengenai badan Penyelenggara Sertifikasi Elektronik penelitian pada skripsi Ratno Tri Handoko mencakup pembahasan kekuatan alat bukti sertifikasi elektronik pada sengketa *e-commarce,* penelitian ini terhubung dengan pembahasan "pembuktian keamanan" terhadap Penyelenggara Sertifikasi Elektronik dan pada penelitian ini membahas "kepercayaan" terhadap Penyelenggara Sertifikasi Elektronik maupun keamanan yang diberikan kepada masyarakat dalam sertifikasi elektronik, perbedaan penelitian ialah penelitian ini menganalisis kebijakan hukum ITE dua negara sedangkan penelitian Ratno Tri Handoko berfokus pada tanggung Jawab Badan Penyelenggara Sertifikasi Elektronik manakala terjadinya sengketa *e-commerce.*

G. Landasan Teori

1. Teori Perbandingan Hukum

a. Pengertian Perbandingan Hukum

Dalam Kamus Lengkap Bahasa Indonesia, disebutkan bahwa perbandingan ialah dari kata banding yaitu berarti persamaan, dan membandingkan yang mempunyai arti bahwa mengadu dua hal untuk diketahui bandingannya. Menurut Sjachran Basah perbandingan ialah metode mengkaji dan menyelidiki di antara dua objek yang dikaji, selanjutnya dalam konteks hukum tata negara, perbandingan hukum (*comparative law)* dilakukan agar dapat memahami persamaan dan perbedaan pada sistem ketatanegaraan dari berbagai negara. Proses ini bertujuan untuk

mengidentifikasi 1)struktur pemerintah, 2)membagikan kekuasaan seperti eksekutif, legislative, dan yudikatif, serta 3)membandingkan hak dan konstitusi. Perbandingan juga mencakup studi empiris mengenai pola pola yang mungkin serupa atau berbeda di berbagai negara. Perbandingan juga bertujuan untuk meningkatkan pemahaman mengenai kelebihan dan kekurangan sistem ketatanegaraan yang berbeda. Menurut Prof. Mirza Satria Buana, Guru Besar perbandingan Hukum Tata Negara dan Hak Asasi Manusia mengemukakan di dalam bukunya bahwasanya sejatinya perbandingan hukum merupakan wacana filsafat dikarena daikatkan dengan ontology, epistemology, dan aksiologi. konteks perbandingan hukum juga dimaknai dengan "mencipta" atau "mewujudkan sesuatu yang baru" dapat berarti upaya untuk memformulasi atau menyesuaikan aturan-aturan hukum yang baru dengan memanfaatkan ide-ide dari berbagai sistem hukum di dunia (*to produce shape, forge, realiza first something new, to find through the force of creative imagination)* secara keseluruhan, konsep tersebut menggambarkan bagaimana hukum bukan hanya tentang penerapan aturan yang ada, tetapi juga tentang kemampuan untuk berinovasi, menyesuaikan diri, dan menciptakan aturan yang relevan dengan kebutuhan masyarakat modern.[24] Perbandingan hukum sendiri juga menyasar pada 'budaya hukum' (*legal culture)* yang berarti bahwa studi perbandingan ini tidak hanya melihat perbedaan dan persamaan dalam teks hukum (seperti undang-undang atau peraturan) dari berbagai negara, tetapi juga mempertimbangkan bagaimana hukum tersebut diimplementasikan dan diterima dalam masyarakat. *Budaya hukum* mencakup nilai-nilai, kepercayaan, sikap, dan perilaku masyarakat terhadap hukum.Manfaat dari teori perbandingan hukum menurut Winerton juga suatu metode yang membandingkan sistem sistem hukum yang perbandingannya menghasilkan data yang layak dibandingkan. Dari

[24] Mirza Satrua Buana 2022 Perbandingan Hukum Tata Negara: Filsafat, Teori, dan Praktik. Disunting oleh Kurniawan Ahmad. Jakarta Timur: Sinar Grafika.)

penjelasan mengenai perbandingan hukum yang merupakan sistematis hukum dari dua atau lebih sistem hukum dengan memanfaatkan metode perbandingan, jadi Ketika terdapat sistem hukum lebih dari satu, dapat dibandingkan satu sama lain agar menemukan kesimpulan dari beberapa sudut pandang. Dan manfaat menurut Rane David dan Brierley juga dapat membantu mengembangkan pemahaman terhadap hubungan internasional, Adapun manfaat menurut Ade Maman Suherman yaitu negara dapat mengambil sikap yang tepat untuk melakukan hubungan hukum dengan negara yang berbeda system hukumnya.[25]

b. Landasan Teori Perbandingan

Di Indonesia, umunya perbandingan merupakan suatu bidang ilmu hukum dan merupakan metode penelitian secara sederhana untuk mengadakan identifikasi terhadap persamaan atau perbedaan diantara dua system hukum, hal ini diungkapkan oleh Soerjono Soekanto.[26] Tidak ada undang-undang khusus yang mengatur perbandingan hukum namun ini lebih karena konsep perbandingan hukum bersifat akademis daripada praktis atau normatif dalam konteks regulasi. Perbandingan hukum adalah metode yang digunakan untuk memahami bagaimana aturan hukum dari satu negara atau sistem berbeda dari aturan di negara lain. Ini biasanya dilakukan dalam studi atau penelitian hukum dan jarang berfungsi sebagai dasar pengaturan dalam sistem hukum nasional.

c. Tujuan Teori Perbandingan

Tujuan perbandingan hukum berdasar pada asal usul perkembangannya, dari teori penanggulangan tujuan perbandingan hukum meliputi sistem sistem hukum untuk melihat persamaan dan perbedaannya dalan rangka

[25] Safriani Jurisprudentie and Safriani 2018)

[26] Dr. Djoni Sumardi Gozali "Pengantar Perbandingan Sistem Hukum (Civil Law, Common Law, dan Hukum Adat)," 2020)

mengembangkan hukum itu sendiri. Namun jika dari sudut pragtimas semata mata bukan hanya mencari persamaan maupun perbedaan akan tetapi memperbaharui hukum.[27] Namum jika dari segi fungsional perbandingan hukum merupakan jawaban atas problem-problem salah satunya pada pembahasan penelitian ini. Adapun di Indonesia metode perbandingan digunakan dalam pembuatan Undang-Undang untuk membuat kebijakan dengan belajar dari pemahamaham negara atau sistem hukum lain, yang memastikan undang-undang itu dibuat efektif, relevan, dan dapat diterima oleh masyarakat.

Contohnya pada Perbandingan Perzinahan dalam UU No. 1 Tahun 2023 dengan Hukum Islam, saat UU No. 1 Tahun 2023 dibuat perbandingannya ditinjau dari Hukum Islam, seperti pada prinsip penerapan bahwasanya penerapan ini berfokus pada aspek perlindungan privat, artinya zina hanya diusut jika ada pihak yang dirugikan dan melaporkannya. Hukumnya bertujuan sebagai efek jera tetapi tidak terlalu berat. Sedangkan, pada hukum Islam Prinsipnya lebih menekankan pada pencegahan moral dan sosial, dengan hukuman yang keras untuk menjaga kesucian masyarakat dan menghindari fitnah. Proses pembuktiannya sangat ketat untuk menghindari tuduhan palsu (*qadzaf*). [28] Dapat dilihat bahwa perbandingan merupakan metode yang amat diperlukan dalam membentuk peraturan perundang-undangan.

2. Teori Negara Hukum

a. Pengertian Negara Hukum

Konsep negara hukum telah dirumuskan sejak zaman Yunani Kuno oleh para filsuf. Plato, melalui karyanya The Republic, berpendapat bahwa

[27] Dr. H. MD Shodiq Perbandingan Sistem Hukum, tahun 2023

[28] Wahyuningsih, Perbandingan Hukum Perzinahan dalam UU No. 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (KUHP) dengan Hukum Islam Article Abstract tahun 2023

negara ideal dapat diwujudkan untuk mencapai tujuan utama, yaitu kebaikan yang menjadi esensinya. Negara hukum yang berarti pemerintah dapat mencegah kemerosotan kekuasaan seseorang.[29] Konstitusionalisme melahirkan konsep Rechtsstaat yang berkembang di kalangan ahli hukum Eropa Kontinental dan Rule of Law yang dianut oleh ahli hukum Anglo-Saxon. Dalam konteks Indonesia, kedua konsep ini diterjemahkan sebagai Negara Hukum. Hal ini berarti bahwa negara, dalam menjalankan fungsinya, harus berlandaskan pada prinsip-prinsip hukum. Namun, konsep negara hukum tidak hanya terbatas pada hal tersebut. Negara hukum juga mengandung gagasan nomokrasi, yang secara etimologis berasal dari kata *nomos* yang berarti norma, dan *kratien* yang berarti kekuasaan.

Dengan demikian, istilah nomokrasi mengandung makna bahwa hukum menjadi landasan utama bagi setiap tindakan pemerintah maupun rakyat sebagai bagian dari negara yang menyeluruh. Ini menunjukkan bahwa pemimpin sejati dalam suatu negara adalah hukum itu sendiri.[30] Setiap negara memiliki karakteristik yang unik, sehingga konsep negara hukum disatu negara tidak dapat diterapkan secara langsung pada negara lain. Indonesia, dengan ideologi Pancasila, memiliki landasan untuk mewujudkan negara hukum yang mampu membawa kebahagiaan bagi rakyatnya jika diterapkan secara konsisten.[31]

[29] Negara Hukum Indonesia Kebalikan Nachtwachterstaat "Zulkarnain Ridlwan" Tahun 2012)

[30] *(*Made Ivani.vidyawertta Analisa Tentang Konsep Dan Teori Negara Hukum Di Indonesia tahun . 2023*)*

[31] MENGGAGAS Indonesia SEBAGAI NEGARA HUKUM YANG MEMBAHAGIAKAN RAKYATNYA Hamzani, tahun 2014

b. Landasan Teori Negara Hukum

Negara Kesatuan Republik Indonesia tentunya merupakan negara yang berlandaskan konsep negara hukum (*rechtsstaaf)*, bukan hanya kekuasaan semata *(machtstaaf).* Hal ini terdapat pada Pasal 1 Ayat (3) Undang-Undang Dasar 1945 "Negara Republik Indonesia adalah negara hukum" sesuai dengan UUD 1945, setiap warga negara berhak atas rasa aman dan bebas dari segala bentuk kejahatan. Dengan upaya yang dilakukan penegakan hukum diharapkan dapat menimbulkan ketertiban, keamanan, dan ketentraman di antara masyarakat. Adapun dijelaskan pada pasal 7 ayat (1) Undang-Undang Nomor 12 Tahun 2011 menyatakan bahwa Undang Undang Dasar Negara Republik Indonesia adalah hukum tertinggi, yang diatur pada peraturan perundang-undangan bahwa peraturan yang lebih rendah tidak dapat bertentangan dengan peraturan yang lebih tinggi. Dengan demikian, Kemerdekaan Kebangsaan Indonesia dituangkan dalam Undang-Undang Dasar Negara Indonesia.

Sebagai negara hukum, setiap tindakan yang dilakukan oleh penyelenggara negara dan warga negara harus mematuhi hukum yang berlaku. Inilah prinsip nomokrasi yang diterapkan dalam UUD 1945.[32] Menurut Jimly Ashidique, dalam konsep demokrasi terkandung prinsip-prinsip kedaulatan rakyat *(democratie),* sementara dalam konsep negara hukum terkandung prinsip-prinsip negara hukum *(nomocratie).* Kedua prinsip ini dijalankan secara bersamaan sebagai dua sisi dari satu mata uang. Paham negara hukum seperti ini dikenal dengan sebutan "negara hukum yang demokratis" *(democratische rechtsstaat)*, atau dalam bentuk konstitusional disebut sebagai *constitutional democracy*.

Sebutan ini merujuk pada negara yang menggabungkan prinsip hukum dan demokrasi secara seimbang. Gagasan tentang negara hukum

[32] Pusat Pancasila dan Konstitusi, 'Modul Pendidikan Negara Hukum Dan Demokrasi' tahun 2016

dibangun dengan mengembangkan sistem hukum yang fungsional dan berkeadilan. Sistem ini dikembangkan dengan menyusun supra struktur dan infrastruktur kelembagaan politik, ekonomi, serta sosial yang tertib dan teratur. Selain itu, negara hukum juga dibina melalui pembangunan budaya dan kesadaran hukum yang rasional dan impersonal dalam kehidupan bermasyarakat, berbangsa, dan bernegara.

c. Tujuan Teori Negara Hukum

Menurut Aristoteles, tujuan negara adalah mewujudkan kehidupan yang terbaik *(the best life possible),* yang hanya dapat dicapai melalui supremasi hukum. Hukum dianggap sebagai manifestasi dari kebijaksanaan kolektif masyarakat *(collective wisdom),* sehingga keterlibatan warga negara sangat penting dalam proses pembentukannya.[33] Menurut Aminuin Ilmar, Dalam konsep negara hukum, kekuasaan yang menjalankan pemerintahan harus berlandaskan pada kedaulatan hukum atau supremasi hukum, dengan tujuan utama untuk mewujudkan ketertiban hukum dalam penyelenggaraan pemerintahan. Pemerintahan yang didasarkan pada hukum akan menjamin perlindungan terhadap hak-hak dasar masyarakat, sehingga kepentingan antara pemerintah yang menjalankan kekuasaan negara dan rakyat sebagai pemilik negara dapat selalu sejalan atau sesuai.[34] Tujuan negara memiliki peranan yang sangat penting, sehingga beberapa negara mencantumkan tujuan negaranya dalam konstitusi mereka. Indonesia adalah salah satu negara yang mencantumkan tujuan negara dalam Pembukaan Undang-Undang Dasar 1945, yang merupakan dasar hukum negara Republik Indonesia. Setiap negara memiliki tujuan yang berbeda-

[33] Syafa'at Pradana "Legal Hermeneutic of Secondary Education in Indonesia: A Hermeneutical Approach" 2019

[34] Rais, Negara Hukum Indonesia: Gagasan Dan Penerapannya

beda, yang disesuaikan dengan latar belakang sejarah, budaya, dan pandangan hidup masing-masing. Hal ini menyebabkan perbedaan dalam menentukan cara mencapai tujuan negara, termasuk dalam menentukan sistem hukumnya.[35]

3. Teori Sistem Hukum

a. Pengertian Sistem Hukum

Sistem hukum adalah keseluruhan aturan hukum yang berlaku di suatu negara atau masyarakat, sistem hukum juga disebut dengan kerangka maupun struktur hukum, sistem hukum diatur dan diterapkan oleh lembaga-lembaga yang berwenang, seperti pengadilan, aparat penegak hukum, dan lembaga negara lainnya. Sistem hukum mencakup berbagai aspek, mulai dari pembentukan hukum, penerapan, hingga pengawasan agar hukum dapat ditegakkan secara adil dan sesuai dengan tujuan yang ingin dicapai. Indonesia dan Singapura merupakan negara yang berasal dari Asia Tenggara. Berbagai sistem hukum di dunia meliputi sistem hukum Eropa Kontinental, sistem hukum Anglo-Saxon, hukum Islam, hukum adat, serta sistem hukum Indonesia dan sistem lainnya.

Meskipun setiap masyarakat memiliki sistem hukum yang berbeda, tujuan yang ingin dicapai tetap sama, yaitu untuk mengatur aktivitas manusia dalam kehidupan bermasyarakat. Joseph Dainow menyatakan bahwa tujuan utama dari sistem hukum adalah untuk mengatur dan mengharmonisasi aktivitas manusia dalam masyarakat sebagai bagian dari budaya, peradaban, sejarah, dan kehidupan masyarakat tersebut.[36]

---

[35] Maleha Soemarsono, 'Negara Hukum Indonesia Ditinjau Dari Sudut Teori Tujuan Negara, 2007

[36] Syofyan Hadi, Mengkaji Sistem Hukum Indonesia (Kajian Perbandingan Dengan Sistem Hukum Lainnya) 1," Tahun 2016.)

b. Landasan Sistem Hukum

Landasan sistem hukum merujuk pada dasar atau fondasi yang menjadi pijakan dalam pembentukan dan pelaksanaan sistem hukum suatu negara. Landasan ini mencakup prinsip-prinsip dasar, nilai-nilai, dan norma-norma yang memengaruhi bagaimana hukum dibuat, diterapkan, dan ditegakkan. Sistem hukum yang dirancang harus mendapatkan dukungan luas dari masyarakat (kesadaran hukum). Dengan kata lain, landasan sistem hukum secara terstruktur mencakup seperti aspek hukum dan prosedur substantif, kelembagaan, termasuk pejabat terkait, mekanisme kerja lembaga hukum, serta infrastruktur pendukung yang diperlukan, tingkat kesadaran dan budaya hukum masyarakat yang berperan sebagai subjek hukum.[37]

c. Tujuan Sistem Hukum

Sistem hukum bertujuan menciptakan kesadaran hukum, lebih mudahnya bertujuan untuk menumbuhkan dan mengembangkan masyarakat dan tentunya negara. Sistem hukum menjaga hukum sesuai dengan prinsip keadilan dan nilai-nilai yang hidup dalam masyarakat, dalam menjalankan sistem hukum, negara membentuk badan peradilan sebagai sarana untuk menyelesaikan permasalahan hukum..[38]

4. Teori Efektivitas Hukum

a. Pengertian Efektivitas Hukum

Teori efektivitas hukum berfokus pada evaluasi apakah suatu peraturan hukum dapat berfungsi sebagaimana mestinya dalam mengatur

[37] Evandy, Barlian, Dan Permata Herista, Urnal Lembaga Ketahanan Nasional Republik Indonesia Pembangunan Sistem Hukum Indonesia Berdasarkan Nilai-Nilai Pancasila Sebagai Ideologi Politik Bangsa (Development Of Indonesian Legal System Based On Pancasila Values As A Nation Political Ideology)

[38] Ekawati, Model of the Indonesian Legal System 2023

perilaku masyarakat, mencapai tujuan legislatif, dan menghasilkan dampak yang diinginkan. Menurut Soerjono Soekanto, seorang ahli sosiologi hukum Indonesia, efektivitas hukum ditentukan oleh sejauh mana hukum tersebut dipatuhi, diterapkan, dan menghasilkan perubahan perilaku sesuai dengan maksud pembuat undang-undang. Efektivitas hukum tidak hanya bergantung pada substansi hukum, tetapi juga pada faktor pendukung seperti kelembagaan, infrastruktur, dan penerimaan masyarakat. Menurut Hans Kelsen, pembahasan tentang efektivitas hukum tidak terlepas dari konsep validitas hukum. Validitas hukum mengacu pada sifat mengikatnya norma-norma hukum, yang mewajibkan individu untuk bertindak sesuai dengan ketentuan norma tersebut serta mematuhi dan melaksanakannya. Sementara itu, efektivitas hukum merujuk pada kenyataan bahwa individu benar-benar mematuhi dan menerapkan norma-norma hukum tersebut dalam perilaku mereka, sehingga norma-norma tersebut benar-benar berlaku dan dijalankan sesuai dengan yang diharuskan.

Menurut teori efektivitas hukum Soerjono Soekanto, hukum sebagai kaidah merupakan pedoman yang mengatur perilaku atau tindakan yang dianggap sesuai. Pendekatan berpikir yang digunakan adalah deduktif-rasional, yang cenderung menghasilkan pola pikir dogmatis. Sebaliknya, ada pandangan yang memahami hukum sebagai pola perilaku yang teratur dan konsisten (ajeg). Dalam pandangan ini, metode berpikir induktif-empiris digunakan, sehingga hukum dipandang sebagai tindakan yang berulang dalam bentuk yang sama dengan tujuan tertentu.

Efektivitas hukum dalam kenyataan atau praktik dapat dinilai dari keberhasilan atau kegagalan suatu kaidah hukum dalam mencapai tujuannya. Hal ini biasanya terlihat dari kemampuan kaidah tersebut untuk mengatur perilaku atau tindakan masyarakat sesuai dengan tujuan yang diinginkan. Dengan kata lain, efektivitas hukum diukur berdasarkan sejauh mana tujuan hukum tercapai. Salah satu cara untuk mendorong kepatuhan

masyarakat terhadap kaidah hukum adalah dengan menetapkan sanksi, yang dapat berupa sanksi negatif (hukuman) atau sanksi positif (penghargaan).[39] Untuk memastikan hukum dapat memengaruhi sikap, tindakan, atau perilaku manusia, diperlukan pemenuhan sejumlah kondisi tertentu. Salah satu kondisi utama adalah hukum harus dapat dikomunikasikan dengan baik. Komunikasi hukum terutama ditujukan untuk membentuk sikap, karena sikap mencerminkan kesiapan mental seseorang yang cenderung memberikan pandangan positif atau negatif, yang pada akhirnya termanifestasi dalam perilaku nyata. Jika komunikasi hukum tidak mampu menjangkau atau menangani masalah-masalah yang langsung dihadapi oleh targetnya, maka akan muncul berbagai kendala. Akibatnya, hukum tersebut bisa jadi tidak memiliki pengaruh sama sekali atau bahkan menimbulkan dampak negatif. Hal ini terjadi karena kebutuhan masyarakat tidak terpenuhi atau tidak dipahami, sehingga dapat memicu frustrasi, tekanan, atau bahkan konflik.

Efektivitas hukum memiliki keterkaitan yang sangat erat dengan penegakan hukum.[40] Untuk mencapai efektivitas hukum, diperlukan kehadiran aparat penegak hukum yang bertugas melaksanakan sanksi. Sanksi tersebut dapat diwujudkan dalam bentuk kepatuhan masyarakat (compliance), dan kondisi ini menjadi indikator bahwa hukum tersebut efektif. Budaya hukum merupakanaspek yang bersifat internal masyarakat, yaitu meliputi kesadaran dan pemahaman kolektif masyarakat atas suatu hukum sehingga hukum dilaksanakan dalam kehidupan se-hari-hari sebagai bagian dari rutinitas kegiatan di masyarakat. Oleh karena itu, berdasarkan perspektif dari Lawrence M. Friedman, sistem hukum yang baik adalah sistem hukum yang mampu mewujudkan substansi,

[39] Galih Orlando, 'Efektivitas Hukum Dan Fungsi Hukum Di Indonesia', *Jurnal Pendidikan Agama Dan Sains*, 6 (2022), pp. 50–58 <https://www.ejurnal.stita.ac.id/index.php/TBQ/article/download/77/70>.

[40] Lalu M. Alwin Ahadi, 'Efektivitas Hukum Dalam Perspektif Filsafat Hukum: Relasi Urgensi Sosialisasi Terhadap Eksistensi Produk Hukum', Jurnal Usm Law Review, 5.1 (2022), p. 110, doi:10.26623/julr.v5i1.4965.

struktur, dan budaya hukum yang optimal.Sistem hukum sebagaimana yang dijelaskan oleh Lawrence M. Friedman sejatinya berkaitan dengan keberlakukan hukum di masyarakat. Tidak optimalnya salah satu unsur dalam sistem hukum dapat mempengaruhi keberlakuan hukum di masyarakat. Maka, keberlakuan hukum di masyarakat tidak hanya berkaitan dengan aspek hukum secara internal yang dalam istilah disebut sebagai substansi hukum (legal substance). Keberlakuan hukum di masyarakat juga memerlukan struktur hukum dan budaya hukum sehingga dalam keberlakuannya hukum memerlukan bantuan dari berbagai aspek dalam mewujudkan tujuannya.

b. Landasan Efektivitas Hukum

Landasan efektivitas hukum merujuk pada dasar-dasar atau prinsip-prinsip yang menjadi fondasi agar suatu peraturan hukum dapat berjalan secara efektif dalam mengatur perilaku masyarakat dan mencapai tujuan yang diharapkan.. Landasan efektivitas hukum mencakup validitas norma, substansi hukum yang relevan, penegakan hukum, komunikasi yang efektif, kepatuhan masyarakat, dukungan infrastruktur, dan kesesuaian dengan budaya. Ketujuh landasan ini saling berkaitan untuk memastikan hukum dapat mengatur perilaku masyarakat secara efektif dan mencapai tujuannya. Dalam konteks sertifikasi elektronik, landasan ini menjadi kunci untuk mengevaluasi keberhasilan implementasi hukum di Indonesia dan Singapura.

Masyarakat yang cerdas hukum adalah masyarakat yang memiliki pemahaman menyeluruh tentang hukum, termasuk hak dan kewajiban mereka. Mereka mengetahui apa yang diperbolehkan dan dilarang, serta memahami manfaat dan risiko dari tindakan hukum yang mereka lakukan. Dengan sikap teliti dan hati-hati dalam mengambil langkah hukum, mereka mampu menghindari tindakan yang dapat menyebabkan pelanggaran hukum. Membangun budaya hukum merupakan upaya untuk melibatkan

masyarakat dalam meningkatkan efektivitas penegakan hukum. Mengembangkan nilai, sikap, dan perilaku yang mendukung pemahaman dan kepatuhan terhadap hukum sangat penting untuk membentuk budaya hukum. Budaya hukum dapat dikembangkan melalui berbagai cara, seperti memberikan edukasi hukum kepada masyarakat, menanamkan sikap patuh hukum sejak dini, dan melibatkan masyarakat dalam kegiatan sosialisasi hukum, sehingga terwujud masyarakat yang adil dan taat hukum melalui pembentukan budaya hukum ini.[41]

c. Tujuan Efektivitas Hukum

Tujuan efektivitas hukum adalah untuk memastikan bahwa peraturan hukum dapat berfungsi secara optimal dalam mengatur perilaku masyarakat, mencapai tujuan yang telah ditetapkan oleh pembuat hukum, dan memberikan manfaat bagi kehidupan bermasyarakat. Tujuan efektivitas hukum adalah untuk memastikan hukum dapat mengatur perilaku masyarakat sesuai tujuan pembuatnya, mendorong kepatuhan, menciptakan keadilan, mencegah pelanggaran, membangun budaya hukum, dan menjaga stabilitas sistem hukum. Dalam konteks sertifikasi elektronik, tujuan ini diwujudkan melalui pengakuan hukum, keamanan transaksi, dan peningkatan kepercayaan masyarakat terhadap teknologi digital. Pemahaman dan pengetahuan mengenai hukum serta peranannya dalam kehidupan sehari-hari, yang dimiliki oleh individu atau masyarakat, disebut sebagai kesadaran hukum. Secara umum, tingkat kesadaran hukum di masyarakat Indonesia masih tergolong rendah. Salah satu upaya untuk mengatasi minimnya pengetahuan hukum, yang dipengaruhi oleh berbagai faktor termasuk kurangnya pemahaman tentang ketentuan hukum, adalah

[41] Intan Dila Safitri, 'Dinamika Masyarakat Dalam Meningkatkan Efektivitas Penegakan Hukum', *Socius: Jurnal Penelitian Ilmu-Ilmu Sosial*, 1 (2024), pp. 83–88 <https://ojs.daarulhuda.or.id/index.php/Socius/article/view/145%0Ahttps://ojs.daarulhuda.or.id/index.php/Socius/article/download/145/145>.

dengan meningkatkan kesadaran masyarakat melalui penanaman nilai-nilai budaya hukum melalui pendidikan.

Pada intinya, sosiologi hukum dan efektivitas hukum memiliki keterkaitan yang sangat erat. Hal ini disebabkan karena kajian sosiologi hukum selalu berkaitan dengan penilaian sejauh mana hukum dapat berfungsi secara efektif di tengah masyarakat sebagai bagian dari fenomena sosial.[42]

5. Teori Sistem Teknologi dan Informasi

a. Pengertian Sistem Teknologi dan Informasi

Teori Sistem Teknologi dan Informasi (Information Systems Theory) adalah kerangka teoritis yang digunakan untuk memahami, menganalisis, dan mengelola interaksi antara teknologi informasi, manusia, dan organisasi dalam suatu sistem untuk mencapai tujuan tertentu. Teori ini berfokus pada bagaimana teknologi informasi, seperti perangkat keras, perangkat lunak, data, jaringan, dan prosedur, berinteraksi dengan pengguna dan konteks sosial untuk mendukung proses, pengambilan keputusan, dan pencapaian efisiensi atau efektivitas dalam suatu sistem.[43] Penerapan Teori Sistem Teknologi dan Informasi dalam konteks hukum sertifikasi elektronik adalah untuk memahami, menganalisis, dan mengoptimalkan interaksi antara teknologi informasi, manusia, dan kebijakan hukum guna mendukung efektivitas, keamanan, dan keandalan sistem sertifikasi elektronik. teori ini memastikan bahwa infrastruktur teknologi, seperti Public Key Infrastructure (PKI), yang digunakan dalam

[42] Mohd. Yusuf and others, 'Tinjauan Yuridis Faktor-Faktor Yang Mempengaruhi Efetivitas Penegakan Hukum Di Masyarakat', *JPin: Jurnal Pendidik Indonesia*, 5.2 (2022), pp. 1–9 <http://jurnal.intancendekia.org/index.php/JPIn/article/view/369>.

[43] Faldin Fahza Alfaizi, Yesi Airohmah, and Bakti Fatwa Anbiya, 'Analisis Konsep, Teori Teknologi Informasi Dan Implikasinya Dalam Pengembangan Teknologi Pembelajaran PAI Di Indonesia: Sistematik Literatur Riview', *Jurnal Sosial Teknologi*, 3.11 (2023), pp. 931–43, doi:10.59188/jurnalsostech.v3i11.985.

sertifikasi elektronik dapat menjamin autentikasi, integritas, dan kerahasiaan data dalam transaksi elektronik. Misalnya, di Indonesia, UU ITE dan PP PSTE mengatur penggunaan PKI oleh BSrE, sedangkan di Singapura, ETA mendukung standar keamanan internasional seperti ISO/IEC 27001. Tujuan teori sistem teknologi dan informasi dalam hukum sertifikasi elektronik adalah untuk mengoptimalkan interaksi antara teknologi, manusia, dan regulasi hukum guna menciptakan sistem yang aman, andal, efisien, dan sesuai dengan kebutuhan masyarakat. Dalam konteks Indonesia dan Singapura, teori ini membantu mengatasi tantangan seperti literasi digital rendah di Indonesia atau memanfaatkan keunggulan teknologi di Singapura untuk mendukung ekosistem transaksi elektronik yang terpercaya.

b. Landasan Sistem Teknologi dan Informasi

landasan teori sistem informasi dan teknologi (SIT) mencakup konsep-konsep dasar yang menjelaskan bagaimana sistem informasi dirancang, dikembangkan, dan digunakan untuk mendukung proses organisasi dengan memanfaatkan teknologi. Landasan teori SIT berfokus pada bagaimana teknologi informasi dapat diintegrasikan dengan proses organisasi untuk menciptakan nilai. Teori-teori seperti TAM, DOI, dan prinsip desain sistem memberikan kerangka untuk memahami, merancang, dan mengimplementasikan sistem informasi yang efektif dan efisien. Teknologi informasi merujuk pada perangkat keras, perangkat lunak, dan sumber daya manusia (useware) serta sistem dan metode yang digunakan untuk mengumpulkan, mengirim, memproses, menafsirkan, menyimpan, mengelola, dan memanfaatkan data secara efektif dan bermakna. Landasan teori sistem informasi dan teknologi yang paling umum pada dasarnya adalah kumpulan konsep dan kerangka kerja yang menjelaskan cara sistem informasi dirancang, diimplementasikan, dan digunakan untuk mendukung

kebutuhan organisasi dengan memanfaatkan teknologi. Intinya, teori-teori ini berusaha memahami bagaimana teknologi, manusia, dan proses bisa bekerja sama secara harmonis untuk mengelola informasi secara efektif.

Salah satu landasan yang sering dipakai adalah teori sistem, yang melihat sistem informasi sebagai sebuah kesatuan yang terdiri dari input, proses, output, dan umpan balik. Konsep ini membantu menjelaskan bagaimana data masuk, diolah oleh teknologi, dan menghasilkan informasi yang berguna untuk pengambilan keputusan. Misalnya, sebuah perusahaan memasukkan data penjualan, sistem mengolahnya, dan menghasilkan laporan yang membantu manajer membuat strategi. Jadi, secara umum, landasan teori ini berputar di sekitar bagaimana teknologi dan informasi bisa bekerja sama dengan manusia untuk menciptakan nilai, baik itu lewat efisiensi, keputusan yang lebih baik, atau adopsi yang sukses.[44]

c. Tujuan Sistem Teknologi dan Informasi

Tujuan sistem informasi dan teknologi (SIT) adalah untuk mendukung dan meningkatkan efisiensi, efektivitas, serta produktivitas dalam pengelolaan informasi di berbagai bidang, terutama dalam organisasi. Lebih jauh, SIT bertujuan untuk memberikan keunggulan kompetitif dengan memanfaatkan data untuk analisis strategis, seperti memahami tren pasar atau perilaku pelanggan melalui analitik big data. SIT juga berperan dalam menjaga keamanan informasi, memastikan data terlindungi dari ancaman siber. Pada akhirnya, SIT dirancang untuk mendukung inovasi, mempermudah adaptasi terhadap perubahan, dan menciptakan nilai tambah bagi organisasi, pengguna, serta masyarakat secara keseluruhan. Teknologi informasi berfungsi sebagai penghubung yang memediasi hubungan antara

[44] Bambang Warsita Bambang Warsita, 'Landasan Teori Dan Teknologi Informasi Dalam Pengembangan Teknologi Pembelajaran', *Jurnal Teknodik*, XV (2014), pp. 84–96, doi:10.32550/teknodik.v0i0.91.

karakteristik lingkungan dengan struktur organisasi.[45] Teknologi informasi berfungsi sebagai penghubung yang memediasi hubungan antara karakteristik lingkungan dengan struktur organisasi.

6. Teori keamanan Informasi dan Identitas digital

a. Pengertian keamanan Informasi dan Identitas digital

Keamanan informasi adalah upaya untuk melindungi data dan informasi dari ancaman seperti akses tidak sah, perubahan, pencurian, atau kerusakan, baik dalam bentuk digital maupun non-digital. Tujuannya adalah menjaga kerahasiaan (confidentiality), integritas (integrity), dan ketersediaan (availability) informasi, yang dikenal sebagai prinsip CIA Triad.[46] Dalam konteks teknologi, keamanan informasi melibatkan penggunaan alat seperti enkripsi, firewall, dan sistem autentikasi untuk memastikan data hanya diakses oleh pihak yang berwenang, tetap utuh tanpa manipulasi, dan tersedia saat dibutuhkan. dentitas digital adalah representasi elektronik dari individu, organisasi, atau entitas dalam sistem digital, yang digunakan untuk mengidentifikasi dan mengotentikasi keberadaan mereka di dunia maya. Identitas ini bisa berupa informasi seperti nama pengguna, kata sandi, alamat email, sertifikat digital, atau data biometrik (seperti sidik jari atau pengenalan wajah). Identitas digital memungkinkan verifikasi saat mengakses layanan online, seperti login ke aplikasi atau menandatangani dokumen elektronik. Dalam konteks hukum, keamanan informasi dan identitas digital memiliki peran penting untuk memastikan kepatuhan terhadap regulasi, melindungi hak privasi, dan mendukung keabsahan transaksi atau bukti digital dalam sistem hukum,

[45] Yusuf and others, 'Tinjauan Yuridis Faktor-Faktor Yang Mempengaruhi Efetivitas Penegakan Hukum Di Masyarakat'.

[46] Fitriah Agustika and others, 'Telaah Teknologi Informasi Dan Sistem Informasi Dalam Organisasi Dengan Lingkungan', *Jurnal Bisnis Kolega*, 9.1 (2023), pp. 24–33, doi:10.57249/jbk.v9i1.104.

Keamanan informasi dalam hukum berfokus pada perlindungan data sensitif agar sesuai dengan peraturan yang berlaku, seperti Undang-Undang Perlindungan Data Pribadi (UU PDP) di Indonesia, Identitas digital dalam hukum merujuk pada representasi elektronik yang diakui secara hukum untuk mengidentifikasi individu atau entitas dalam transaksi atau interaksi digital. Dalam sistem hukum, identitas digital harus divalidasi dengan mekanisme seperti tanda tangan elektronik yang diatur dalam UU ITE (Undang-Undang Informasi dan Transaksi Elektronik) di Indonesia. Keamanan informasi adalah langkah-langkah untuk menjaga aset informasi dari berbagai ancaman. Secara tidak langsung, keamanan informasi mendukung kelancaran operasional bisnis, meminimalkan risiko yang timbul, dan memungkinkan optimalisasi keuntungan dari investasi.[47]

b. Landasan Kemanan Informasi dan Identitas Digital

Teknologi informasi adalah cabang ilmu yang mencakup teknologi komunikasi untuk mengolah, menyimpan, dan mengirimkan informasi melalui saluran komunikasi yang efisien dan cepat. Berdasarkan Undang-Undang Nomor 19 Tahun 2016, yang mengubah Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), teknologi informasi didefinisikan sebagai teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisis, dan/atau mendistribusikan informasi. Teknologi informasi bermanfaat sebagai sumber dan alat pencarian informasi yang dibutuhkan, sebagai media yang mempermudah penyampaian informasi agar mudah diterima dan dipahami, serta sebagai sarana untuk mengembangkan keterampilan

[47] Shinta Nurul, Shynta Anggrainy, and Siska Aprelyani, 'Faktor-Faktor Yang Mempengaruhi Keamanan Sistem Informasi: Keamanan Informasi, Teknologi Informasi Dan Network (Literature Review Sim)', Jurnal Ekonomi Manajemen Sistem Informasi, 3.5 (2022), pp. 564–73, doi:10.31933/jemsi.v3i5.992.

pembelajaran dan keterampilan berbasis teknologi informasi melalui berbagai aplikasi.[48]

c. Tujuan Keamanan Informasi dan Identitas Digital

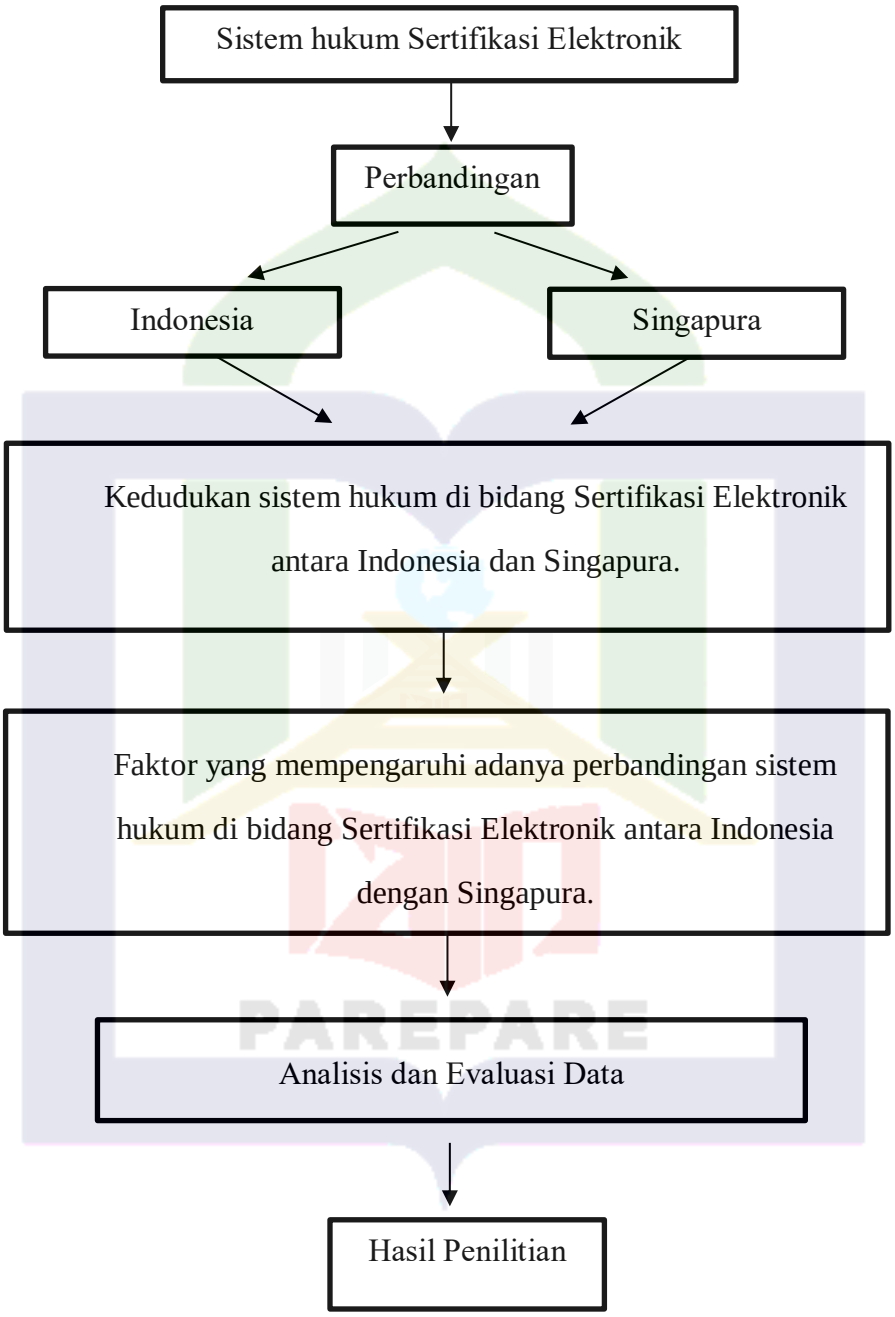
Tujuan keamanan informasi dan identitas digital dalam konteks hukum dan umum adalah untuk melindungi data serta memastikan kepercayaan, keabsahan, dan kelancaran dalam interaksi digital. Keamanan informasi bertujuan untuk menjaga kerahasiaan, integritas, dan ketersediaan data agar terhindar dari ancaman seperti peretasan, kebocoran, atau manipulasi. Dalam hukum, ini berarti memastikan data sensitif, seperti dokumen kontrak atau informasi pribadi, terlindungi sesuai regulasi, misalnya UU Perlindungan Data Pribadi atau UU ITE di Indonesia. Tujuannya adalah mencegah kerugian finansial, reputasi, atau hukum, seperti denda akibat pelanggaran privasi, sekaligus mendukung kelangsungan bisnis dengan mengurangi risiko siber. Keamanan informasi juga memastikan bukti digital tetap sah di pengadilan, misalnya melalui enkripsi atau audit log, sehingga mendukung penegakan hukum. **Identitas digital** bertujuan untuk menyediakan representasi elektronik yang sah dan terpercaya untuk mengidentifikasi individu atau entitas dalam transaksi digital. Dalam konteks hukum, identitas digital, seperti tanda tangan elektronik atau sertifikat digital, digunakan untuk memastikan keabsahan dokumen atau transaksi, seperti kontrak online, sesuai UU ITE. Tujuannya adalah mencegah penipuan identitas, memastikan otentikasi yang kuat, dan memberikan kepastian hukum dalam interaksi digital, seperti e-commerce atau komunikasi resmi. Identitas digital juga mendukung interoperabilitas

[48] Nabilla Zahra, Recca Ayu Hapsari, and Melisa Safitri, 'Perlindungan Hukum Teknologi Identitas Digital Melalui Sistem Verifikasi Identitas Berbasis Biometrik', *Supremasi: Jurnal Pemikiran Dan Penelitian Ilmu-Ilmu Sosial, Hukum, & Pengajarannya*, XIX.1 (2024), pp. 86–98.

global, memungkinkan verifikasi identitas lintas negara, yang penting untuk perdagangan atau kerja sama internasional.

Secara keseluruhan, keamanan informasi dan identitas digital bertujuan untuk menciptakan ekosistem digital yang aman, patuh hukum, dan efisien, sehingga meningkatkan kepercayaan, mengurangi risiko, dan mendukung keabsahan hukum serta operasional organisasi.

H. Kerangka Pikir



I. METODE PENELITIAN

A. Pendekatan dan Jenis Penelitian

Penelitian ini terkait tentang Analisis Komparasi Hukum Di Bidang Sertifikasi Elektronik Antara Indonesia Dan Singapura yang merupakan penelitian studi kepustakaan (*library research)*. Metode penelitian digunakan dalam menggambarkan semua proses yang dilalui oleh peneliti dalam mengumpulkan, menganalisis, serta menafsirkan data sehingga mampu memperoleh temuan dalam penelitian. Adapun dalam penulisan penelitian ini penulis merujuk pada pedoman Penulisan Karya Ilmiah yang diterbitkan oleh IAIN Parepare tahun 2020, dan juga pedoman ilmiah lainnya

Penelitian ini menganalisis sumber data *library research* dan penelitian normatif yang bersumber dari norma, undang-undang, asas hukum. Dan data data kepustakaan, dan dibantu dengan referensi dari buku-buku, website internet yang terverifikasi, jurnal-jurnal, serta karya ilmiah. Penelitian merujuk Sertifikasi Elektronik Antara Indonesia Dan Singapura. Jenis penelitian ini adalah yuridis normatif, sebab penelitian ini berdasar pada peraturan undang-undang dan peristiwa yang terjadi di Masyarakat dan norma-norma hukum tertulis. Penelitian ini tidak melakukan observasi lapangan, jadi tidak mengumpulkan data empiris. Yuridis normatif biasanya diapakai dalam penelitian bidang hukum seperti pada penelitian ini. Adapun jenis lainnya yaitu studi literatur dengan metode mengumpulkan data pustaka, membaca, serta mencatat dan mengolah bahan penelitian. Studi kepustakaan juga menentukan dugaan sementara atau hipotetis penelitian. Oleh sebab itu, penulis dapat mengelompokkan, mengalokasikan, mengorgansisasikan, dan tentunya

menggunakan varisasi pustaka pada penelitian kali ini.[49] menggunakan penelitian jenis pustaka juga lebih efektif. Pendekatan kualitatif dalam penelitian ini berfokus pada pemahaman mendalam terhadap fenomena, kebijakan, dan pengalaman terkait. Pendekatan kualitatif Penelitian dilakukan dalam konteks nyata tanpa mengintervensi situasi atau kondisi.[50] Peneliti memahami proses, kebijakan, dan institusi dalam penggunaan sertifikasi elektronik, observasi dilakukan dalam konteks kebijakan pemerintah terkait UU ITE dan edukasi literasi digital oleh Kominfo dan tentunya situs *https://sso.agc.gov.sg*/. Perbedaannya terletak pada sumber data atau informasi yang digunakan sebagai bahan penelitian. Pendekatan ini tidak memerlukan pengumpulan data primer melalui wawancara, observasi, atau survei, melainkan menitik beratkan pada pengolahan dan analisis kritis terhadap sumber.[51]

Berdasarkan kajian pustaka, variabel-variabel yang digunakan dalam penelitian ini adalah sebagai berikut:

1. Variabel Bebas (Independent Variable)

   Variabel bebas adalah variabel yang memengaruhi atau menyebabkan perubahan pada variabel terikat (dependen). Dalam penelitian ini, variabel bebas (X) adalah kebijakan, strategi, maupun pendekatan yang diterapkan untuk penggunaan sertifikasi elektronik.

[49] Nasution T, educandumedia (Jurnal Pendidikan dan Kependidikan) Persamaan Dan Perbedaan Sistem Demokrasi Indonesia Dengan Negara Lain)

[50] (Cahyono, Jurnal Ilmiah Pamenang-Jip The Role Of Development Of Performance Management Of Health Administration On Improving The Quality Of Health Services In Community Health Centers 2021)

[51] (Meling, Indonesian Journal of Primary Education Pengaruh Penggunaan Media Pembelajaran dalam Dunia Pendidikan tahun 2019)

2. Variabel Terikat (Dependent Variable)

Variabel terikat adalah variabel yang dipengaruhi atau menjadi hasil dari adanya variabel bebas. Dalam penelitian ini, variabel terikat (Y) adalah efektivitas sertifikasi elektronik.

Maka dari itu, pendekatan melalui variabel-variabel dalam penelitian ini, agar peneliti maupun *audiens* dapat memahami pentingnya sebab akibat dalam penelitian membandingkan sertifikasi elektronik Indonesia dan Singapura.

B. Fokus Penelitian

Penelitian ini berfokus mengenai bagaimana kebijakan Komparasi Sistem Hukum Di Bidang Sertifikasi Elektronik Antara Indonesia Dan Singapur dirancang, diterapkan, dan diterima oleh masyarakat. Serta memahami konteks dalam perbandingan kebijakan, sosial, budaya, dan politik di Indonesia maupun Singapura dalam penggunaan sertifikasi elektronik yang memengaruhi efektivitas kebijakan di masing-masing negara.

Penelitian berlangsung dua bulan, atau sesuai dengan kondisi penelitian saat ini dan kebutuhan tambahan. Waktu penelitian dihitung mulai dari seminar proposal hingga perolehan surat izin penelitian.

C. Jenis dan Sumber Data

Pengumpulan data dalam bidang ini tentunya berkaitan dengan Analisis dokumen hukum, kebijakan, laporan resmi, dan artikel ilmiah yang relevan. Yang dapat diperoleh melalui internet seperti UU ITE (Indonesia), ETA (Singapura),

UNCITRAL, laporan Kominfo, dan act of singapore. Setidaknya untuk penelitian kualitatif, sumber datanya adalah kata dan tindakan, dan selebihnya merupakan data tambahan seperti data dari website internet, jurnal ilmiah, serta buku-buku.

Sumber data utama adalah kebijakan pada Undang-Undang. Sumber data utama dikumpulkan melalui situs resmi SSO *Singapore Statutes Online & PsrE (*Penyelenggara Sertifikasi Elektronik) Inonesia. Sedangkan sumber data tertulis lainnya dapat dikategorikan menjadi sumber dari buku dan jurnal ilmiah, sumber dari arsip, dan dokumen resmi dari situs *Singapore Academy of Law Journal (SAcLJ) & Komdigi (Kementrian Komunikasi dan Digital).*

Ada dua sumber yang digunakan dalam penelitian yaitu sumber data primer dan sekunder yaitu sebagai berikut:

1. Sumber data Primer

   Primer yang digunakan, mengobservasi penggunaan teknologi atau alat pendeteksi hoaks yang ada pada platform sosial media dan internet. Penulis juga menggali seberapa besar keuntungan dan kerugian bagi pengguna sertifikasi elektronik
2. Sumber data Sekunder

   Sekunder yang digunakan peneliti dalam penelitian ini yaitu terdiri dari buku-buku, jurnal, tesis, dan situs internet.

D. Teknik Pengumpulan dan Pengelolaan Data

Suatu penelitian dapat dikatakan valid apabila dapat dibuktikan kebenaran data yang diperolehnya. Untuk memperoleh data yang valid diperlukan metodologi

yang tepat dalam pengumpulannya. Metode yang digunakan untuk mengumpulkan data dalam penelitian ini adalah:

1. Pengumpulan data

   Teknik pengumpulan data ini yaitu mengamati data langsung dengan cara mencatat pernyataan dari kata-kata. Peneliti mengumpulkan data pada lapangan melalui proses telaah dari jurnal-jurnal mengenai sertifikasi elektronik di Indonesia dan Singapura.

2. Reduksi data

   Reduksi data ialah tahap pemilihan, yang bertujuan untuk menyederhanakan data, pengabstrakan dan transformasi data yang diperoleh melalui catatan catatan yang tertulis di lapangan. Adapun data yang terkumpul dapat dilihat pada kerangka konseptual, rumusan masalah, pendekatan pengumpulan data. Reduksi data meliputi 1)ringkas data, 2)menelusuri tema, 3)seleksi data, 4)menggolongkan pengumpulan data.

3. Penyajian data

   Teknik pengumpulan data tertulis melengkapi sekumpulan informasi yang disusun, sehingga memberikan kesimpulan. Bentuk penyajian data berupa *teks* yang diperoleh dari macam macam sumber data. Bentuk ini menggabungkan informasi tersusun yang mudah dibaca dan dicermati sehingga kesimpulan yang diberikan sudah tepat maupun kebalikannya.

E. Uji Keabsahan Data

Pemeriksaan terhadap keabsahan data pada dasarnya, selain digunakan untuk menyanggah balik yang dituduhkan kepada penelitian kualitatif yang mengatakan tidak ilmiah, juga merupakan sebagai unsur yang tidak terpisahkan dari tubuh

pengetahuan penelitian kualitatif. Dalam penelitian kualitatif, pengujian validitas dan reliabilitas disebut dengan pemeriksaan keabsahan data. Pemeriksaan ini melibatkan empat kriteria utama, yaitu derajat kepercayaan (credibility), keteralihan (transferability), kebergantungan (dependability), dan kepastian (confirmability), penelitian ini menggunakan ketekunan pengamatan, dan kecukupan referensi dan uraian rinci.[52] Pada penelitian ini, fokus utama adalah triangulasi, yang merupakan teknik pemeriksaan data yang paling sering digunakan dalam penelitian skripsi mahasiswa.

F. Teknik Analisis Data

Analisis data adalah proses menyusun dan mengkategorikan data serta mencari pola atau tema dengan tujuan menemukan maknanya. Mengorganisasikan data berarti mengelompokkannya ke dalam tema, pola, atau kategori sesuai dengan maksud Anda. Tanpa struktur data ini, maka timbul permasalahan dalam penelitian, yang dibahas. Susunan data ini memberikan berbagai penafsiran dan penafsiran yang bermakna untuk memberi makna pada analisis dan penjelasan pola dan kategori serta untuk mencari hubungan antar konsep yang berbeda. Dalam penelitian ini penulis menggunakan analisis data yang mencakup data yaitu:

1. Induktif Data

   Induktif, yaitu cara berpikir bahwa terdapat unsur kesamaan pada dengan menganalisis data tertentu dan menarik kesimpulan umum. Metode ini digunakan untuk memahami permasalahan yang bersifat kontingen, khususnya berupa perbandingan penanggulangan hoaks antara Indonesia dan Singapura ke kesimpulan yang bersifat umum.
2. Deduktif Data

[52] Hadi, Pemeriksaan Keabsahan Data Penelitian Kualitatif Pada Skripsi tahun 2010

Deduktif, yaitu memulai dengan pernyataan umum, mengandalkan pertanyaan yang berkaitan dengan penelitian, dan memberikan alasan berdasarkan kesimpulan. Pendekatan deduktif fokus pada penggunaan teori atau hipotesis yang ada untuk mengarahkan proses pengumpulan dan analisis data.

Peristiwa, tindakan, kejadian, dan keadaan yang ada di masyarakat dapat dianggap sebagai data konkret yang menunggu untuk ditafsirkan. Makna yang terkandung dalam data tersebut kemudian dicari dan digali melalui tradisi penelitian kualitatif. Dalam penelitian kuantitatif, proses dimulai dengan perumusan masalah, diikuti dengan penyusunan hipotesis, pembuatan instrumen pengumpulan data, pengumpulan data itu sendiri, kemudian analisis data, dan akhirnya penulisan laporan penelitian. Semua tahapan ini harus dilakukan secara berurutan dan linier tanpa boleh tertukar. Sebaliknya, dalam penelitian kualitatif, konseptualisasi, kategorisasi, dan deskripsi berkembang berdasarkan "kejadian" yang terjadi.

Oleh karena itu, antara pengumpulan data dan analisis data dalam penelitian kualitatif tidak bisa dipisahkan, karena keduanya saling terkait dan berlangsung secara bersamaan.[53] Setelah data dianalisis, peneliti menginterpretasikan temuan dan menarik kesimpulan. Interpretasi ini harus didasarkan pada teori atau hipotesis yang ada dan menjawab pertanyaan penulis.

[53] Ahmad Rijali, Analisis Data Kualitatif, Uin Banjarmasin 2018*)*

BAB II

Kedudukan Sistem Hukum Di Bidang Sertifikasi Elektronik Antara Indonesia dan Singapura

A. Sistem Hukum Sertifikasi Elektronik Di Indonesia

1. Undang Undang Nomor 1 Tahun 2024

Sistem hukum sertifikasi elektronik di Indonesia diatur dalam beberapa peraturan perundang-undangan yang bertujuan untuk menjamin keamanan, keandalan, dan keabsahan transaksi elektronik**.** Indonesia, sebagai negara dengan pertumbuhan pengguna internet yang pesat, tidak luput dari ancaman siberterorisme. Untuk mengatasi tantangan ini, pemerintah telah mengesahkan Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik (UU ITE), yang merupakan revisi dari peraturan sebelumnya. UU ini bertujuan memperkuat kerangka hukum untuk menangani kejahatan siber, termasuk siberterorisme, dengan mengatur aspek seperti penyalahgunaan informasi, perlindungan data, dan penegakan hukum terhadap pelaku kejahatan digital.

Namun, efektivitas UU Nomor 1 Tahun 2024 dalam mencegah dan menangani siberterorisme masih dipertanyakan. Sejumlah pihak menilai bahwa regulasi ini memiliki kelemahan, baik dari segi substansi hukum, pelaksanaan, maupun koordinasi antarinstansi. Sebagai contoh, terdapat keragaman interpretasi terhadap beberapa pasal UU ITE, serta kesulitan dalam menyesuaikan regulasi dengan perkembangan teknologi yang bergerak cepat.[54] Undang-Undang No. 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik (UU ITE) merupakan langkah legislasi terbaru yang bertujuan untuk memberikan kerangka hukum dalam mengatur aktivitas di dunia maya, termasuk pencegahan cyberterrorism. UU ini menggantikan Undang-

[54] Muhammad Arkhan and others, 'Jurnal Hukum Mimbar Justitia (JHMJ) Evaluasi Efektivitas Undang-Undang No . 1 Tahun 2024 Tentang Informasi Dan Transaksi Elektronik Dalam Pencegahan Cyberterrorism Evaluation of the Effectiveness of Law No . 1 of 2024 on Information and Electronic Trans', 5681.2 (2024), pp. 430–43.

Undang sebelumnya dan memperkenalkan sejumlah perubahan signifikan, termasuk penambahan pasal-pasal baru yang berfokus pada perlindungan masyarakat dari penyalahgunaan teknologi informasi. Namun, meskipun UU ITE diharapkan dapat memberikan perlindungan yang lebih baik terhadap kejahatan siber, pelaksanaan undang-undang ini masih menghadapi berbagai kejahatan siber, ancaman dan permasalahannya. Ini menunjukkan bahwa ada kekurangan dalam kesadaran publik mengenai bahaya cybercrime, lemahnya penegakan hukum, serta perlunya interpretasi yang lebih jelas terhadap pasal-pasal dalam undang-undang. Selain itu, terdapat kritik mengenai potensi penyalahgunaan kewenangan pemerintah dalam menerapkan undang-undang ini, yang dapat mengancam kebebasan berekspresi Masyarakat. Hukum telah lama mengembangkan penafsiran asas dan norma untuk menangani benda tak berwujud, seperti pencurian listrik sebagai tindak pidana. Dalam dunia siber, aktivitas kini jauh lebih kompleks karena tidak terbatas pada wilayah negara, dapat diakses kapan saja dan dari mana saja. Kerugian bisa menimpa pelaku transaksi maupun pihak lain yang tidak terlibat, seperti pencurian data kartu kredit melalui transaksi daring.

Berdasarkan Pasal 30 ayat (1) Undang-Undang Nomor 1 Tahun 2024, yang merupakan perubahan kedua atas UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, tindak pidana *hacking* diatur sebagai perbuatan sengaja dan tanpa hak atau melawan hukum untuk mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apa pun.[55] Hubungan antara *hacking* dan sertifikasi elektronik dalam konteks Undang-Undang Nomor 1 Tahun 2024, yang merupakan perubahan kedua atas UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), dapat dilihat dari upaya hukum untuk mengatur keamanan dan keabsahan transaksi elektronik, termasuk perlindungan terhadap tindak pidana *hacking*. Pasal 30 ayat (1) UU ITE mengatur bahwa setiap orang yang dengan sengaja dan tanpa hak

[55] Ditinjau Dari and others, 'Pertanggungjawaban Pidana Terhadap Pelaku Hacking Hukum Dalam Tindak Pidana Cyber Crime Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik)', 4307.May (2025), pp. 1707–17.

mengakses komputer atau sistem elektronik milik orang lain secara melawan hukum melakukan tindak pidana *hacking*. Tindakan ini mencakup upaya merusak, mencuri data, atau mengganggu keamanan sistem elektronik, yang dapat mengancam integritas transaksi elektronik, termasuk yang menggunakan sertifikasi elektronik. Sertifikasi elektronik (atau sertifikat elektronik) adalah mekanisme yang digunakan untuk memastikan keamanan, keabsahan, dan integritas transaksi elektronik, seperti tanda tangan elektronik atau identitas digital. Dalam UU ITE, sertifikasi elektronik diatur untuk memberikan jaminan bahwa data atau transaksi elektronik sah, terpercaya, dan dilindungi dari manipulasi.

Penyelenggara sertifikasi elektronik (misalnya, otoritas sertifikasi atau CA) bertugas memastikan sistem keamanan yang kuat untuk mencegah penyalahgunaan, termasuk serangan *hacking*. *Hacking* dapat menargetkan sistem sertifikasi elektronik untuk mencuri identitas digital, memalsukan tanda tangan elektronik, atau merusak kepercayaan terhadap transaksi elektronik. Misalnya, peretasan terhadap server penyelenggara sertifikasi elektronik dapat membahayakan keamanan data pengguna. UU Nomor 1 Tahun 2024 memperkuat perlindungan terhadap sistem elektronik, termasuk yang digunakan untuk sertifikasi elektronik, dengan menetapkan sanksi tegas terhadap *hacking* (Pasal 30). Hal ini bertujuan untuk menjaga kepercayaan publik terhadap sistem elektronik, termasuk transaksi yang menggunakan sertifikasi elektronik. Sertifikasi elektronik berperan sebagai lapisan keamanan untuk mencegah atau meminimalkan risiko *hacking*, misalnya melalui enkripsi data atau autentikasi yang kuat, sehingga transaksi elektronik lebih terlindungi.UU ITE tidak hanya mengatur sanksi terhadap *hacking*, tetapi juga mengatur penyelenggaraan sertifikasi elektronik (misalnya, pada pasal-pasal terkait tanda tangan elektronik dan penyelenggara sistem elektronik).

Dengan demikian, hubungan keduanya terletak pada upaya menciptakan ekosistem digital yang aman, di mana sertifikasi elektronik menjadi alat untuk mencegah dan mengurangi dampak tindak pidana *hacking*., Jadi *hacking* dan sertifikasi elektronik saling terkait dalam UU Nomor 1 Tahun 2024, di mana *hacking*

merupakan ancaman terhadap keamanan sistem elektronik, sementara sertifikasi elektronik berfungsi sebagai mekanisme perlindungan untuk menjaga integritas dan kepercayaan dalam transaksi digital. Maraknya kasus cybercrime di Indonesia dipengaruhi oleh kemajuan teknologi informasi yang mengubah budaya masyarakat, seperti perubahan peran gender, peningkatan rasa percaya diri, dan tekanan sosial yang dirasakan. Budaya yang telah mengakar kuat dalam masyarakat Indonesia, yang sangat memengaruhi kehidupan sosial, turut menjadi faktor munculnya cybercrime. Kelemahan dalam budaya sosial masyarakat menjadi celah yang dimanfaatkan untuk masuknya kasus-kasus tersebut.[56] Selain aspek teknis dan hukum, UU ini juga mempertimbangkan dampak budaya digital di Indonesia. Dengan meningkatnya kasus *cybercrime* yang dipengaruhi oleh perubahan budaya, seperti peran gender atau tekanan sosial, UU ini berupaya menciptakan ekosistem digital yang lebih aman dengan mengatasi celah-celah sosial yang dimanfaatkan pelaku kejahatan siber.

Secara keseluruhan, UU Nomor 1 Tahun 2024 bertujuan untuk menciptakan lingkungan digital yang aman, terpercaya, dan mendukung perkembangan ekonomi digital di Indonesia, sambil mengatasi berbagai bentuk kejahatan siber di luar *hacking*, seperti penipuan daring, pelanggaran data pribadi, dan penyebaran konten ilegal Undang-Undang Nomor 1 Tahun 2024, sebagai perubahan kedua atas UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), menempatkan perlindungan data pribadi sebagai salah satu fokus utama untuk menciptakan ekosistem digital yang aman di Indonesia. Perlindungan data pribadi dalam UU ini selaras dengan semangat Undang-Undang Perlindungan Data Pribadi (UU PDP) yang mulai berlaku, menekankan pentingnya menjaga privasi individu di tengah maraknya transaksi elektronik dan ancaman kejahatan siber. UU ini mengatur bagaimana data pribadi, yang mencakup informasi seperti nama, alamat, nomor identitas, data keuangan, hingga riwayat kesehatan, harus dikelola dengan aman oleh

[56] Adelina Damayanti and Rina Arum Prastyanti, 'Kajian Hukum Dan Regulasi Terkait Serangan Hacking Pada Platform Digital Di Indonesia', *Multidisciplinary Indonesian Center Journal (MICJO)*, 1.2 (2024), pp. 1043–54, doi:10.62567/micjo.v1i2.117.

penyelenggara sistem elektronik (PSE), baik pihak publik maupun swasta, untuk mencegah penyalahgunaan seperti kebocoran data, pencurian identitas, atau penggunaan tanpa izin.

Dalam UU ITE, perlindungan data pribadi diatur terutama melalui pasal-pasal yang mengatur kewajiban PSE dalam menjaga keamanan data. Meskipun UU ini tidak menyebutkan nomor pasal spesifik untuk perlindungan data pribadi secara eksplisit seperti dalam UU PDP, beberapa ketentuan terkait dapat ditemukan, misalnya pada Pasal 26 yang mengatur tanggung jawab PSE untuk menjaga kerahasiaan, integritas, dan ketersediaan data pribadi yang mereka kelola.

Pasal ini menegaskan bahwa setiap pengelola data wajib memastikan data pribadi tidak digunakan di luar izin pemilik data, kecuali atas dasar hukum atau persetujuan eksplisit. Pelanggaran terhadap ketentuan ini dapat dikenakan sanksi, baik administratif maupun pidana, seperti yang diatur dalam pasal-pasal sanksi di UU ITE, misalnya Pasal 48 yang menyebutkan ancaman pidana bagi pelaku yang dengan sengaja menyebabkan kerugian akibat penyalahgunaan data elektronik. Selain itu, UU ini juga mengatur aspek pencegahan kebocoran data melalui standar keamanan sistem elektronik. Pasal 3 ayat (2) UU ITE, misalnya, menekankan bahwa penyelenggara sistem elektronik harus memenuhi standar teknis keamanan untuk melindungi data dari ancaman seperti peretasan atau manipulasi. Ini mencakup penggunaan enkripsi, autentikasi, dan mekanisme keamanan lainnya untuk memastikan data pribadi tidak jatuh ke tangan yang tidak berwenang. Dalam konteks transaksi elektronik, seperti e-commerce atau layanan digital, PSE diwajibkan untuk menyediakan sistem yang menjamin keamanan data pengguna, seperti saat menggunakan sertifikasi elektronik atau tanda tangan digital, yang juga diatur dalam UU ini untuk mendukung kepercayaan publik terhadap teknologi.

UU Nomor 1 Tahun 2024 juga mengakui pentingnya hak individu atas data pribadinya. Pemilik data memiliki hak untuk mengakses, memperbaiki, atau bahkan meminta penghapusan data pribadi mereka yang disimpan oleh PSE, sebagaimana tersirat dalam pasal-pasal yang mengatur pengelolaan informasi elektronik. Hal ini

mencerminkan prinsip-prinsip seperti *right to be forgotten* yang diadopsi dari regulasi perlindungan data global. Jika terjadi kebocoran data, PSE wajib melaporkan insiden tersebut kepada otoritas terkait dan pihak yang terdampak, sebagaimana diatur dalam ketentuan pelaporan pelanggaran sistem elektronik.

Lebih lanjut, UU ini juga memperhatikan tantangan kejahatan siber yang berkaitan dengan data pribadi, seperti *phishing* atau pencurian identitas. Meskipun *hacking* diatur secara spesifik dalam Pasal 30, tindakan seperti manipulasi data (Pasal 31) atau penyebaran informasi elektronik yang merugikan (Pasal 28) juga relevan dengan perlindungan data pribadi, karena pelaku kejahatan siber sering memanfaatkan data pribadi untuk tujuan penipuan atau pemerasan. Sanksi berat, termasuk pidana penjara dan denda, diberlakukan untuk memberikan efek jera, seperti yang tercantum dalam Pasal 45 dan pasal-pasal terkait lainnya. Secara keseluruhan, UU Nomor 1 Tahun 2024 berupaya menciptakan keseimbangan antara kemajuan teknologi informasi dan perlindungan privasi individu.

Dengan mengatur kewajiban PSE, menetapkan standar keamanan, dan memberikan hak kepada individu atas data mereka, UU ini berfungsi sebagai payung hukum yang memperkuat kepercayaan masyarakat terhadap ekosistem digital, sekaligus mengurangi risiko penyalahgunaan data pribadi di tengah meningkatnya ancaman kejahatan siber di Indonesia.[57] Identitas memiliki makna yang sangat luas dan beragam. Identitas dapat merujuk pada identitas individu atau kelompok, yang keduanya merupakan hasil konstruksi sosial. Identitas, baik secara individu maupun kolektif, dapat dilihat dari sudut pandang sosial dan budaya identitas sosial adalah harapan dan pandangan orang lain terhadap diri kita. Identitas sosial seseorang dipengaruhi oleh identitas diri serta lingkungan sekitar, termasuk pengaruh media. juga menyebutkan bahwa tanda-tanda identitas tercermin melalui selera, kepercayaan,

[57] Damayanti and Prastyanti, 'Kajian Hukum Dan Regulasi Terkait Serangan Hacking Pada Platform Digital Di Indonesia'.

perilaku, dan gaya hidup Sementara itu, identitas budaya berkaitan dengan cara seseorang merepresentasikan nilai, ideologi, atau budaya tertentu.[58]

Undang-Undang Nomor 1 Tahun 2024, sebagai perubahan kedua atas UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), memperbarui kerangka sanksi untuk pelanggaran di ranah elektronik dengan tujuan menciptakan efek jera terhadap kejahatan siber. UU ini memperkenalkan penyesuaian denda dan pidana penjara yang lebih tegas untuk berbagai tindak pidana elektronik, seperti penyebaran konten ilegal, manipulasi data, ujaran kebencian, dan penipuan daring. Misalnya, pelaku penyebaran informasi elektronik yang melanggar kesusilaan atau menyebarkan hoaks yang menyebabkan kerusuhan dapat menghadapi pidana penjara hingga enam tahun dan/atau denda hingga satu miliar rupiah, sebagaimana diatur dalam Pasal 27 dan Pasal 28. Untuk kasus perjudian daring, sanksi bahkan lebih berat, dengan ancaman pidana penjara hingga sepuluh tahun dan denda hingga sepuluh miliar rupiah, seperti tercantum dalam Pasal 27 ayat (2) jo. Pasal 45 ayat (3). Selain itu, tindakan seperti pencemaran nama baik melalui media elektronik diatur dalam Pasal 27A, dengan ancaman pidana penjara hingga dua tahun dan/atau denda hingga empat ratus juta rupiah, sementara fitnah dapat dikenakan sanksi hingga empat tahun penjara dan denda hingga tujuh ratus lima puluh juta rupiah. Ketentuan ini dirancang untuk memberikan kepastian hukum sekaligus menyesuaikan besaran sanksi dengan dampak kejahatan siber yang semakin kompleks di era digital.

Selain memperbarui sanksi, UU ini juga memperluas kewenangan penegak hukum dalam menangani kejahatan siber. Penegak hukum, seperti kepolisian dan jaksa, diberi wewenang untuk melakukan tindakan seperti membatasi akses ke sistem elektronik yang digunakan untuk kejahatan, meminta informasi dari penyelenggara sistem elektronik, serta melakukan penyidikan dan penyadapan sesuai prosedur yang diatur, misalnya melalui perubahan Pasal 31 ayat (4) yang kini mensyaratkan

[58] Soraya Fadhal and Lestari Nurhajati, 'Identifikasi Identitas Kaum Muda Di Tengah Media Digital (Studi Aktivitas Kaum Muda Indonesia Di Youtube)', *Jurnal Al Azhar Indonesia Seri Pranata Sosial*, 1.3 (2012), pp. 176–99 <http://main.makeuseoflimited.netdna-cdn.com/>.

pengaturan penyadapan dalam undang-undang, bukan hanya peraturan pemerintah. Yang tak kalah penting, UU ini menekankan pentingnya kerja sama internasional untuk menangani kasus lintas negara, mengingat sifat kejahatan siber yang sering kali melampaui batas yurisdiksi nasional.

Dengan maraknya kejahatan seperti phishing, pencurian data lintas negara, atau penyebaran konten ilegal melalui platform global, UU ini memungkinkan penegak hukum Indonesia untuk bekerja sama dengan otoritas asing, misalnya melalui pertukaran informasi atau koordinasi penegakan hukum, untuk memastikan pelaku kejahatan siber dapat dijerat meskipun beroperasi dari luar negeri. Pendekatan ini mencerminkan kesadaran bahwa kejahatan siber bersifat transnasional, sehingga membutuhkan kolaborasi global untuk menangani tantangan seperti server yang berlokasi di luar negeri atau pelaku yang menggunakan identitas anonim.

Dengan demikian, UU Nomor 1 Tahun 2024 tidak hanya memperkuat sanksi untuk menciptakan efek jera, tetapi juga memberdayakan penegak hukum dengan alat dan kerja sama internasional yang lebih efektif untuk melindungi masyarakat dari ancaman di ruang digital. Sanksi pidana untuk pelanggaran tertentu diatur dalam Pasal 45 ayat (3) UU Nomor 19 Tahun 2016, yang merupakan perubahan atas UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, dengan ancaman pidana penjara maksimal 4 tahun dan/atau denda hingga Rp750.000.000,00 (tujuh ratus lima puluh juta rupiah). Namun, dalam UU Nomor 1 Tahun 2024, yang merupakan perubahan kedua atas UU Nomor 11 Tahun 2008, ketentuan Pasal 27 ayat (3) telah dihapus dan digantikan oleh Pasal 27A. Penghapusan Pasal 27 ayat (3) ini dilakukan karena pasal tersebut dianggap sebagai "pasal karet" yang membatasi kebebasan berpendapat masyarakat, aturan yang awalnya dimaksudkan untuk menciptakan keseimbangan dalam penggunaan internet demi ketertiban umum ternyata belum efektif, bahkan justru menimbulkan keresahan di kalangan

masyarakat.[59] Tumpang tindih wewenang antara pemerintah pusat dan daerah menjadi hambatan dalam efektivitas penegakan hukum. Minimnya koordinasi antarlembaga pemerintah dapat menimbulkan kebingungan dalam penanganan kasus kejahatan teknologi apalagi yang mengarah ke ranah seksual, sehingga hukum diterapkan secara tidak konsisten. Selain itu, korban sering menghadapi stigma sosial yang membuat mereka tertekan untuk tidak melaporkan kasus. Lingkungan sosial yang kurang mendukung memperparah keadaan, karena banyak korban merasa enggan untuk membuka pengalaman mereka.[60]

Dalam Undang-Undang Nomor 1 Tahun 2024, yang merupakan perubahan kedua atas UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), pengaturan sanksi untuk pelanggaran di ranah elektronik menjadi salah satu fokus utama untuk memastikan keamanan dan ketertiban di ruang digital. Selain sanksi untuk tindak pidana seperti hacking, penyebaran hoaks, atau pencemaran nama baik yang telah dibahas sebelumnya, UU ini juga memperluas cakupan sanksi untuk menangani berbagai bentuk kejahatan siber yang semakin kompleks. Misalnya, untuk pelanggaran terkait penyebaran konten yang melanggar kesusilaan, seperti pornografi atau perjudian daring, UU ini menetapkan ancaman pidana penjara hingga tujuh tahun dan denda yang bisa mencapai miliaran rupiah, seperti diatur dalam Pasal 27 jo. Pasal 45. Sanksi ini dirancang untuk memberikan efek jera, terutama karena dampak kejahatan siber dapat menyebar luas dan cepat melalui platform digital.

Selain itu, UU ini juga mengatur sanksi administratif untuk penyelenggara sistem elektronik (PSE) yang lalai dalam menjaga keamanan data atau gagal mematuhi regulasi, seperti kewajiban pendaftaran PSE atau penerapan standar keamanan sistem. Sanksi administratif ini bisa berupa peringatan tertulis, denda, hingga pencabutan izin operasi, yang diatur dalam pasal-pasal terkait pengelolaan sistem elektronik. Untuk kasus manipulasi data elektronik, seperti mengubah atau

[59] Radita Gora Musqith, Munadhil Abdul; Tayibnapis, 'Jurnal Sosial Dan Budaya Syar-I', *Jurnal Sosial Dan Budaya Syar-I*, 9.4 (2022), pp. 1307–18, doi:10.15408/sjsbs.v10i6.38412.

[60] Anggini Salsabillah and Yudi Kornelis, 'Melalui Media Sosial Menurut Undang Undang Nomor 1 Tahun 2024 Tentang Ite', 2024.

menghapus informasi tanpa hak, Pasal 31 jo. Pasal 48 menetapkan ancaman pidana penjara hingga lima tahun dan denda hingga satu miliar rupiah, menekankan pentingnya menjaga integritas data dalam transaksi digital. UU ini juga memperhatikan kejahatan seperti phishing atau penipuan daring, dengan sanksi yang disesuaikan untuk melindungi pengguna dari kerugian finansial atau pencurian identitas. Selain sanksi pidana dan administratif, UU Nomor 1 Tahun 2024 juga mendorong pendekatan preventif melalui penguatan literasi digital, meskipun tidak secara langsung diatur sebagai sanksi, tetapi menjadi bagian dari upaya mengurangi pelanggaran dengan meningkatkan kesadaran masyarakat. Namun, tantangan dalam penerapan sanksi ini tetap ada, seperti tumpang tindih kewenangan antarlembaga atau kurangnya koordinasi dalam penegakan hukum, yang dapat mengurangi efektivitas sanksi tersebut.

Meski demikian, dengan memperbarui besaran denda dan pidana serta memperluas cakupan pelanggaran yang diatur, UU ini berupaya menciptakan ekosistem digital yang lebih aman dan terpercaya di Indonesia.

2. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE)

Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE) adalah regulasi di Indonesia yang mengatur secara rinci mengenai sistem elektronik dan transaksi elektronik untuk mendukung transformasi digital yang aman dan andal. Sistem elektronik didefinisikan sebagai sekumpulan perangkat dan prosedur elektronik yang digunakan untuk menyiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirim, dan/atau menyebarkan informasi elektronik. Sementara itu, berdasarkan Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, Penyelenggara Sistem Elektronik (PSE) adalah setiap individu, instansi negara, badan usaha, atau masyarakat yang menyediakan, mengelola, dan mengoperasikan sistem elektronik, baik secara mandiri

maupun bersama-sama, untuk kebutuhan sendiri atau pihak lain. Berdasarkan Pasal 19 Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, Penyelenggara Sistem Elektronik diwajibkan untuk menerapkan tata kelola sistem elektronik yang baik dan dapat dipertanggungjawabkan. Selain itu, Penyelenggara Sistem Elektronik juga berkewajiban untuk memastikan keamanan komponen sistem elektronik yang digunakan.[61] Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP 71/2019) merupakan regulasi yang menggantikan PP Nomor 82 Tahun 2012, disusun untuk menyesuaikan perkembangan teknologi informasi dan mendukung pertumbuhan ekonomi digital serta penegakan kedaulatan negara atas informasi elektronik di Indonesia.

Dalam Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP 71/2019), kerja sama internasional dan keamanan siber menjadi aspek penting untuk menangani tantangan kejahatan siber yang bersifat lintas negara. Mengingat sifat dunia digital yang tidak mengenal batas geografis, kejahatan siber seperti phishing, peretasan, pencurian data, atau penyebaran konten ilegal sering kali melibatkan pelaku, server, atau infrastruktur yang berada di luar yurisdiksi Indonesia. Untuk mengatasi hal ini, PP 71/2019 mendorong kerja sama internasional melalui koordinasi antarnegara dalam penegakan hukum, pertukaran informasi, dan pelacakan pelaku kejahatan siber. Misalnya, otoritas Indonesia dapat bekerja sama dengan lembaga penegak hukum asing untuk mengidentifikasi pelaku yang beroperasi dari luar negeri atau menutup akses ke server yang digunakan untuk aktivitas kriminal, seperti situs perjudian daring atau platform penyebar hoaks.

Kerja sama ini juga mencakup harmonisasi standar keamanan siber, seperti berbagi praktik terbaik dalam perlindungan data atau penanganan insiden kebocoran

[61] Arkhan and others, 'Jurnal Hukum Mimbar Justitia (JHMJ) Evaluasi Efektivitas Undang-Undang No . 1 Tahun 2024 Tentang Informasi Dan Transaksi Elektronik Dalam Pencegahan Cyberterrorism Evaluation of the Effectiveness of Law No . 1 of 2024 on Information and Electronic Trans'.

informasi. Dari sisi keamanan siber, PP 71/2019 menekankan pentingnya penyelenggara sistem elektronik (PSE) menerapkan langkah-langkah teknis untuk melindungi sistem mereka dari ancaman seperti peretasan, malware, atau manipulasi data. PSE diwajibkan mematuhi standar keamanan, seperti penggunaan enkripsi dan autentikasi yang kuat, untuk menjaga integritas dan kerahasiaan data pengguna. Regulasi ini juga mengatur tanggung jawab PSE dalam mencegah dan menangani insiden siber, termasuk melaporkan kebocoran data kepada otoritas terkait, seperti Kementerian Komunikasi dan Informatika. Dengan pendekatan ini, PP 71/2019 berupaya menciptakan ekosistem digital yang lebih aman melalui kolaborasi global dan penguatan infrastruktur keamanan siber, meskipun tantangan seperti kurangnya koordinasi antarlembaga atau kompleksitas pelacakan pelaku lintas negara masih menjadi hambatan dalam implementasinya. Keberhasilan perlindungan data pribadi sangat bergantung pada penerapan pengamanan data dan keamanan siber yang tepat serta memadai.

Pengamanan data dan keamanan siber menjadi aspek krusial dalam sebuah sistem informasi, karena tanpa implementasi dan pemeliharaan yang baik, dapat timbul kerugian baik secara finansial maupun non-finansial bagi organisasi dan pihak-pihak yang terlibat. Jika pengamanan data dilakukan dengan benar, baik secara fisik maupun non-fisik, maka tiga aspek utama dalam pengamanan data—kerahasiaan, integritas, dan ketersediaan—dapat terpenuhi. Perlindungan data pribadi dari sisi pengamanan data dan keamanan siber diatur secara eksplisit dalam Undang-Undang Perlindungan Data Pribadi, tetapi dalam hal implementasi, aspek-aspek ini diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, serta Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik.

Dalam Peraturan Pemerintah Nomor 71 Tahun 2019, Penyelenggara Sistem Elektronik (PSE) diwajibkan melakukan audit siber secara berkala, sebagaimana

diatur dalam Pasal 18 dan Pasal 69. Selain itu, Pasal 65 hingga Pasal 72 mengatur tentang lembaga sertifikasi keandalan yang berkaitan erat dengan keamanan siber. Sertifikat keandalan harus diterbitkan oleh lembaga sertifikasi untuk memastikan bahwa standar operasional PSE telah sesuai dengan peraturan di Indonesia dan praktik terbaik di industri. Sementara itu, Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 menegaskan kewajiban PSE untuk memiliki aturan internal perlindungan data pribadi guna mencegah kegagalan dalam pengelolaan data pribadi. Aturan internal ini sering disebut sebagai *internal privacy policy*. Secara umum, PSE yang berperan sebagai pengendali data pribadi juga perlu menyusun *internal privacy policy* dan *external privacy policy* (privacy notice) untuk memastikan perlindungan data yang optimal.[62]

Dalam konteks Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP 71/2019), kerja sama internasional dan keamanan siber menjadi elemen krusial untuk menghadapi tantangan kejahatan siber yang bersifat lintas batas. Kejahatan siber seperti peretasan, penipuan daring, atau penyebaran konten ilegal sering kali melibatkan pelaku atau infrastruktur teknologi yang berada di luar wilayah Indonesia, sehingga memerlukan kolaborasi global untuk penanganannya. PP 71/2019 mendorong kerja sama internasional melalui mekanisme seperti pertukaran informasi antarnegara, koordinasi penegakan hukum, dan pembagian praktik terbaik dalam keamanan siber.

Misalnya, otoritas Indonesia dapat bekerja sama dengan lembaga asing untuk melacak server yang digunakan dalam aktivitas kriminal seperti situs perjudian daring atau platform yang menyebarkan malware, memastikan pelaku dapat diidentifikasi meskipun beroperasi dari luar negeri. Kerja sama ini juga mencakup upaya harmonisasi standar keamanan siber untuk memperkuat perlindungan data lintas yurisdiksi, mengingat data pribadi sering kali disimpan atau diakses melalui server

[62] Cindy Vania and others, 'Tinjauan Yuridis Terhadap Perlindungan Data Pribadi Dari Aspek Pengamanan Data Dan Keamanan Siber', *Jurnal Multidisiplin Indonesia*, 2.3 (2023), pp. 654–66, doi:10.58344/jmi.v2i3.157.

global. Dari sisi keamanan siber, PP 71/2019 mewajibkan Penyelenggara Sistem Elektronik (PSE) untuk menerapkan langkah-langkah pengamanan seperti enkripsi, autentikasi ganda, dan pemantauan sistem secara berkala untuk mencegah ancaman seperti peretasan atau kebocoran data. PSE juga harus melaporkan insiden siber kepada Kementerian Komunikasi dan Informatika, memastikan respons cepat terhadap pelanggaran keamanan. Ketentuan ini mencerminkan pentingnya infrastruktur digital yang tangguh, terutama karena dampak kejahatan siber dapat merugikan individu, organisasi, hingga stabilitas ekonomi digital. Namun, implementasi kerja sama internasional sering terkendala oleh perbedaan hukum antarnegara dan kompleksitas pelacakan pelaku anonim, sementara keamanan siber menuntut investasi teknologi dan sumber daya manusia yang memadai. Meski begitu, PP 71/2019 berupaya menciptakan ekosistem digital yang lebih aman dengan mengintegrasikan kolaborasi global dan penguatan teknis untuk melindungi pengguna di tengah ancaman siber yang terus berkembang.

Esensi Hak Asasi Manusia (HAM) merujuk pada inti atau hakikat dari hak-hak yang melekat pada setiap individu sebagai manusia, tanpa memandang latar belakang seperti ras, agama, jenis kelamin, atau kebangsaan. HAM bersifat universal, tidak dapat dicabut, dan melekat sejak seseorang lahir, karena didasarkan pada martabat manusia sebagai ciptaan yang memiliki harkat dan nilai intrinsik. Dalam konteks diskusi sebelumnya tentang perlindungan data pribadi, keamanan siber, dan regulasi seperti UU Nomor 1 Tahun 2024 serta PP Nomor 71 Tahun 2019, esensi HAM dapat dihubungkan dengan hak atas privasi, kebebasan berekspresi, dan perlindungan terhadap penyalahgunaan data pribadi di era digital.[63]

Dalam ranah keamanan siber dan kerja sama internasional, seperti yang diatur dalam PP 71/2019, esensi HAM tercermin dalam upaya melindungi individu dari ancaman lintas negara yang dapat merugikan hak mereka, seperti pencurian identitas

[63] Fakultas Syariah and others, 'Kemelitan Penegakan Hukum Terhadap Hak Kebebasan Berpendapat Syafa ' at Anugrah Pradana Rusdianto Sudirman', *Jurnal Syariah Dan Hukum*, 20 (2022), pp. 156–68.

atau penyebaran konten ilegal. Kerja sama dengan negara seperti Singapura, meskipun tidak diatur secara eksplisit dalam PP tersebut, menunjukkan komitmen untuk memperkuat perlindungan HAM melalui keamanan siber yang lebih baik, misalnya dengan berbagi praktik terbaik untuk mencegah kebocoran data yang dapat merusak privasi individu. Namun, tantangan seperti stigma sosial terhadap korban kejahatan siber atau tumpang tindih kewenangan antarlembaga dapat menghambat penegakan HAM, karena korban sering kali enggan melapor akibat tekanan sosial atau ketidakpastian hukum.

Secara keseluruhan, esensi HAM dalam konteks ini adalah menempatkan martabat manusia sebagai inti dari setiap regulasi dan kebijakan digital, memastikan bahwa teknologi tidak hanya memajukan ekonomi atau efisiensi, tetapi juga melindungi hak-hak dasar seperti privasi, kebebasan berekspresi, dan keamanan. Regulasi seperti UU ITE, UU PDP, dan PP 71/2019 berupaya mewujudkan esensi ini, meskipun tantangan implementasi masih memerlukan koordinasi yang lebih baik dan kesadaran masyarakat yang lebih tinggi akan hak-hak mereka di ruang digital. Konsep hak asasi manusia (HAM) tentang kebebasan berpendapat sering kali dianggap berbenturan dengan prinsip negara hukum. Sebagai negara hukum, Indonesia telah meratifikasi sejumlah perjanjian internasional yang mendukung kebebasan berpendapat, dan konstitusi juga menjamin hak ini, sehingga pemerintah diharapkan tidak menghalangi kritik dari masyarakat.[64]

Dalam Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP 71/2019), kerja sama internasional dan keamanan siber menjadi aspek penting untuk menangani kejahatan siber yang bersifat lintas negara, namun tidak disebutkan secara spesifik kerja sama dengan Singapura dalam regulasi ini. Meski begitu, Indonesia dan Singapura memiliki sejarah kolaborasi di bidang keamanan siber, sebagaimana tercatat dalam berbagai inisiatif di luar PP 71/2019. Misalnya, pada Oktober 2023, Kepala Badan Siber dan Sandi

[64] Ersa Kusuma, 'Kebebasan Berpendapat Dan Kaitannya Dengan Hak Asasi Manusia (HAM)', *Sanskara Hukum Dan HAM*, 1.03 (2023), pp. 97–101, doi:10.58812/shh.v1i03.63.

Negara (BSSN) Hinsa Siburian bertemu dengan Menteri Komunikasi dan Informasi Singapura, Josephine Teo, dalam acara Singapore International Cyber Week 2023. Dalam pertemuan tersebut, Indonesia menyampaikan dukungan terhadap upaya Singapura menggelar acara tahunan yang mempertemukan pembuat kebijakan, pelaku industri, dan akademisi untuk berbagi praktik terbaik dalam keamanan siber.

Hinsa mengusulkan pembuatan Memorandum of Understanding (MoU) untuk memperkuat kerja sama bilateral di bidang keamanan siber, mencerminkan keinginan Indonesia untuk belajar dari pengalaman dan keahlian Singapura, yang dikenal memiliki infrastruktur keamanan siber yang maju di ASEAN. Menteri Josephine menanggapi dengan menyebutkan bahwa kerja sama dapat dilakukan melalui Badan Keamanan Siber Singapura (CSA) dan forum ASEAN Ministerial Conference on Cybersecurity (AMCC), menunjukkan adanya peluang untuk kolaborasi yang lebih intensif. Selain itu, Singapura telah mendirikan ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE) untuk meningkatkan kapasitas keamanan siber di kawasan, yang juga melibatkan Indonesia dalam berbagai pelatihan dan pertukaran informasi. Kerja sama ini relevan mengingat Singapura pernah mengalami serangan siber besar pada 2018, ketika data kesehatan 1,5 juta warganya diretas, menunjukkan bahwa bahkan negara dengan sistem canggih tetap rentan. Dalam konteks kebebasan berpendapat yang dijamin sebagai hak asasi manusia (HAM) namun sering dianggap berbenturan dengan prinsip negara hukum, sanksi untuk pelanggaran di ranah elektronik di Indonesia diatur terutama melalui Undang-Undang Nomor 1 Tahun 2024, yang merupakan perubahan kedua atas UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), serta regulasi turunannya seperti Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP 71/2019).

Sanksi untuk pelanggaran di ranah elektronik mencakup berbagai bentuk, mulai dari pidana penjara hingga denda, yang dirancang untuk memberikan efek jera sekaligus menjaga ketertiban di ruang digital. Dalam UU Nomor 1 Tahun 2024, pelanggaran seperti penyebaran konten yang melanggar kesusilaan, misalnya

pornografi atau perjudian daring, dapat dikenakan ancaman pidana penjara hingga tujuh tahun dan denda hingga miliaran rupiah, sebagaimana diatur dalam Pasal 27 jo. Pasal 45. Untuk kasus pencemaran nama baik melalui media elektronik, yang sempat kontroversial karena dianggap membatasi kebebasan berpendapat, Pasal 27A menetapkan sanksi pidana penjara hingga dua tahun dan/atau denda hingga Rp400 juta, sedangkan tindakan fitnah dapat dihukum hingga empat tahun penjara dan denda hingga Rp750 juta. Revisi ini dilakukan untuk menghapus "pasal karet" seperti Pasal 27 ayat (3) dalam UU sebelumnya, yang sering digunakan untuk mengkriminalisasi kritik, seperti pada kasus Prita Mulyasari, guna lebih melindungi kebebasan berekspresi sesuai prinsip HAM yang dijamin konstitusi dan perjanjian internasional yang diratifikasi Indonesia, seperti Kovenan Internasional tentang Hak Sipil dan Politik (ICCPR).

Selain itu, untuk pelanggaran seperti manipulasi data elektronik atau peretasan, Pasal 31 jo. Pasal 48 UU ITE menetapkan pidana penjara hingga lima tahun dan denda hingga Rp1 miliar, menekankan pentingnya menjaga integritas sistem elektronik. PP 71/2019 juga mengatur sanksi administratif untuk Penyelenggara Sistem Elektronik (PSE) yang lalai, seperti gagal mendaftar atau tidak menerapkan standar keamanan siber. Sanksi ini bisa berupa peringatan tertulis, denda, hingga pemutusan akses, meskipun ketentuan ini sempat dikritik karena dianggap melampaui wewenang UU ITE. Misalnya, PSE yang tidak melindungi data pribadi pengguna dari kebocoran dapat menghadapi sanksi administratif dari Kementerian Komunikasi dan Informatika, sejalan dengan Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik, yang mewajibkan PSE memiliki kebijakan privasi internal. Penegakan hukum yang adil dan merata memegang peranan krusial dalam konteks ini. Negara memiliki tanggung

jawab untuk menjamin bahwa setiap individu diperlakukan secara setara di hadapan hukum tanpa adanya diskriminasi atau bias dalam pelaksanaan hukum.[65]

Namun, penerapan sanksi ini sering kali menimbulkan tantangan, terutama karena tumpang tindih kewenangan antarlembaga pemerintah dan kurangnya koordinasi, yang dapat menyebabkan penegakan hukum yang tidak konsisten. Selain itu, stigma sosial terhadap korban kejahatan siber, seperti penipuan daring atau pencemaran nama baik, sering membuat mereka enggan melapor, sehingga pelaku tidak selalu dijerat sanksi. Dalam konteks kebebasan berpendapat, sanksi yang terlalu ketat juga berisiko menekan HAM, seperti yang terlihat pada kasus-kasus awal UU ITE sebelum revisi, di mana individu seperti Narliswandi Piliang atau Erick J. Adriansyah dijerat karena kritik yang dianggap melanggar.

Oleh karena itu, UU Nomor 1 Tahun 2024 berupaya menciptakan keseimbangan dengan memperjelas definisi pelanggaran dan sanksi, serta mendorong kerja sama internasional untuk menangani kasus lintas negara, seperti yang didukung PP 71/2019, agar pelaku kejahatan siber dapat dijerat meskipun beroperasi dari luar Indonesia. Dengan demikian, sanksi elektronik ini bertujuan melindungi masyarakat sekaligus menjaga esensi HAM, meskipun implementasinya masih menghadapi kendala praktis dan sosial. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP 71/2019) merupakan regulasi yang dirancang untuk memperkuat ekosistem digital di Indonesia dengan mengatur penyelenggaraan sistem elektronik, transaksi elektronik, dan keamanan siber, sekaligus mendukung pertumbuhan ekonomi digital dan perlindungan hak asasi manusia (HAM) seperti privasi dan kebebasan berekspresi.

Secara keseluruhan, PP ini bertujuan menciptakan lingkungan digital yang aman, terpercaya, dan sesuai dengan prinsip negara hukum, meskipun menghadapi tantangan dalam implementasinya. PP 71/2019 mengatur kewajiban Penyelenggara

[65] Gianluca Fredrick Wou Dopo, I Nyoman Putu Budiartha, and Ida Ayu Putu Widiati, 'Kebebasan Berpendapat Dalam Hubungannya Dengan Tindak Pidana Ujaran Kebencian (Studi Putusan Pengadilan Tinggi Denpasar Nomor 72/ Pid.Sus/2020/Pt.Dps)', *Jurnal Analogi Hukum*, 5.2 (2023), pp. 162–66.

Sistem Elektronik (PSE), baik publik maupun swasta, untuk mendaftar ke Kementerian Komunikasi dan Informatika serta mematuhi standar keamanan seperti enkripsi dan audit siber berkala guna melindungi data pribadi dari ancaman seperti peretasan atau kebocoran. Regulasi ini juga menekankan pentingnya sertifikasi elektronik, termasuk tanda tangan elektronik, untuk memastikan keabsahan transaksi digital, dengan PSE wajib menjaga kerahasiaan, integritas, dan ketersediaan data. Sanksi administratif, seperti peringatan, denda, hingga pemutusan akses, diberlakukan bagi PSE yang lalai, meskipun ketentuan ini menuai kritik karena dianggap kurang memiliki dasar kuat dalam UU ITE.

Dalam konteks keamanan siber, PP ini mendorong kerja sama internasional untuk menangani kejahatan siber lintas negara, seperti phishing atau penyebaran konten ilegal, melalui koordinasi antarnegara dan pertukaran informasi, sejalan dengan kebutuhan menangani ancaman transnasional. Meski tidak menyebutkan secara spesifik kerja sama dengan negara seperti Singapura, PP ini mendukung kolaborasi regional, misalnya melalui forum ASEAN, untuk memperkuat kapasitas keamanan siber. Namun, tantangan seperti tumpang tindih kewenangan antarlembaga, kurangnya koordinasi, dan potensi overreach regulasi, seperti kewajiban pendaftaran PSE, menghambat efektivitas implementasi. Selain itu, aspek HAM, seperti perlindungan privasi dan kebebasan berekspresi, menjadi fokus penting, terutama karena pengalaman masa lalu dengan "pasal karet" dalam UU ITE yang dianggap membatasi kritik. PP 71/2019 berupaya menyeimbangkan keamanan digital dengan perlindungan HAM, tetapi keberhasilannya bergantung pada koordinasi yang lebih baik, literasi digital masyarakat, dan harmonisasi dengan regulasi lain seperti UU Nomor 1 Tahun 2024 dan UU Perlindungan Data Pribadi. Dengan demikian, PP ini menjadi landasan penting untuk ekosistem digital Indonesia, meskipun memerlukan

penyempurnaan dalam praktiknya agar adil, merata, dan mendukung inovasi tanpa mengorbankan hak-hak dasar individu.[66]

Dalam konteks keamanan siber, PP 71/2019 mewajibkan Penyelenggara Sistem Elektronik (PSE) untuk menerapkan standar keamanan seperti enkripsi dan audit siber berkala, yang sejalan dengan praktik terbaik yang dibagikan dalam forum seperti yang diadakan Singapura.

3. Peraturan Menteri Komunikasi dan Digital Nomor 11 Tahun 2022 tentang Tata Kelola Penyelenggaraan Sertifikasi Elektronik

Peraturan Menteri Komunikasi dan Digital Nomor 11 Tahun 2022 tentang Tata Kelola Penyelenggaraan Sertifikasi Elektronik merupakan regulasi yang mengatur tata cara penyelenggaraan sertifikasi elektronik di Indonesia, menggantikan Peraturan Menteri Komunikasi dan Digital Nomor 11 Tahun 2018. peraturan Menteri Komunikasi dan Digital Nomor 11 Tahun 2022 memperkuat tata kelola penyelenggaraan sertifikasi elektronik di Indonesia dengan mengatur PSrE, penerbitan sertifikat elektronik, dan pengawasan untuk memastikan keamanan dan keandalan transaksi elektronik.

Ketentuan ini telah diatur dalam Pasal 2 Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yang pada intinya menyatakan bahwa setiap individu yang melakukan tindakan atau perbuatan hukum terkait elektronik, termasuk Penyedia Sistem Elektronik (PSE), wajib mematuhi UU ITE serta peraturan pemerintah turunannya. Dengan demikian, meskipun berada di luar wilayah atau hukum Indonesia, jika seseorang melakukan perbuatan hukum terkait elektronik yang berlaku di Indonesia, maka ia harus mematuhi ketentuan dan prosedur hukum yang berlaku di Indonesia.[67]

---

[66] H Syafa'at Anugrah Pradana And Muhammad Andri Alvian, 'Kompabilitas Mekanisme Omnibus Law Dalam Pengaturan Perpajakan', *Jurnal Ilmu Hukum Amanna Gappa*, 21.1 (2021), Pp. 114–15.

[67] Kanti Rahayu, Nathania Salsabila Marikar Ssahib., Soesi Idayanti. dan, 'Problematika Aturan Penyelenggara Sistem Elektronik (PSE) Di Indonesia', *Pancasakti Law Journal*, 1.1 (2023), p.

Peraturan Menteri Komunikasi dan Digital Nomor 11 Tahun 2022 tentang Tata Kelola Penyelenggaraan Sertifikasi Elektronik (Permenkominfo 11/2022) merupakan regulasi yang disusun untuk memperbarui ketentuan sebelumnya, yaitu Permenkominfo Nomor 11 Tahun 2018, yang dianggap tidak lagi relevan dengan kebutuhan hukum masyarakat di era digital yang terus berkembang. Regulasi ini berfokus pada pengaturan tata kelola penyelenggaraan sertifikasi elektronik untuk mendukung keamanan, keabsahan, dan kepercayaan dalam transaksi elektronik, sejalan dengan Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP 71/2019). Permenkomdigi 11/2022 menggantikan aturan lama untuk memastikan bahwa infrastruktur dan layanan sertifikasi elektronik, termasuk tanda tangan elektronik, dapat dioperasikan dengan standar yang lebih sesuai dengan perkembangan teknologi dan kebutuhan hukum saat ini.

Regulasi ini mendefinisikan sistem elektronik sebagai serangkaian perangkat dan prosedur elektronik untuk mengelola informasi elektronik, mulai dari pengumpulan, pengolahan, hingga penyebaran, serta transaksi elektronik sebagai perbuatan hukum yang dilakukan melalui komputer atau media elektronik lainnya. Penyelenggara Sertifikasi Elektronik (PSrE), baik PSrE Indonesia yang berbadan hukum Indonesia dan berdomisili di dalam negeri maupun PSrE Asing yang beroperasi di luar yurisdiksi Indonesia, diatur untuk memastikan bahwa mereka berfungsi sebagai pihak tepercaya yang mengeluarkan dan mengaudit sertifikat elektronik. PSrE Indonesia memiliki kewenangan untuk memeriksa kebenaran identitas, memperpanjang masa berlaku, serta memblokir atau mencabut sertifikat elektronik, baik secara mandiri maupun melalui kerja sama dengan pihak lain, sebagaimana diatur dalam pasal-pasal seperti Pasal 51, 53, 54, 56, 63, 67, 69, 71, dan 72 dari PP 71/2019. PSrE juga wajib memenuhi standar operasional yang mencakup

---

69 <https://fh.pps-upstegal.ac.id/index.php/plj/article/view/8%0Ahttps://fh.pps-upstegal.ac.id/index.php/plj/article/download/8/7>.

kemampuan sumber daya manusia dan sistem elektronik untuk menjamin keandalan penerbitan sertifikat.

Permenkomdigi 11/2022 menekankan pentingnya Pernyataan Penyelenggaraan Sertifikasi Elektronik (Certification Practice Statement), yaitu prosedur operasional yang mengatur tata cara penerbitan sertifikat elektronik, untuk memastikan proses yang transparan dan terstandarisasi. Regulasi ini juga mengatur peran Kementerian Komunikasi dan Informatika sebagai pengawas, dengan Direktur Jenderal memiliki tanggung jawab untuk menyediakan layanan sertifikasi elektronik jika kebutuhan tertentu belum terpenuhi oleh PSrE. Dalam hal pengawasan, Tim Pengawas Penyelenggara Sertifikasi Elektronik dibentuk untuk menilai kelayakan PSrE berdasarkan kompetensi sumber daya manusia dan kecukupan sistem elektronik, terutama jika lembaga sertifikasi keandalan belum tersedia.

Dari perspektif hak asasi manusia (HAM), regulasi ini mendukung perlindungan privasi dengan memastikan bahwa sertifikat elektronik, yang digunakan untuk autentikasi dan verifikasi identitas dalam transaksi digital, dilindungi dari penyalahgunaan seperti peretasan atau pemalsuan identitas.

Namun, tantangan muncul dalam implementasi, seperti kebutuhan koordinasi yang lebih baik antarlembaga untuk menghindari tumpang tindih kewenangan, serta potensi ketidaksesuaian dengan praktik global yang dapat menghambat kerja sama internasional, misalnya dengan negara seperti Singapura yang memiliki infrastruktur keamanan siber lebih maju. Selain itu, sanksi administratif untuk pelanggaran, seperti kelalaian PSrE dalam menjaga keamanan sistem, diatur untuk memastikan kepatuhan, meskipun detailnya diserahkan kepada peraturan menteri lebih lanjut.

Berdasarkan Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) serta Peraturan Pemerintah No. 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE), tanda tangan elektronik diakui secara sah menurut hukum di Indonesia apabila memenuhi syarat-

syarat berikut: keaslian (authentication), keutuhan (integrity), dan sifat nirsangkal (non-repudiation).[68]

Secara keseluruhan, Permenkominfo 11/2022 berupaya menciptakan ekosistem digital yang aman dan terpercaya dengan mengatur tata kelola sertifikasi elektronik secara lebih rinci, memperkuat keamanan siber, dan mendukung keabsahan transaksi elektronik. Namun, keberhasilannya bergantung pada kemampuan pemerintah untuk menangani tantangan implementasi, seperti peningkatan kapasitas sumber daya manusia, harmonisasi dengan regulasi lain seperti UU ITE dan UU PDP, serta penguatan kerja sama internasional untuk menghadapi ancaman siber lintas negara.[69] Regulasi ini menjadi langkah penting dalam menyeimbangkan inovasi teknologi dengan perlindungan HAM, khususnya privasi. Peraturan Menteri Komunikasi dan Informatika Nomor 11 Tahun 2022 mengatur Tata Kelola Penyelenggaraan Sertifikasi Elektronik di Indonesia. Implementasi yang diharapkan dari peraturan ini berfokus pada penguatan tata kelola, pengawasan, dan pengakuan hukum terhadap sertifikasi elektronik, termasuk tanda tangan elektronik, agar memenuhi standar keamanan dan keabsahan hukum. Peraturan Menteri Nomor 11 Tahun 2018 tentang Penyelenggaraan Sertifikasi Elektronik dicabut dan digantikan oleh peraturan ini untuk menyesuaikan dengan perkembangan kebutuhan hukum masyarakat. Pemerintah perlu menjamin ketersediaan infrastruktur teknis, seperti jaringan internet dan server pendukung layanan sertifikat digital, secara merata di seluruh wilayah Indonesia.[70]

Berdasarkan Peraturan Menteri Komunikasi dan Digital Nomor 11 Tahun 2018 tentang Penyelenggara Sertifikasi Elektronik, Penyelenggara Sertifikasi Elektronik (PSrE) diartikan sebagai badan hukum yang bertindak sebagai pihak terpercaya untuk menyediakan, mengelola, mengoperasikan infrastruktur sertifikasi

[68] 'Nathania Salsabila Marikar Sahib1 , Soesi Idayanti2 , Kanti Rahayu Problematika Aturan Penyelenggara Sistem Elektronik (PSE) di Indonesia no. 1 (2024).

[69] Syarifaatul Hidayah, 'Tantangan Dan Peluang Sertifikat Elektronik Dalam Reformasi Pendaftaran Tanah Di Era Digital .', 1.6 (2024), pp. 186–99.

[70] H. Syafa'at Anugrah and Rustam Magun Pikahulan, 'Mulawarman LawReview', *Mulawarman Law Review*, 4.1 (2019), pp. 1–15.

elektronik, serta memberikan dan mengaudit sertifikat elektronik. Kegiatan penyelenggaraan sertifikasi elektronik mencakup penyediaan, pengelolaan, pengoperasian infrastruktur PSrE, dan/atau pemberian serta audit sertifikat elektronik. PSrE yang beroperasi di Indonesia wajib mengikuti prinsip satu induk, di mana mereka harus mendapatkan pengakuan dari Menteri dengan berinduk pada PSrE induk yang diselenggarakan oleh Menteri.[71]

Implementasi ini mengharuskan semua pemangku kepentingan, termasuk PSrE, untuk mengadopsi ketentuan baru yang lebih relevan dan sesuai dengan dinamika teknologi, Pemenuhan standar sertifikasi elektronik, sebagaimana diatur dalam Peraturan Menteri Komunikasi dan Digital Nomor 11 Tahun 2022, merujuk pada upaya untuk memastikan bahwa sertifikasi elektronik, termasuk tanda tangan elektronik, memenuhi kriteria tertentu agar diakui sah secara hukum di Indonesia. Maksudnya adalah menciptakan sistem yang dapat menjamin keaslian identitas pengguna, menjaga keutuhan data elektronik agar tidak diubah atau dimanipulasi, serta memastikan bahwa tindakan hukum yang dilakukan dengan sertifikasi tersebut tidak dapat disangkal oleh pihak yang menggunakannya. Sertifikat elektronik umumnya menggunakan standar teknis X.509 versi 3 (X.509.v3) yang merupakan standar internasional untuk sertifikat digital, berfungsi untuk mengidentifikasi subjek hukum dalam transaksi elektronik dan mendukung tanda tangan elektronik serta enkripsi data.[72]

Penelitian ini menyoroti tiga aspek utama terkait implementasi perlindungan data pribadi berdasarkan UU PDP. Pertama, dari segi regulasi, terdapat kebutuhan mendesak untuk mempercepat penyusunan peraturan pelaksana UU PDP guna memberikan panduan operasional yang lebih rinci dan jelas bagi pemangku kepentingan. Proses ini mencakup pembentukan peraturan pemerintah, peraturan menteri, dan regulasi teknis lainnya yang diperlukan untuk mengoperasikan prinsip-

[71] Wita Dewisari and Tasya Author, 'Analisis Keamanan Penyelenggara Sertifikasi Elektronik Indonesia : PT Privy Identitas Digital', 18218037 (2022).

[72] Yulianto Wibowo and Ida Aryati Dpw, 'Tinjauan Yuridis Tentang Perlindungan Data Pribadi Masyarakat Pada Era Digitalisasi', 18.01 (2025), pp. 1–6.

prinsip perlindungan data. Partisipasi aktif masyarakat dalam penyusunan regulasi ini penting untuk memastikan bahwa aturan yang dihasilkan mencerminkan kepentingan semua pihak. Kedua, dari aspek infrastruktur teknologi, penelitian menekankan perlunya memperkuat kapasitas teknologi nasional untuk menghadapi ancaman keamanan siber yang semakin kompleks. Upaya ini meliputi pembaruan infrastruktur digital, pengembangan sistem keamanan yang lebih mutakhir, serta peningkatan kemampuan untuk mendeteksi dan menangani ancaman siber. Investasi dalam teknologi ini harus diimbangi dengan pengembangan sumber daya manusia yang memiliki keahlian di bidang keamanan siber dan perlindungan data.

Ketiga, penelitian menegaskan pentingnya meningkatkan koordinasi dan sinergi antarlembaga untuk mendukung implementasi perlindungan data pribadi. Tantangan fragmentasi kewenangan dan ego sektoral dapat diatasi melalui pembentukan mekanisme koordinasi yang lebih efektif, seperti pembentukan lembaga pengawas independen yang kuat, penetapan protokol koordinasi yang jelas, dan pengembangan sistem informasi terintegrasi untuk mendukung pengawasan serta penegakan hukum.

Hal ini melibatkan pengembangan infrastruktur teknis oleh Penyelenggara Sertifikasi Elektronik (PSrE) yang mencakup pengolahan, penyimpanan, dan penyebaran informasi elektronik dengan standar keamanan tinggi. Tujuannya adalah memberikan kepastian hukum bagi transaksi elektronik, baik yang dilakukan oleh individu, badan usaha, maupun instansi pemerintah, sehingga transaksi tersebut dapat dipercaya dan sesuai dengan ketentuan Undang-Undang Informasi dan Transaksi Elektronik serta peraturan turunannya. Berdasarkan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), Penyelenggara Sertifikasi Elektronik (PSrE) didefinisikan sebagai badan hukum yang berperan sebagai pihak terpercaya yang bertugas memberikan dan mengaudit Sertifikat Elektronik (Pasal 1 angka 10).

Sertifikat Elektronik sendiri dijelaskan pada Pasal 1 angka 9 UU ITE sebagai sertifikat berbentuk elektronik yang berisi Tanda Tangan Elektronik dan identitas

yang mencerminkan status subjek hukum para pihak dalam Transaksi Elektronik, yang diterbitkan oleh PSrE. Dari ketentuan pasal tersebut, muncul pertanyaan lebih lanjut mengenai peran PSrE dalam memberikan dan mengaudit Sertifikat Elektronik, jenis Sertifikat Elektronik yang dimaksud, serta fungsinya bagi pelaku usaha. Dalam konteks keamanan dan legalitas transaksi di internet, khususnya untuk menjamin keamanan transaksi perdagangan elektronik, peran PSrE menjadi krusial. Hal ini menimbulkan isu hukum terkait keterlibatan PSrE dalam aktivitas jual beli di ranah digital untuk memastikan kepercayaan dan keabsahan transaksi.

Selain sertifikat elektronik untuk tanda tangan digital, ada juga sertifikat server (sertifikat SSL) yang digunakan untuk mengamankan komunikasi situs web, meskipun pengaturannya tidak sedetail sertifikat tanda tangan elektronik Sertifikat server, dalam konteks teknologi informasi dan keamanan siber, adalah dokumen digital yang diterbitkan oleh otoritas sertifikasi (Certificate Authority) untuk memverifikasi identitas sebuah server dalam jaringan, seperti situs web atau layanan daring. Sertifikat ini berfungsi untuk memastikan bahwa komunikasi antara pengguna dan server dilakukan secara aman melalui protokol seperti HTTPS, dengan menggunakan enkripsi SSL/TLS. Sertifikat server berisi informasi seperti nama domain, kunci publik, dan tanda tangan digital dari otoritas sertifikasi, yang menjamin keaslian server dan mencegah penyadapan atau manipulasi data oleh pihak ketiga. Dalam transaksi elektronik, sertifikat server membantu membangun kepercayaan pengguna dengan memastikan bahwa mereka terhubung ke server yang sah, sehingga mendukung keamanan dan legalitas aktivitas daring, termasuk perdagangan elektronik. Di Indonesia, sesuai dengan regulasi seperti UU ITE dan Peraturan Menteri Kominfo, sertifikat ini dikelola oleh Penyelenggara Sertifikasi Elektronik (PSrE) untuk memenuhi standar keamanan dan kepastian hukum.[73]

[73] Siti Maisarah, 'Fungsi Sertifikasi Elektronik Bagi Pelaku Usaha Dalam Transaksi Perdagangan Elektronik', *Badamai Law Journal*, 4.1 (2019), p. 126, doi:10.32801/damai.v4i1.9233.

Sertifikat elektronik memiliki akibat hukum yang sama dengan dokumen tertulis jika memenuhi ketentuan undang-undang, khususnya UU ITE dan Peraturan Pemerintah tentang Sistem dan Transaksi Elektronik (PP PSTE).

Akan tetapi, pada dasarnya peraturan ini dibuat untuk melaksanakan ketentuan dalam beberapa pasal Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, khususnya yang berkaitan dengan lembaga sertifikasi Penyelenggara Sertifikasi Elektronik terakreditasi, dasar Hukum dan Kebutuhan Pelaksanaan PP Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik mengatur secara umum sistem dan transaksi elektronik, termasuk sertifikasi elektronik. Namun, PP ini bersifat umum dan memerlukan peraturan teknis untuk mengatur aspek operasional, seperti tata kelola, verifikasi identitas, dan pengarsipan data dalam penyelenggaraan sertifikasi elektronik. Permenkomdigi Nomor 11 Tahun 2022 hadir untuk mengisi kebutuhan ini dengan memberikan panduan teknis dan prosedural. Permenkomdigi Nomor 11 Tahun 2022 secara spesifik mengatur tata kelola penyelenggaraan sertifikasi elektronik, seperti yang disebutkan dalam web JDIH Kemkomdigi. Ini mencakup pengelolaan informasi dan dokumen elektronik, verifikasi identitas pengirim dan penerima, serta pengarsipan log operasional, yang semuanya merupakan amanat dari PP Nomor 71 Tahun 2019 untuk memastikan keandalan dan keamanan sistem elektronik. Peraturan ini juga bertujuan untuk menyesuaikan ketentuan sebelumnya (misalnya, Permenkomdigi Nomor 11 Tahun 2018) dengan PP Nomor 71 Tahun 2019. Penyelenggara Sertifikasi Elektronik (PSrE) yang sudah terdaftar atau tersertifikasi diberikan waktu satu tahun untuk menyesuaikan operasionalnya dengan aturan baru, seperti yang diatur dalam Permenkomdigi Nomor 11 Tahun 2022. PP Nomor 71 Tahun 2019 menunjuk Kementerian Komunikasi dan Digital sebagai pihak yang bertanggung jawab atas pengawasan dan pengaturan sistem elektronik. Oleh karena itu, Permenkominfo Nomor 11 Tahun 2022 menjadi instrumen untuk

melaksanakan tugas tersebut, termasuk pengelolaan sistem elektronik oleh Direktur Jenderal untuk keperluan pengawasan, penilaian kelaikan, dan penegakan hukum.[74]

Permenkomdigi Nomor 11 Tahun 2022 merupakan peraturan pelaksana yang berada di bawah Peraturan Pemerintah Nomor 71 Tahun 2019. PP tersebut mengatur secara umum sistem dan transaksi elektronik, termasuk sertifikasi elektronik. Namun, karena PP bersifat umum, diperlukan peraturan menteri untuk menjabarkan aspek teknis dan operasional, seperti tata kelola, verifikasi identitas, dan pengarsipan data. Pembentukan Permenkominfo ini sesuai dengan prinsip hierarki, di mana peraturan yang lebih rendah (Permen) tidak boleh bertentangan dengan peraturan yang lebih tinggi (PP dan UU). Permenkomdigi Nomor 11 Tahun 2022 mengacu pada PP Nomor 71 Tahun 2019 dan UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagai landasan hukumnya. Dari Hans Kelsen, negara sebenarnya merupakan *Zwangsordnun,* ialah tertib hukum yang bersifat memaksa yang menimbulkan hak memerintah dan diperintahkan tunduk.[75] Dalam konteks Permen Komdigi No. 11 Tahun 2022, peraturan ini dibuat untuk melaksanakan ketentuan yang diatur dalam Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, sehingga Permen ini harus selaras dan tidak bertentangan dengan PP tersebut dan peraturan yang lebih tinggi dalam hierarki.

Permenkomdigi Nomor 11 Tahun 2022 memiliki beberapa pasal kunci yang mengatur tata kelola penyelenggaraan sertifikasi elektronik secara spesifik. Misalnya, Pasal 6 ayat (1) menetapkan bahwa Penyelenggara Sertifikasi Elektronik (PSrE) wajib melakukan verifikasi identitas pemohon sertifikat elektronik dengan memastikan kebenaran data pribadi atau badan hukum melalui dokumen resmi,

---

[74] Yasmina Fayza, Muhamad Amirulloh, and Mustofa Haffas, 'Berdasarkan Peraturan Perundang-Undangan Terkait Sales Of Covid-19 Vaccine Certificate By Facebook Users Based On Related Law Indonesia Menjamin Hak Komunikasi Warga Negara Melalui Pasal 28F Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 Yang M', no. 42 (2022), pp. 16–32.

[75] Hasananuddin Hasan, 'Hierarki Peraturan Perundang-Undangan Negara Republik Indonesia Sebagai Suatu Sistem', *Madani Legal Review*, 1.2 (2017), pp. 120–30, doi:10.31850/malrev.v1i2.32.

seperti KTP, paspor, atau akta pendirian perusahaan, untuk menjamin keabsahan identitas dalam transaksi elektronik. Pasal 13 ayat (1) mengatur bahwa PSrE harus menyimpan log operasional selama minimal 10 tahun, mencakup data transaksi dan aktivitas sistem, untuk keperluan audit dan penegakan hukum. Pasal 25 mengamanatkan bahwa PSrE Indonesia wajib menggunakan infrastruktur teknologi yang berlokasi di Indonesia, kecuali untuk keperluan interoperabilitas internasional yang diizinkan oleh Kementerian Kominfo, untuk memastikan keamanan data nasional.

Pasal 45 ayat (1) dan (2) memberikan masa transisi satu tahun sejak 20 Desember 2022 bagi PSrE yang sudah terdaftar untuk menyesuaikan operasionalnya dengan ketentuan baru, seperti peningkatan standar teknis atau pelaporan. Pasal 47 mencabut Permenkominfo Nomor 11 Tahun 2018, menegaskan bahwa aturan ini menggantikan regulasi sebelumnya untuk menyelaraskan dengan PP Nomor 71 Tahun 2019. Pada pasal 10, diatur bahwa Penyelenggara Sertifikasi Elektronik (PSrE) wajib menerbitkan sertifikat elektronik yang memuat data identitas pemohon dan kunci publik, serta memastikan sertifikat itu terlindungi dari pemalsuan dengan teknologi kriptografi. Pasal 19 juga menarik, mewajibkan PSrE untuk menyediakan sistem yang bisa memverifikasi status sertifikat elektronik secara real-time, biar transaksi aman dan terpercaya.

Pasal-pasal ini menunjukkan fokus pada keamanan, kepatuhan, dan penyesuaian teknis dalam ekosistem sertifikasi elektronik.

B. Sistem Hukum Sertifikasi Elektronik di Singapura

1. UNCITRAL *model law on electronic signature*

UNCITRAL Model Law on Electronic Signatures (Model Hukum UNCITRAL tentang Tanda Tangan Elektronik) adalah sebuah instrumen hukum internasional yang dirancang untuk membantu negara-negara mengembangkan kerangka hukum nasional yang modern dan konsisten dalam hal penggunaan tanda tangan elektronik

dalam transaksi elektronik.[76] Merupakan *model law* (undang-undang contoh) yang disusun oleh **UNCITRAL** (United Nations Commission on International Trade Law / Komisi Hukum Perdagangan Internasional **PBB**) dan diadopsi pada tahun 2001. Tujuannya adalah untuk memberikan kerangka hukum yang seragam dan dapat diadopsi oleh negara-negara dalam mengatur dan mengakui legalitas tanda tangan elektronik.

UNCITRAL Model Law menekankan bahwa tanda tangan elektronik harus andal agar diakui secara hukum. Salah satu cara untuk memastikan keandalan tersebut adalah melalui sertifikat elektronik yang dikeluarkan oleh pihak terpercaya. Model Law ini dirancang untuk memfasilitasi penggunaan tanda tangan elektronik dengan menetapkan kriteria keandalan teknis yang memungkinkan tanda tangan elektronik memiliki efek hukum yang setara dengan tanda tangan tangan basah (tanda tangan manual).

Di Singapura, lembaga yang berfungsi seperti PSrE disebut Certification Authority (CA). Mereka juga menerbitkan sertifikat digital untuk mendukung tanda tangan elektronik yang aman dan diakui hukum. IMDA juga mengelola National Trust Framework untuk memastikan standar keamanan tinggi dalam transaksi digital. Contoh CA di Singapura adalah Netrust Pte Ltd (CA terbesar dan bersertifikasi nasional) dan SingCert (bagian dari GovTech, lebih fokus ke keamanan siber).[77]

ETA 2021 mengakui dokumen elektronik dan tanda tangan elektronik sebagai alat bukti hukum yang sah, setara dengan dokumen fisik dan tanda tangan manual, selama memenuhi syarat keandalan, seperti identifikasi penanda tangan dan metode autentikasi yang terpercaya, misalnya melalui Public Key Infrastructure (PKI). Tanda tangan elektronik aman, yang didukung sertifikat elektronik dari Certification Authority (CA) terakreditasi, dianggap otomatis sah secara hukum, seperti tanda

[76] Syifaun Nafisah, 'Electronic Information and Transaction Law, a Means of Information Control in Libraries', Jurnal Kajian Informasi & Perpustakaan, 11.1 (2023), p. 57, doi:10.24198/jkip.v11i1.35354.

[77] Syafa'at Anugrah Pradana, Sunandar, and EMi Asriati Makmur, 'Urgensi Kajian Fiqh Al-Bi'ah Dalam Pemenuhan Urusan Konkuren Bidang Pelayanan Kebersihan Di Kabupaten Luwu Timur', *Gorontalo Law Review*, 5.2 (2022), pp. 486–97.

tangan digital melalui SingPass yang dikelola oleh Assurity Trusted Solutions. Namun, penggunaan tanda tangan elektronik bersifat sukarela, dan dokumen tertentu seperti surat wasiat atau akta kepemilikan tanah dikecualikan, kecuali diatur oleh hukum sektoral. Electronic Transactions (Amendment) Act 2021 Singapura merupakan langkah penting dalam modernisasi hukum transaksi elektronik dengan mengadopsi standar internasional UNCITRAL untuk dokumen elektronik pindahtangan.

Hal ini meningkatkan efisiensi perdagangan internasional dan memberikan kepastian hukum bagi penggunaan dokumen elektronik dalam sektor logistik dan keuangan. Penyelenggara Sertifikasi Elektronik (CA) bertugas menerbitkan sertifikat elektronik untuk memverifikasi identitas dalam transaksi elektronik, berperan seperti notaris digital. CA dapat memilih untuk diakreditasi secara sukarela oleh Infocomm Media Development Authority (IMDA), yang menetapkan standar keamanan ketat, termasuk audit berkala dan kepatuhan terhadap Electronic Transactions (Certification Authority) Regulations 2010. Hanya dua CA terakreditasi hingga 2025, yaitu Netrust Pte Ltd dan Assurity Trusted Solutions Pte Ltd, meskipun CA tidak terakreditasi tetap wajib menjaga keandalan sistem dan kerahasiaan kunci penandatanganan.

CA bertanggung jawab untuk penerbitan, perpanjangan, penangguhan, dan pencabutan sertifikat elektronik, dengan pengawasan ketat dari Controller of Certification Authorities di bawah IMDA, yang juga berwenang menyelidiki pelanggaran, termasuk aktivitas siber ilegal.[78] Keselarasan antara regulasi hukum dagang nasional dan standar internasional dapat dilihat dari beberapa sudut. Salah satunya, prinsip hukum internasional seperti yang diatur oleh UNIDROIT dapat diadopsi ke dalam hukum nasional untuk memfasilitasi transaksi dan menyatukan sistem hukum.

Walaupun Undang-Undang yang mengesahkan perjanjian internasional tidak serta-merta mengintegrasikan norma-norma hukum internasional ke dalam sistem

[78] Penyelenggaraan Sistem Elektronik and Pribadi D I Indonesia, 'Aktual Justice', 5.2, pp. 132–45.

hukum nasional Indonesia, proses adaptasi tetap dibutuhkan agar isi dari perjanjian tersebut dapat diakomodasi dalam peraturan perundang-undangan nasional. Selanjutnya, hukum perdagangan internasional yang mengatur interaksi ekonomi lintas negara dapat membawa pengaruh besar terhadap individu maupun entitas hukum di dalam negeri. Di samping itu, sejumlah asas dalam hukum dagang seperti prinsip perlakuan nasional, perlakuan paling disukai, akses pasar terbuka, perlakuan preferensial, serta prinsip keadilan, dapat diaplikasikan secara luas dalam interaksi ekonomi antarnegara.

prinsip-prinsip yang tertuang dalam ketentuan WTO seperti perlakuan paling disukai, perlakuan nasional, asas timbal balik, perdagangan bebas, perdagangan yang adil, dan keterbukaan, dapat dijadikan acuan dalam merancang regulasi hukum perdagangan nasional yang lebih selaras dengan standar internasional. Kajian terhadap langkah-langkah harmonisasi antara regulasi hukum dagang nasional dan standar internasional menjadi elemen krusial dalam dinamika perdagangan global yang semakin berkembang. Salah satu entitas yang memiliki peranan sentral dalam mendukung proses harmonisasi ini adalah Komisi Perserikatan Bangsa-Bangsa untuk Hukum Dagang Internasional (UNCITRAL). Lembaga ini telah lama berkontribusi secara signifikan dalam menyatukan sistem hukum dagang di tingkat global, dengan penekanan pada penciptaan perangkat hukum yang bersifat universal dan dapat diterapkan lintas negara.[79]

Melalui pengembangan dan penyebaran berbagai instrumen hukum seperti konvensi, model undang-undang, pedoman, serta prinsip-prinsip hukum internasional, UNCITRAL berupaya membentuk landasan hukum yang seragam dan diterima secara luas dalam konteks perdagangan. Meski UNCITRAL berperan besar, keterlibatan aktif dari berbagai pihak, termasuk pemerintah, pelaku usaha, dan masyarakat sipil, tetap sangat penting untuk memastikan bahwa proses harmonisasi

[79] Pesman Laia, 'Analisis Perspektif Komparatif Regulasi Hukum Dagang Nasional Dengan Standar Internasional', *Jurnal Kajian Hukum Dan Kebijakan Publik*, 1.2 (2024), pp. 174–79.

ini mampu mengakomodasi kepentingan serta sudut pandang yang beragam di tingkat domestik maupun internasional.

Dengan demikian, melalui kontribusi aktif UNCITRAL dan kolaborasi yang inklusif, proses penyesuaian regulasi hukum dagang nasional dengan standar internasional dapat terus berkembang menuju sistem perdagangan internasional yang lebih efisien, adil, dan berkelanjutan.

Berdasarkan prinsip-prinsip dasar yang mendasari Pasal 7 dari Model Hukum UNCITRAL tentang Perdagangan Elektronik (selalu disebutkan dengan judul lengkapnya dalam publikasi ini untuk menghindari kebingungan) terkait pemenuhan fungsi tanda tangan dalam lingkungan elektronik, Model Hukum baru ini dirancang untuk membantu negara-negara dalam membangun kerangka legislatif yang modern, terharmonisasi, dan adil untuk menangani isu-isu tanda tangan elektronik secara lebih efektif. Sebagai tambahan yang sederhana namun signifikan terhadap Model Hukum UNCITRAL tentang Perdagangan Elektronik, Model Hukum baru ini menawarkan standar praktis untuk mengukur keandalan teknis tanda tangan elektronik. Selain itu, Model Hukum ini menyediakan hubungan antara keandalan teknis tersebut dan efektivitas hukum yang dapat diharapkan dari suatu tanda tangan elektronik tertentu.

Model Hukum ini memperluas Model Hukum UNCITRAL tentang Perdagangan Elektronik secara substansial dengan mengadopsi pendekatan di mana efektivitas hukum dari teknik tanda tangan elektronik tertentu dapat ditentukan sebelumnya (atau dinilai sebelum benar-benar digunakan). Dengan demikian, Model Hukum ini dimaksudkan untuk memupuk pemahaman tentang tanda tangan elektronik dan keyakinan bahwa teknik tanda tangan elektronik tertentu dapat diandalkan dalam transaksi yang signifikan secara hukum.[80]

Lebih lanjut, dengan menetapkan seperangkat aturan perilaku dasar yang fleksibel untuk berbagai pihak yang mungkin terlibat dalam penggunaan tanda tangan

[80] United Nations, *UNCITRAL Model Law on Electronic Signatures*, *United Nations Publication*, 2002 <http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2001Model_signatures.html> .

elektronik (yaitu, penandatangan, pihak yang mengandalkan tanda tangan, dan penyedia layanan sertifikasi pihak ketiga), Model Hukum ini dapat membantu membentuk praktik perdagangan yang lebih harmonis di ruang siber.

Istilah "standar" tidak seharusnya dibatasi hanya pada standar yang dikembangkan, misalnya, oleh International Organization for Standardization (ISO) dan Internet Engineering Task Force (IETF), atau pada standar teknis lainnya. Kata "standar" harus diartikan dalam pengertian yang luas, yang mencakup praktik industri dan kebiasaan perdagangan, "standar sukarela" dokumen yang berasal dari organisasi internasional seperti International Chamber of Commerce, badan akreditasi regional yang beroperasi di bawah naungan ISO , badan standardisasi regional, serta karya UNCITRAL sendiri (termasuk Model Law ini dan UNCITRAL Model Law on Electronic Commerce).

Ketiadaan standar yang relevan seharusnya tidak menghalangi orang atau otoritas yang berwenang untuk membuat penilaian Mengenai referensi pada standar yang "diakui", mungkin timbul pertanyaan tentang apa yang dimaksud dengan **"**pengakuan**"** dan oleh siapa pengakuan tersebut diperlukan. Model Law tidak memaksakan atau mengutamakan teknologi tertentu sehingga dapat mengakomodasi perkembangan teknologi di masa depan.

Hal ini membuat hukum ini "futureproof" Dalam setiap proses hukum, tidak ada aturan pembuktian yang boleh diterapkan untuk menolak penerimaan pesan data sebagai bukti hanya karena pesan tersebut berbentuk pesan data. Tanda tangan elektronik adalah sesuatu yang diletakkan pada dokumen elektronik (chip elektronik) yang berbentuk huruf, angka, simbol, tanda, atau lainnya, yang memiliki karakteristik khas dan unik yang memungkinkan untuk mengidentifikasi penandatangan dan membedakannya dari orang lain, Data dalam bentuk elektronik yang dimasukkan ke dalam, ditambahkan pada, atau secara logis terkait dengan pesan data, yang dapat digunakan untuk mengidentifikasi identitas penandatangan sehubungan dengan pesan

data tersebut, dan untuk menunjukkan persetujuan penandatangan terhadap informasi yang terkandung dalam pesan data tersebut.[81]

Dari definisi ini, jelas bahwa UNCITRAL tidak membatasi konsep tanda tangan elektronik atau menentukan metode spesifik yang harus digunakan untuk tanda tangan elektronik. UNCITRAL memberikan kebebasan kepada individu atau negara untuk memilih metode selama metode tersebut memungkinkan identifikasi identitas penandatangan dan menunjukkan persetujuannya terhadap informasi dalam pesan data. Dalam legislasi Yordania, definisi tanda tangan elektronik diatur dalam Pasal 2 dari *Undang-Undang Transaksi Elektronik*, yang mendefinisikannya sebagai data yang berbentuk huruf, tanda, atau lainnya, yang dimasukkan dalam bentuk elektronik atau media serupa lainnya ke dalam catatan elektronik, atau ditambahkan padanya, atau terkait dengannya, dengan tujuan untuk mengidentifikasi identitas pemilik tanda tangan, menunjukkan keunikan penggunaannya, dan membedakannya dari yang lain.

Adapun Model Hukum UNCITRAL tentang Tanda Tangan Elektronik tidak mengatur efek dari tanda tangan elektronik pada catatan elektronik, melainkan menyerahkan hal ini kepada Model Hukum UNCITRAL tentang Perdagangan Elektronik. Lembaga yang menyelaraskan hukum perdagangan elektronik adalah UNCITRAL, organ subsidier PBB. Pengaturan tanda tangan elektronik diatur dalam Model Hukum UNCITRAL tentang Perdagangan Elektronik 1996 dan Model Hukum UNCITRAL tentang Tanda Tangan Elektronik 2001, menunjukkan kebutuhan global akan sesuai dengan perkembangan teknologi transaksi.[82]

Usulan UNCITRAL menangani implikasi filosofis doktriner dengan cara yang mirip seperti Aleksander Agung menghadapi simpul Gordian, yaitu dengan mengusulkan "penyeragaman" yurisprudensi arbitrasi global melalui pembalikan

---

[81] A. H. Jararwah **Electronic Signature (A comparative Analytical Study in Light of the UNCITRAL Model Law on Electronic Signatures and Jordanian Legislation)**Electronic Signatures, : ‘: ةمدقلما’, 6 (2025), pp. 8–17.

[82] Tanda Tangan and others, ‘INTERNASIONAL’, 5.1 (2022), pp. 87–96, doi:10.28946/slrev.Vol5.Iss1.603.pp71-85.2.

radikal. Dalam Pasal 13 dari Model Hukum UNCITRAL tentang Perdagangan Elektronik beserta Panduan Penerapannya, direkomendasikan bahwa undang-undang harus membebankan pembuktian pemalsuan atau kehati-hatian kepada penandatangan yang dituduh, sehingga hampir sepenuhnya membalikkan tradisi yudisial dan bertentangan dengan hukum yang berlaku, seperti Electronic Transactions Act (CWTH) 1999. Bagian 15 dari undang-undang tersebut menolak Pasal 13 UNCITRAL dan menetapkan bahwa imputabilitas tanda tangan digital hanya ditentukan melalui persetujuan eksplisit dari penandatangan yang dituduh.

Kedua ketentuan ini keliru karena menciptakan ketidakseimbangan risiko, namun dalam arah yang berlawanan. Solusi arbitrase simpul Gordian dari UNCITRAL untuk hukum yang mengizinkan autentikator di mana penandatangan tidak memiliki kendali atas pemalsuan bukanlah teori konspirasi fiktif. Hal ini memang tertulis dalam rekomendasi komisi hukum Perserikatan Bangsa-Bangsa.[83] Model Hukum UNCITRAL tentang Tanda Tangan Elektronik adalah panduan dari PBB untuk membantu negara membuat aturan hukum yang mendukung penggunaan tanda tangan elektronik dalam transaksi, terutama perdagangan elektronik. Tujuannya adalah memastikan tanda tangan elektronik diakui secara hukum seperti tanda tangan tulisan tangan, asalkan bisa mengidentifikasi penandatangan dan menunjukkan persetujuannya terhadap dokumen. Model ini tidak memaksakan teknologi tertentu, jadi negara bebas memilih metode tanda tangan elektronik selama cukup andal. Ini juga mengatur peran pihak seperti penandatangan, pihak yang mempercayai tanda tangan, dan penyedia sertifikasi, serta mendorong pengakuan tanda tangan elektronik lintas negara. Meski fleksibel, model ini tidak mengatur detail teknologi atau isu seperti perlindungan data, sehingga negara harus menyesuaikan dengan hukum lokal mereka. Di Indonesia, prinsip ini tercermin dalam UU ITE, tapi implementasinya masih perlu penguatan untuk keamanan dan harmonisasi global.

[83] Pedro A D Rezende, 'The Possible Laws on Digital / Electronic Signature : On the Proposed UNCITRAL Model Department of Computer Science Classification of Laws'.

Model Hukum UNCITRAL tentang Tanda Tangan Elektronik adalah kerangka hukum dari PBB untuk mengatur tanda tangan elektronik agar diakui sah seperti tanda tangan tulis. Aturan ini menekankan bahwa tanda tangan elektronik harus bisa mengidentifikasi penandatangan secara unik, menunjukkan persetujuan atas isi dokumen, dan menggunakan metode yang andal sesuai kebutuhan transaksi. Model ini netral teknologi, artinya tidak memaksa penggunaan teknologi tertentu seperti PKI atau biometrik, selama memenuhi syarat keandalan.

Model Hukum UNCITRAL juga mengatur kewajiban penandatangan, pihak yang mempercayai tanda tangan, dan penyedia sertifikasi (seperti otoritas sertifikat digital), serta mendorong pengakuan lintas batas agar tanda tangan elektronik dari satu negara diakui di negara lain. Dalam Pasal 6 dan 7, dijelaskan bahwa tanda tangan elektronik sah secara hukum jika memenuhi fungsi identifikasi dan persetujuan, sementara Pasal 11 menekankan harmonisasi internasional. Di Indonesia, prinsip ini diadopsi dalam UU No. 11/2008 tentang ITE, tapi tantangannya adalah memastikan keandalan teknologi dan keamanan siber. UNCITRAL Model Law on Electronic Signatures (2001) adalah kerangka hukum dari United Nations Commission on International Trade Law untuk mengatur tanda tangan elektronik agar memiliki kekuatan hukum setara dengan tanda tangan tulisan tangan dalam transaksi elektronik, terutama perdagangan lintas batas. Model ini menetapkan bahwa tanda tangan elektronik sah jika memenuhi tiga fungsi utama: mengidentifikasi penandatangan secara unik, menunjukkan persetujuan penandatangan terhadap isi dokumen, dan menggunakan metode yang andal sesuai tujuan transaksi. Pasal 6 menegaskan keabsahan hukum tanda tangan elektronik berdasarkan kriteria ini, sedangkan Pasal 7 memastikan tanda tangan elektronik dapat menggantikan tanda tangan tulis jika memenuhi syarat keandalan. Model ini netral teknologi, artinya tidak membatasi metode seperti kriptografi PKI, biometrik, atau teknologi lain, memberikan fleksibilitas kepada negara untuk menentukan standar teknis.

Pasal 8 mengatur kewajiban pihak yang mempercayai tanda tangan elektronik untuk memverifikasi keabsahannya secara wajar, sementara Pasal 9 menetapkan

standar keandalan teknologi, seperti keamanan data dan integritas sistem. Pasal 10 mengatur penyedia layanan sertifikasi (Certification Service Providers) yang menerbitkan sertifikat digital untuk memverifikasi identitas penandatangan, dan Pasal 11 mendorong pengakuan tanda tangan elektronik lintas batas untuk mendukung perdagangan global. Model ini melengkapi UNCITRAL Model Law on Electronic Commerce (1996), khususnya Pasal 5 dan 7, yang menetapkan bahwa dokumen atau tanda tangan elektronik tidak boleh ditolak keabsahannya hanya karena formatnya elektronik. Namun, model ini tidak mengatur detail teknologi atau isu perlindungan data, sehingga negara harus menyesuaikan dengan hukum lokal.

Di Indonesia, prinsip ini diadopsi dalam UU No. 11/2008 tentang Informasi dan Transaksi Elektronik (UU ITE), terutama Pasal 11, yang mengakui tanda tangan elektronik sebagai alat bukti sah jika memenuhi syarat keandalan, dan PP No. 71/2019, yang mengatur penyelenggara sertifikasi elektronik seperti BSrE. Tantangan di Indonesia meliputi harmonisasi dengan standar internasional, penguatan infrastruktur keamanan siber, dan akreditasi penyedia sertifikasi untuk mencegah pemalsuan. Meski fleksibel, model ini kadang dianggap kurang spesifik dalam menangani risiko teknologi modern seperti serangan siber atau blockchain, sehingga implementasi nasional perlu adaptasi ketat.[84]

Alasan Singapura mengadopsi UNCITRAL Model Law on Electronic Signatures (2001) melalui Electronic Transactions Act 2010 karena ingin menciptakan kerangka hukum yang mendukung perdagangan elektronik global dengan standar internasional yang netral teknologi, memastikan tanda tangan elektronik diakui sah, dan memberikan perlindungan hukum maksimal bagi warga serta bisnis dalam transaksi digital, sekaligus mendorong harmonisasi hukum lintas batas untuk mempermudah perdagangan internasional.

[84] Syafa'at Anugrah Pradana and others, 'Regulation of Esports in the Context of the Employment in Indonesia', *Amsir Law Journal*, 4.1 (2022), pp. 15–31, doi:10.36746/alj.v4i1.98.

2. *Electronic Transactions (Certification Authority) Regulations (*2010) & *Electronic Transactions (Amandement) Act* (2021*)*

Electronic Transactions (Certification Authority) Regulations 2010 (ETR) adalah peraturan turunan dari *Electronic Transactions Act (ETA)* di Singapura yang mengatur secara spesifik operasional dan akreditasi Penyelenggara Sertifikasi Elektronik (*Certification Authorities/CA*). Diberlakukan pada 2010 dan tetap relevan hingga 2025 sebagai pelengkap ETA 2021, ETR menetapkan standar teknis dan hukum untuk memastikan keamanan, keandalan, dan kepatuhan CA dalam menerbitkan sertifikat elektronik. Electronic Transactions Act (ETA) 2021 di Singapura adalah revisi dari Electronic Transactions Act (ETA) 2010 yang bertujuan memperkuat kerangka hukum untuk transaksi elektronik, meningkatkan keamanan siber, dan mendukung transformasi digital yang andal. Revisi ini diberlakukan pada 19 Maret 2021 setelah disahkan oleh Parlemen Singapura untuk menyesuaikan regulasi dengan perkembangan teknologi dan ancaman siber. ETA pertama kali diperkenalkan pada 1998 dan direvisi pada 2010 untuk mengadopsi prinsip-prinsip dari *UNCITRAL Model Law on Electronic Commerce 1996* dan *United Nations Convention on the Use of Electronic Communications in International Contracts (ECC)*. Singapura adalah negara yang responsif terhadap perkembangan internet. Menjadi pusat e-commerce internasional adalah salah satu tujuan utama Singapura untuk mewujudkan visinya sebagai pusat produk informasi dan teknologi global. Singapura telah merancang strategi untuk mencapai tujuan ini sejak awal munculnya internet pada tahun 1980. Implementasi strategi ini terdiri dari empat fase. Fase awal pada tahun 1980-1985 adalah realisasi sistem pemerintahan yang terkomputerisasi. Fase kedua, pada tahun 1986-1990, berupaya menjadikan akses informasi yang terkomputerisasi dan mudah diterima oleh seluruh masyarakat, sehingga pada fase ketiga di tahun 1990-1999, Singapura dapat menjadi 'Pulau Cerdas' dan pusat TI. Pada awal tahun 2000, Singapura memasuki fase keempat dengan mengubah negara ini menjadi Pusat TI Global dengan upaya besar untuk mengimplementasikan strateginya. Implementasi dimulai dengan komputerisasi industri, pemerintahan, dan

universitas. Pada fase ketiga, Singapura mulai merancang regulasi terkait penggunaan media baru.

ETR 2010 bertujuan untuk mendukung kepercayaan publik terhadap transaksi elektronik dengan mengatur CA, yaitu pihak terpercaya yang menerbitkan sertifikat elektronik untuk memverifikasi identitas pengguna dalam transaksi digital, seperti tanda tangan elektronik. Peraturan ini menetapkan dua kategori CA: terakreditasi dan tidak terakreditasi. CA terakreditasi, seperti *Netrust Pte Ltd* dan *Assurity Trusted Solutions Pte Ltd*, secara sukarela memenuhi standar ketat yang ditetapkan oleh *Infocomm Media Development Authority (IMDA)*, termasuk audit berkala, keamanan sistem berbasis *Public Key Infrastructure (PKI)*, dan kepatuhan terhadap pedoman tata kelola. CA tidak terakreditasi tetap wajib mematuhi kewajiban dasar, seperti menjaga keandalan sistem dan kerahasiaan kunci penandatanganan.

Peraturan ini mewajibkan CA untuk melakukan verifikasi identitas sebelum menerbitkan sertifikat elektronik, mengelola proses penerbitan, perpanjangan, penangguhan, dan pencabutan sertifikat dengan prosedur yang jelas, serta menyimpan catatan transaksi secara aman. CA harus menggunakan teknologi yang andal, seperti PKI, untuk memastikan integritas dan autentikasi dokumen elektronik, yang penting untuk mencegah penyalahgunaan teknologi, termasuk ancaman siberterorisme seperti peretasan atau penipuan identitas. *Controller of Certification Authorities* di bawah IMDA bertugas mengawasi kepatuhan CA, melakukan inspeksi, dan menangani pelanggaran, termasuk potensi kejahatan siber.[85]

Dengan demikian, sistem hukum di bidang sertifikasi elektronik antara kedua negara, yakni Indonesia dan Singapura, mencerminkan pendekatan yuridis yang berbeda namun saling melengkapi dalam konteks pengembangan infrastruktur hukum digital. Perbedaan tersebut tampak dalam hal dasar hukum, mekanisme pengakuan tanda tangan elektronik, serta kelembagaan otoritas sertifikasi yang diatur masing-masing negara. Kendati demikian, keduanya memiliki tujuan yang sejalan, yaitu

[85] Stephen Mason, Electronic Signatures in Law, 3rd Edition, Electronic Signatures in Law, 3rd Edition, 2012, doi:10.1017/CBO9780511998058.

untuk menjamin integritas, keaslian, serta keamanan dalam transaksi elektronik lintas sektor, sejalan dengan tuntutan globalisasi dan perkembangan teknologi informasi yang terus mengalami akselerasi. Hal ini menunjukkan bahwa baik Indonesia maupun Singapura berupaya menyesuaikan kerangka hukumnya agar tetap relevan dan adaptif terhadap dinamika digitalisasi yang terjadi secara global.[86]

Kedua peraturan ini merupakan bagian dari upaya Singapura untuk menjadi pusat ekonomi digital global. Regulations 2010 berfokus pada pengaturan CA sebagai tulang punggung keamanan transaksi elektronik, sedangkan Amendment Act 2021 memperluas cakupan ETA untuk mencakup teknologi modern seperti identitas digital dan blockchain. Bersama-sama, keduanya memastikan bahwa transaksi elektronik di Singapura memiliki dasar hukum yang kuat, mendukung inovasi, dan melindungi pengguna. amandemen dilakukan untuk menyesuaikan kerangka hukum dengan perkembangan teknologi, kebutuhan ekonomi digital, dan standar global yang terus berkembang. Regulations 2010 dirancang pada era ketika teknologi seperti tanda tangan elektronik dan sertifikat digital berbasis Public Key Infrastructure (PKI) menjadi standar.

Namun, sejak 2010, teknologi baru seperti blockchain, smart contracts, biometrik, dan identitas digital (contoh: SingPass) telah berkembang pesat. Amandemen 2021 memperbarui ETA agar tetap relevan dengan mengadopsi pendekatan teknologi-netral, sehingga teknologi baru dapat diakui secara hukum tanpa perlu perubahan regulasi berulang. Singapura sedang mengejar visi Smart Nation, yang menekankan digitalisasi di berbagai sektor seperti pemerintahan, keuangan, dan layanan publik. Regulations 2010 tidak secara eksplisit mendukung sistem identitas digital terpusat seperti SingPass atau teknologi terdesentralisasi seperti blockchain. [87]

---

[86] Mohamad Rivaldi Moha and others, 'The Comparative Law Study: E-Commerce Regulation in Indonesia and Singapore', *Jurnal Legalitas*, 16.2 (2023), pp. 248–59, doi:10.33756/jelta.v16i2.20463.

[87] 'Part II ACCREDITATION OF CERTIFICATION AUTHORITIES 3', 2010.

Amandemen 2021 memperkenalkan kerangka hukum untuk identitas digital dan memperkuat pengakuan dokumen elektronik, sehingga mendukung inisiatif digital seperti e-government dan layanan keuangan digital. Amendemen ini memperbarui Electronic Transactions Act untuk mengadopsi UNCITRAL Model Law on Electronic Transferable Records (2017) yang memungkinkan penggunaan dokumen elektronik yang dapat dipindahtangankan (electronic transferable records). Mengatur legalitas dan kesetaraan dokumen elektronik seperti electronic bills of lading (eBLs) dengan dokumen fisik tradisional, yang sangat penting dalam perdagangan internasional dan logistik. Mempercepat proses transaksi dengan mengurangi waktu verifikasi dan risiko pemalsuan melalui teknologi digital seperti tanda tangan digital dan blockchain. Memperluas cakupan hukum elektronik untuk mencakup dokumen yang sebelumnya tidak termasuk, seperti consignment notes dan warehouse receipts.

Melakukan penyesuaian pada ketentuan pengiriman dan penerimaan komunikasi elektronik agar sesuai dengan Konvensi PBB tentang Penggunaan Komunikasi Elektronik dalam Kontrak Internasional (ECC). Pendekatan teknologi-netral yang diadopsi dalam Electronic Transactions (Amendment) Act 2021 di Singapura dirancang untuk memastikan bahwa kerangka hukum tetap relevan dan fleksibel dalam menghadapi kemajuan teknologi yang cepat, seperti blockchain, smart contracts, dan teknologi distributed ledger (DLT). Pendekatan ini menghindari pengikatan regulasi pada teknologi spesifik, seperti Public Key Infrastructure (PKI) yang dominan pada Electronic Transactions (Certification Authority) Regulations 2010, sehingga memungkinkan inovasi teknologi baru diakomodasi tanpa memerlukan revisi hukum yang berulang. Dengan kata lain, regulasi tidak menetapkan teknologi tertentu sebagai syarat untuk pengakuan hukum, melainkan

fokus pada hasil fungsional, yaitu keamanan, keandalan, dan integritas transaksi elektronik.[88]

Misalnya, blockchain dan DLT memungkinkan pencatatan data yang terdesentralisasi dan tahan terhadap manipulasi, yang berbeda dari sistem terpusat seperti yang digunakan oleh Certification Authorities (CA). Smart contracts, yang merupakan program otomatis yang menjalankan perjanjian secara mandiri di blockchain, juga menawarkan cara baru untuk mengotomatisasi transaksi tanpa perantara. Pendekatan teknologi-netral memungkinkan teknologi ini diakui secara hukum selama memenuhi standar tertentu, seperti kemampuan untuk memverifikasi identitas pihak yang terlibat, mencegah perubahan data tanpa izin, dan memastikan bahwa transaksi dapat dilacak serta diaudit.

Untuk dokumen elektronik, amandemen ini memperluas definisi dan pengakuan hukum terhadap dokumen yang dihasilkan oleh teknologi baru, seperti kontrak yang disimpan di blockchain atau catatan transaksi berbasis DLT. Pengakuan ini mensyaratkan bahwa dokumen tersebut memenuhi standar keamanan, seperti memiliki mekanisme otentikasi yang kuat (misalnya, tanda tangan elektronik yang aman) dan keandalan, seperti kemampuan untuk menjaga integritas data selama siklus hidup dokumen. Dengan demikian, amandemen ini memungkinkan Singapura untuk mendukung inovasi seperti platform keuangan terdesentralisasi (DeFi), tokenisasi aset, atau sistem identitas digital berbasis blockchain, sambil tetap memastikan perlindungan hukum dan kepercayaan publik dalam ekosistem digital. Pendekatan ini juga selaras dengan visi Singapura sebagai Smart Nation, yang bertujuan memanfaatkan teknologi mutakhir untuk meningkatkan efisiensi dan daya saing ekonomi digital, sekaligus menjaga keselarasan dengan standar internasional seperti UNCITRAL Model Law on Electronic Commerce untuk mendukung transaksi lintas batas. Mengingat pesatnya perubahan teknologi, IMDA menyadari bahwa kerangka

[88] Vincent Ooi and Vincent Ooi, 'Institutional Knowledge at Singapore Management University Adapting Taxation for the Digital Economy in Singapore Singapore Adapting Taxation for the Digital Economy in Singapore', 2021, pp. 1–10.

legislatif Singapura harus tetap mendukung dan tidak menghambat perkembangan serta adopsi sarana komunikasi dan transaksi elektronik yang praktis dan layak secara komersial seiring ketersediaannya yang semakin luas. Meskipun penting sebagai tolok ukur, norma internasional dan preferensi yurisdiksi lain untuk penggunaan salinan fisik dalam transaksi tertentu, seperti pengalihan properti tidak bergerak, tidak seharusnya, dengan sendirinya, membatasi pendekatan kami untuk mendukung penerapan ETA yang lebih luas. Adalah kepentingan Singapura untuk memastikan bahwa undang-undangnya terus mendukung dan memfasilitasi komunikasi dan transaksi elektronik di masa depan yang semakin terdigitalisasi, bahkan jika itu berarti melangkah lebih maju dari norma dan praktik internasional.

Oleh karena itu, IMDA berpendapat bahwa, secara umum, ketentuan kesetaraan fungsional dalam ETA harus, pada prinsipnya, berlaku untuk dokumen dan transaksi yang sebelumnya dikecualikan, kecuali terdapat pertimbangan kepentingan publik yang lebih utama. Jika terdapat kekhawatiran tentang konsekuensi dari perubahan tersebut, berbagai langkah mitigasi dan perlindungan dapat diterapkan untuk mengatasi kekhawatiran tersebut. Untuk informasi lebih lengkap IMDA adalah singkatan dari Infocomm Media Development Authority, sebuah badan pemerintah di Singapura yang bertanggung jawab atas pengembangan dan regulasi sektor teknologi informasi, komunikasi, dan media. IMDA dibentuk pada tahun 2016 melalui penggabungan dua badan sebelumnya, yaitu Infocomm Development Authority (IDA) dan Media Development Authority (MDA). Tujuan utama IMDA adalah mendorong transformasi digital, mendukung visi Smart Nation Singapura, dan memastikan ekosistem digital yang aman, inovatif, dan kompetitif.

Hubungan IMDA (Infocomm Media Development Authority) dengan pendekatan teknologi-netral yang diadopsi dalam Electronic Transactions (Amendment) Act 2021 di Singapura sangat erat, karena IMDA adalah badan pemerintah yang bertanggung jawab merancang, mengawasi, dan menerapkan regulasi terkait teknologi informasi dan komunikasi, termasuk kerangka hukum untuk transaksi elektronik. Berikut penjelasan rinci tentang hubungan tersebut:

IMDA memiliki mandat untuk mendorong transformasi digital dan mendukung visi Smart Nation Singapura, yang bertujuan menjadikan Singapura sebagai pusat teknologi dan ekonomi digital global. Salah satu cara IMDA mencapai tujuan ini adalah dengan memastikan bahwa regulasi, seperti Electronic Transactions Act (ETA), tetap relevan di tengah perkembangan teknologi yang pesat, seperti blockchain, smart contracts, dan teknologi distributed ledger (DLT). Pendekatan teknologi-netral yang diadopsi dalam amandemen 2021 mencerminkan strategi IMDA untuk menciptakan kerangka hukum yang fleksibel dan tidak membatasi inovasi. IMDA menyadari bahwa teknologi seperti blockchain dan smart contracts memiliki potensi besar untuk mengubah cara transaksi elektronik dilakukan, misalnya melalui otomatisasi kontrak atau penyimpanan data yang terdesentralisasi. [89]

Dengan mengadopsi pendekatan teknologi-netral, IMDA memastikan bahwa ETA tidak terpaku pada teknologi spesifik seperti Public Key Infrastructure (PKI) yang digunakan dalam Electronic Transactions (Certification Authority) Regulations 2010. Sebaliknya, regulasi berfokus pada standar fungsional seperti keamanan, keandalan, dan otentikasi, sehingga teknologi baru dapat diakui secara hukum tanpa memerlukan revisi undang-undang setiap kali muncul inovasi, IMDA berperan dalam memperbarui ETA untuk memungkinkan pengakuan hukum terhadap dokumen elektronik yang dihasilkan oleh teknologi baru, selama memenuhi standar keamanan dan keandalan. Misalnya, dokumen atau kontrak yang disimpan di blockchain dapat dianggap sah secara hukum jika memenuhi persyaratan seperti integritas data dan otentikasi pihak.

Pendekatan teknologi-netral ini keuangan memungkinkan IMDA untuk mendukung berbagai aplikasi digital, seperti platform terdesentralisasi (DeFi) atau sistem identitas digital, tanpa membatasi jenis teknologi yang digunakan. , IMDA bertugas memastikan bahwa Singapura tetap kompetitif sebagai pusat e-commerce

[89] Infocomm, 'Consultation Paper Issued by the Infocomm Media Development Authority on Embedded SIM Technology', *Consultation Paper*, no. June (2018), p. 19 <https://www.imda.gov.sg/-/media/imda/files/inner/pcdg/consultations/consultation-paper/public-consultation-on-embedded-sim-technology/consultation-document-for-esim.pdf?la=en>.

dan teknologi global. Pendekatan teknologi-netral memungkinkan pelaku industri, mulai dari startup hingga perusahaan besar, untuk mengembangkan solusi inovatif tanpa terkendala oleh regulasi yang kaku. Misalnya, IMDA mendukung pengembangan SingPass sebagai identitas digital yang dapat digunakan lintas platform, dan pendekatan teknologi-netral memastikan bahwa sistem ini dapat diintegrasikan dengan teknologi baru seperti biometrik atau blockchain. IMDA memainkan peran sentral dalam inisiatif Smart Nation, yang mencakup digitalisasi layanan pemerintah, keuangan, dan sektor swasta. Pendekatan teknologi-netral mendukung visi ini dengan memberikan ruang bagi inovasi seperti smart contracts untuk otomatisasi layanan atau DLT untuk manajemen data yang aman.

IMDA memastikan bahwa regulasi seperti ETA 2021 tidak hanya mendukung teknologi saat ini, tetapi juga siap untuk teknologi masa depan yang belum dikembangkan. egulasi Singapura dengan standar internasional, seperti UNCITRAL Model Law on Electronic Commerce, untuk memfasilitasi transaksi lintas batas. Pendekatan teknologi-netral memungkinkan IMDA untuk mengakui berbagai teknologi yang digunakan di yurisdiksi lain, selama memenuhi standar keamanan, sehingga memperkuat posisi Singapura sebagai pusat perdagangan elektronik global. IMDA tidak hanya merancang regulasi, tetapi juga mengawasi implementasinya, termasuk akreditasi Certification Authorities (CA) dan pengembangan pedoman untuk keamanan transaksi elektronik.

Dengan pendekatan teknologi-netral, IMDA dapat memperluas pengawasan ke teknologi baru tanpa memerlukan perubahan besar pada struktur regulasi yang ada, seperti yang terlihat pada peran CA dalam Regulations 2010. IMDA mengadopsi pendekatan teknologi-netral dalam Electronic Transactions Amendment Act 2021 untuk memastikan bahwa regulasi tetap relevan, mendukung inovasi, dan memperkuat posisi Singapura sebagai pusat ekonomi digital. Pendekatan ini memungkinkan IMDA untuk mengakomodasi teknologi baru seperti blockchain dan smart contracts tanpa membatasi perkembangan di masa depan, sekaligus menjaga keamanan, keandalan, dan kepercayaan dalam transaksi elektronik. Ini mencerminkan

peran strategis IMDA dalam mendorong transformasi digital yang selaras dengan visi Smart Nation dan standar global. Menghapus daftar pengecualian dalam Lampiran Pertama ETA juga dapat mengatasi kesalahpahaman yang ada dan potensial mengenai validitas hukum versi elektronik dari dokumen yang dikecualikan dari penerapan ETA.

Dari diskusi dengan pemangku kepentingan, IMDA menerima masukan bahwa versi elektronik dari dokumen yang dikecualikan dari penerapan ETA umumnya dianggap tidak sah secara hukum. Hal ini terjadi meskipun hukum umum telah mengakui bahwa catatan dan tanda tangan elektronik dapat memenuhi persyaratan formalitas “tertulis” dan “ditandatangani”, bahkan ketika versi elektronik dari dokumen tersebut dikecualikan dari penerapan ETA.

BAB III

Fakor-Faktor Yang Mempengaruhi Adanya Perbandingan Sistem Hukum Di Bidang Sertifikasi Elektronik Antara Indonesia dan Singapura

A. Faktor Internasional atau Global Standards

Faktor awal sertifikasi elektronik antara Indonesia dan Singapura dibandingkan dalam konteks standar global relevan karena kedua negara memiliki pendekatan berbeda dalam mengatur transaksi elektronik, tetapi sama-sama bertujuan untuk memenuhi standar internasional guna mendukung transformasi digital yang aman dan andal. Indonesia dan Singapura, sebagai negara di kawasan ASEAN, memiliki peran penting dalam ekonomi digital Asia Tenggara, dengan pertumbuhan pengguna internet yang pesat dan tantangan keamanan siber yang serupa, seperti siberterorisme. Standar global, seperti *UNCITRAL Model Law on Electronic Commerce 1996* menjadi acuan untuk memastikan interoperabilitas, keamanan, dan kepercayaan dalam transaksi elektronik lintas negara. Membandingkan kedua negara membantu memahami sejauh mana regulasi mereka selaras dengan standar ini, yang krusial untuk perdagangan digital internasional dan kolaborasi regional.

Faktor global standar dan internasional dalam konteks perbandingan bidang hukum sertifikasi elektronik merujuk pada elemen-elemen utama yang menjadi acuan bersama di tingkat global untuk memastikan sistem sertifikasi elektronik, seperti tanda tangan elektronik dan infrastruktur kunci publik (PKI), dapat diakui, interoperable, dan memenuhi kebutuhan hukum serta teknis lintas negara. Faktor-faktor ini mencakup kerangka hukum, standar teknis, dan praktik operasional yang diadopsi secara luas oleh komunitas internasional untuk menjamin keamanan, keabsahan, dan kepercayaan dalam transaksi digital.

Faktor global standar dan internasional berfokus pada harmonisasi aturan dan teknologi agar sertifikasi elektronik memiliki legitimasi yang seragam di berbagai

yurisdiksi. Pertama, dari sisi hukum, banyak negara, termasuk Indonesia dan Singapura, mengacu pada model hukum internasional seperti UNCITRAL Model Law on Electronic Signatures (2001) yang dikeluarkan oleh Perserikatan Bangsa-Bangsa. Model ini memberikan panduan agar tanda tangan elektronik memiliki kekuatan hukum setara dengan tanda tangan tulis, selama memenuhi syarat seperti identifikasi yang jelas dan integritas data. Kerangka ini memungkinkan negara-negara untuk menyusun undang-undang nasional yang kompatibel dengan standar global, sehingga transaksi elektronik lintas batas diakui secara hukum. Sttandar teknis internasional memainkan peran penting. Organisasi seperti International Organization for Standardization (ISO) dan International Electrotechnical Commission (IEC) menetapkan standar seperti ISO/IEC 27001 untuk sistem manajemen keamanan informasi dan ISO/IEC 24760 untuk manajemen identitas. Standar ini memastikan bahwa teknologi yang digunakan dalam sertifikasi elektronik, seperti enkripsi dan otentikasi, memenuhi persyaratan keamanan dan interoperabilitas global. Selain itu, protokol seperti X.509 untuk sertifikat digital menjadi acuan universal agar sertifikat yang diterbitkan oleh otoritas sertifikasi (Certificate Authority/CA) di satu negara dapat dipercaya di negara lain.

Terkait standar ISO, sertifikasi merupakan jaminan dari badan sertifikasi bahwa suatu layanan, produk, atau sistem telah memenuhi ketentuan standar yang ditetapkan. Meskipun ISO mengembangkan standar, badan sertifikasi pihak ketiga bertugas memverifikasi kesesuaian dengan standar tersebut. Menurut ISO, istilah "sertifikasi ISO" tidak tepat digunakan untuk menyatakan bahwa produk atau sistem telah disertifikasi sesuai standar ISO. Sebagai gantinya, ISO menganjurkan penggunaan identifikasi lengkap dari standar yang dimaksud, misalnya, "bersertifikasi ISO 9001:2015" daripada hanya "bersertifikasi ISO". Penyebutan ini mencakup nama dan versi standar, dalam hal ini ISO 9001 versi 2015. Walaupun ISO tidak melakukan sertifikasi, Komite Penilaian Kesesuaian ISO berperan dalam mengembangkan standar terkait proses sertifikasi.

Oleh karena itu di negara Indonesia, adanya BSN (Badan Standardisasi Nasional) menjadi wakil resmi dari organisasi ISO. BSN bertugas untuk merumuskan dan memerankan standar ISO di Indonesia, misalnya ISO 9001 (manajemen mutu), ISO 14001 (lingkungan) dll. Indonesia juga ikut berpartisipasi dalam penyusunan standar ISO global melalui komite teknis dan forum Internasional. Indonesia telah menjadi anggota sejak tahun 1955, diwakili oleh Yayasan Dana Normalisasi Indonesia (YDNI) , dan pada tahun 1997 pemerintah Indonesia mendirikan BSN. Dengan demikian, Indonesia sejak terlibat sejak era Presiden Soekarno Hatta dan terus memperkuat peran pada era Presiden Soeharto.

Beberapa pertanyaan yang dibahas pada penelitian ini yaitu adanya nomor pada ISO. Contohnya seperti ISO 9001 (Standar sistem manajemen mutu), nomor dibelakang ISO berfungsi guna kode identifikasi unik dari standar tertentuyang diterbitkan, nomor tersebut merupakan kode khusus buat jenis standarnya, karena tiap nomor merujuk ke spesifikasi teknis tertentu.

Faktor global juga mencakup praktik operasional, seperti akreditasi CA dan mekanisme audit. Organisasi seperti European Telecommunications Standards Institute (ETSI) dengan standar EN 319 401 mengatur persyaratan untuk penyedia layanan kepercayaan (trust service providers). Di tingkat global, ada upaya untuk menciptakan kerangka kepercayaan bersama (trust framework) yang memungkinkan sertifikat elektronik diakui lintas negara melalui perjanjian bilateral atau multilateral, seperti yang diterapkan dalam eIDAS Regulation di Uni Eropa, yang menjadi referensi bagi banyak negara.

Dalam konteks Indonesia dan Singapura, faktor-faktor ini memengaruhi bagaimana kedua negara mengatur sertifikasi elektronik. Indonesia menggunakan regulasi seperti UU ITE untuk menyelaraskan hukumnya dengan UNCITRAL, sementara Singapura melalui Electronic Transactions Act menyesuaikan dengan standar serupa, namun dengan penekanan lebih kuat pada interoperabilitas global karena posisinya sebagai pusat keuangan internasional. Keduanya juga mengadopsi standar teknis seperti ISO/IEC untuk memastikan keamanan sistem, tetapi Singapura

cenderung lebih maju dalam implementasi teknologi dan kerja sama internasional, misalnya dengan negara-negara ASEAN atau mitra dagang global.

Secara keseluruhan, faktor global standar dan internasional ini mencakup keselarasan hukum, teknologi, dan operasional untuk memastikan sertifikasi elektronik dapat dipercaya, aman, dan berfungsi secara efektif dalam ekosistem digital global, sembari menghormati kebutuhan spesifik masing-masing negara.

Singapura, melalui *Electronic Transactions Act (ETA) 2021* dan *Electronic Transactions (Certification Authority) Regulations 2010*, mengadopsi pendekatan fleksibel dengan akreditasi sukarela untuk Penyelenggara Sertifikasi Elektronik (CA) dan menyelaraskan regulasinya, memungkinkan pengakuan sertifikat elektronik asing. Hal ini mendukung posisi Singapura sebagai pusat teknologi global. Sebaliknya, Indonesia, dengan Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik , PP Nomor 71 Tahun 2019, dan Permenkominfo Nomor 11 Tahun 2022, mewajibkan pendaftaran Penyelenggara Sertifikasi Elektronik (PSrE) dan lebih fokus pada keamanan domestik, meskipun masih berupaya menyesuaikan dengan standar global. Perbandingan ini mengungkapkan kekuatan dan kelemahan masing-masing sistem: Singapura lebih maju dalam interoperabilitas internasional, sementara Indonesia menghadapi tantangan seperti koordinasi antarinstansi dan adaptasi teknologi cepat.[90] Standar global menuntut keamanan tinggi, seperti penggunaan *Public Key Infrastructure (PKI*), perlindungan data, dan autentikasi yang andal, yang penting untuk mencegah siberterorisme dan kejahatan siber lainnya. Dengan membandingkan kedua negara, Indonesia dapat belajar dari fleksibilitas dan harmonisasi internasional Singapura, sementara Singapura dapat mempertimbangkan pendekatan Indonesia dalam pengawasan ketat untuk sektor strategis.

[90] Suhairi, Juli Syahputri, and Fahmi Rizky, 'Strategi & Standarisasi Dalam Pemasaran Global', *Jurnal Masharif Al-Syariah: Jurnal Ekonomi Dan Perbankan Syariah*, 8.1 (2023), pp. 369–77 <http://journal.um-surabaya.ac.id/index.php/Mas/index>.

Perbandingan ini juga membantu mengidentifikasi peluang kolaborasi ASEAN dalam membangun ekosistem digital yang terintegrasi, seperti pengakuan timbal balik sertifikat elektronik, yang mendukung perdagangan dan keamanan regional. Standardisasi merupakan suatu proses yang bersifat dinamis dan terus mengalami evolusi di berbagai belahan dunia. Perkembangannya mencakup perluasan ruang lingkup, penyesuaian prosedur perumusan, hingga aspek implementasinya. Beragam jenis standar yang disusun, disahkan, dan diberlakukan oleh lembaga nasional, regional, internasional, maupun asosiasi tertentu, memiliki peran penting dalam membentuk budaya berbasis konsensus yang bersifat universal.

Tujuan utama dari standardisasi ini adalah untuk menjadi sarana komunikasi yang efektif antar masyarakat, memperkuat saling pengertian, meningkatkan kualitas hidup, serta mendukung kelancaran aktivitas perdagangan.[91]

Singapura memiliki pendekatan yang lebih liberal dengan akreditasi sukarela, memungkinkan fleksibilitas bagi CA, tetapi tetap menjaga keamanan tinggi melalui standar seperti Public Key Infrastructure (PKI) dan audit berkala. Indonesia, sebaliknya, menerapkan pendekatan yang lebih ketat dengan pendaftaran wajib, mencerminkan fokus pada kontrol domestik, tetapi berpotensi membatasi inovasi karena proses birokrasi. Dalam konteks standar global, Singapura lebih selaras dengan eIDAS melalui pengakuan sertifikat asing dan interoperabilitas, sementara Indonesia masih dalam tahap menyesuaikan regulasi untuk mencapai tingkat harmonisasi yang sama.

Standar global netral dan berlaku untuk semua negara merujuk pada kerangka aturan, pedoman, atau spesifikasi teknis yang dikembangkan oleh organisasi internasional untuk diterapkan secara universal di berbagai negara tanpa memihak pada kepentingan nasional tertentu. Standar ini dirancang untuk memastikan konsistensi, interoperabilitas, keamanan, dan kepercayaan dalam berbagai bidang,

[91] Suardi Suardi, Fakhruddin Azmi, and Nurika Khalila Daulay, 'Perkembangan International Standard of Organization', Jurnal Ilmiah Universitas Batanghari Jambi, 23.3 (2023), p. 2625, doi:10.33087/jiubj.v23i3.3411.

termasuk sertifikasi elektronik, sehingga memungkinkan kerja sama lintas batas yang efektif. Misalnya, dalam konteks sertifikasi elektronik, standar seperti yang dikembangkan oleh International Organization for Standardization (ISO), seperti ISO/IEC 27001 untuk manajemen keamanan informasi atau ISO/IEC 24760 untuk identitas digital, menjadi acuan global yang netral karena tidak terikat pada hukum atau budaya suatu negara tertentu, melainkan berfokus pada prinsip teknis dan operasional yang dapat diterima secara luas. Selain itu, model hukum seperti UNCITRAL Model Law on Electronic Signatures juga menawarkan kerangka netral yang memungkinkan negara-negara mengadopsi aturan seragam untuk keabsahan tanda tangan elektronik, memastikan transaksi digital diakui secara global. Standar ini bersifat netral karena dibuat melalui konsensus internasional, melibatkan berbagai pemangku kepentingan dari banyak negara, dan berlaku untuk semua negara yang mengadopsinya, dengan fleksibilitas untuk disesuaikan dengan kebutuhan lokal tanpa mengubah esensi standar. Indonesia harus menggunakan standar global karena standar tersebut sangat penting untuk meningkatkan daya saing produk dan layanan Indonesia di pasar global. Dengan memenuhi standar internasional, produk Indonesia tidak hanya memenuhi kualitas, keamanan, dan mutu yang diakui secara global, tetapi juga memudahkan akses produk ke pasar internasional yang semakin kompetitif.

Apalagi, pada tingkat ekonomi, Masalah global standar dalam konteks ekonomi merujuk pada tantangan yang muncul ketika standar internasional, seperti yang dikembangkan oleh organisasi seperti ISO, WTO, atau UNCITRAL, diterapkan secara universal untuk memfasilitasi perdagangan, investasi, dan kerja sama ekonomi lintas negara, namun menghadapi kendala akibat perbedaan sistem ekonomi, tingkat pembangunan, dan kepentingan nasional. Standar global, yang dirancang untuk netral dan berlaku di semua negara, bertujuan menciptakan harmonisasi dalam praktik bisnis, teknologi, dan regulasi, seperti standar keamanan informasi (ISO/IEC 27001) atau aturan perdagangan WTO, untuk memastikan efisiensi, transparansi, dan kepercayaan dalam ekonomi global. Namun, implementasinya sering kali memunculkan sejumlah masalah.

Salah satu masalah utama adalah kesenjangan kapasitas ekonomi antarnegara. Negara maju, dengan infrastruktur teknologi dan sumber daya yang kuat, lebih mudah mengadopsi dan mematuhi standar global, seperti sertifikasi elektronik atau standar kualitas produk, dibandingkan negara berkembang. Negara berkembang, termasuk Indonesia, sering kali menghadapi keterbatasan dalam hal biaya, keahlian teknis, dan infrastruktur untuk memenuhi standar tersebut, yang dapat meningkatkan biaya produksi dan melemahkan daya saing di pasar global. Misalnya, penerapan standar ISO untuk sertifikasi elektronik memerlukan investasi dalam sistem keamanan siber dan otoritas sertifikasi, yang mungkin menjadi beban bagi pelaku usaha kecil di negara berkembang.

Selain itu, standar global yang netral kadang-kadang dianggap tidak cukup fleksibel untuk mengakomodasi kebutuhan lokal. Negara-negara dengan sistem ekonomi yang berbeda, seperti ekonomi berbasis pasar bebas di Singapura versus ekonomi campuran di Indonesia, mungkin memiliki prioritas yang berbeda dalam menerapkan standar. Sebagai contoh, standar perdagangan internasional yang menekankan liberalisasi pasar dapat menguntungkan negara dengan ekonomi terbuka, tetapi menimbulkan tantangan bagi negara yang melindungi industri lokalnya. Hal ini menciptakan ketegangan antara kepatuhan terhadap standar global dan perlindungan kepentingan ekonomi nasional. Masalah lain adalah dominasi negara-negara besar dalam pengembangan standar global. Meskipun standar dirancang untuk netral, proses penyusunannya sering dipengaruhi oleh negara-negara maju yang memiliki sumber daya untuk berkontribusi dalam organisasi seperti ISO atau WTO. Akibatnya, standar tersebut mungkin lebih mencerminkan kebutuhan ekonomi negara maju, seperti teknologi canggih atau regulasi ketat, yang kurang relevan atau sulit diterapkan di negara berkembang. Hal ini dapat memperlebar ketimpangan ekonomi global.

Dalam era globalisasi saat ini, keterlibatan pihak asing menjadi kebutuhan, terutama di tengah kondisi ekonomi seperti sekarang. Untuk memulihkan

perekonomian agar berjalan stabil, normal, dan terus meningkat, membuka peluang seluas-luasnya bagi pihak asing untuk beroperasi di sektor perbankan menjadi langkah yang tidak terhindarkan. Namun, pengaturan yang bijaksana oleh Pemerintah terkait kepemilikan saham oleh pihak asing perlu dikaji secara mendalam dan hati-hati.[92]

Dalam konteks sertifikasi elektronik, misalnya, standar global seperti X.509 untuk sertifikat digital memungkinkan interoperabilitas transaksi elektronik lintas negara, yang mendukung perdagangan digital. Namun, negara dengan ekonomi digital yang kurang berkembang mungkin kesulitan membangun infrastruktur kunci publik (PKI) yang sesuai standar, sehingga menghambat partisipasi mereka dalam ekonomi digital global. Di sisi lain, negara seperti Singapura, dengan ekonomi yang sangat terdigitalisasi, dapat memanfaatkan standar ini untuk memperkuat posisinya sebagai pusat keuangan global.

Secara keseluruhan, masalah global standar dalam ekonomi berkisar pada kesenjangan kapasitas, fleksibilitas yang terbatas, dan potensi bias dalam penyusunan standar. Meskipun standar global bertujuan mempromosikan efisiensi dan keadilan dalam ekonomi dunia, tantangan ini menuntut pendekatan yang lebih inklusif, seperti bantuan teknis dan finansial bagi negara berkembang, agar manfaat standar dapat dirasakan secara merata tanpa memperburuk ketimpangan ekonomi.

Tantangan utama adalah ketidakmerataan penerapan SNI di berbagai sektor, termasuk perbankan, serta kesenjangan infrastruktur dan akses informasi antar wilayah, terutama di daerah terpencil. Misalnya, SNI Corner yang didirikan untuk menyebarkan informasi standardisasi sering kali menghadapi kendala seperti kemutakhiran konten, kelengkapan dokumen, kecepatan aplikasi, dan kompetensi pengelola. Dalam era globalisasi, adopsi standar internasional seperti ISO 31000 untuk manajemen risiko menjadi penting, terutama untuk mendukung operasional pihak asing di sektor perbankan. Namun, pemahaman mendalam terhadap standar

[92] Zainal Said, *Politik Hukum Perbankan Nasional*, 2019.

induk seperti SNI ISO 31000:2018 masih terbatas di kalangan organisasi di Indonesia, yang dapat menghambat efektivitas penerapan standar baru, meskipun membuka peluang bagi pihak asing di sektor perbankan dianggap penting untuk stabilitas ekonomi, pengaturan kepemilikan saham asing harus dilakukan dengan bijaksana. Tantangan utama adalah merumuskan regulasi yang seimbang antara menarik investasi asing dan melindungi kepentingan nasional, penerapan SNI di sektor perbankan dan industri lainnya membutuhkan dukungan teknologi, seperti platform daring untuk perdagangan produk berstandar SNI. Namun, literasi digital yang rendah dan akses teknologi yang terbatas di beberapa daerah menjadi hambatan. Undang-Undang Nomor 20 Tahun 2014 tentang Perindustrian memberikan wewenang pada setiap instansi untuk membuat peraturan terkait barang yang wajib di standardisasi.

Dalam Undang-Undang Nomor 20 Tahun 2014 pada Pasal 24 ayat (2) dikatakan bahwa pemberlakuan Standar Nasional Indonesia adalah keputusan pimpinan instansi teknis yang berwenang untuk memberlakukan Standar Nasional Indonesia secara wajib terhadap barang dan atau jasa. Pemberlakuan SNI secara wajib adalah regulasi teknis atas barang dan atau jasa yang ditetapkan oleh Menteri dan diberlakukan secara wajib di seluruh wilayah Negara Kesatuan Republik Indonesia. Namun, sebagian SNI dapat diwajibkan penerapannya apabila ia berhubungan erat dengan keamanan, keselamatan kerja dan kelestarian lingkungan hidup (disebut dengan SNI wajib). Tingkat daya saing yang masih rendah di Indonesia, kurangnya kepatuhan pelaku usaha terhadap penerapan Standar Nasional Indonesia (SNI), serta dinamika perdagangan bebas menjadi dasar sosiologis perlunya regulasi daerah tentang standar dan penilaian kesesuaian.

Peraturan daerah merupakan perwujudan konkret dari hukum yang harus selaras dengan realitas, fenomena, perkembangan, kesadaran, serta kebutuhan hukum masyarakat. Saat ini, masyarakat membutuhkan regulasi daerah sebagai acuan utama dan panduan penerapan SNI, karena pembangunan industri oleh pemerintah daerah masih bersifat parsial dan belum terintegrasi. Belum adanya acuan, model, atau

bentuk penerapan standar dan penilaian kesesuaian dalam program kebijakan peningkatan daya saing produk unggulan daerah menyebabkan penyelenggaraan oleh berbagai komponen, seperti pemerintah daerah, Badan Standardisasi Nasional (BSN), lembaga sertifikasi, swasta, BUMN, dan koperasi, belum optimal. Regulasi daerah tentang standar dan penilaian kesesuaian diharapkan dapat membuat pengelolaan bidang perindustrian di daerah lebih terarah, sistematis, dan menyeluruh.[93]

Dengan demikian, standar global ini memfasilitasi harmonisasi teknologi dan hukum, mendukung perdagangan, komunikasi, dan kepercayaan digital di seluruh dunia.

B. Faktor Kelembagaan

Faktor kelembagaan memainkan peran krusial dalam efektivitas sistem hukum sertifikasi elektronik di Indonesia dan Singapura, terutama dalam memenuhi standar global seperti *UNCITRAL Model Law on Electronic Commerce 1996*. Faktor ini mencakup struktur organisasi, koordinasi antarinstansi, kapasitas sumber daya manusia, dan pengawasan kelembagaan yang mendukung keamanan transaksi elektronik dan pencegahan ancaman seperti siberterorisme. Kelembagaan kedua negara secara ringkas dan jelas. Penyelenggara Sertifikat Elektronik (PSrE) berperan sebagai pelopor tingkat nasional dalam penyelenggaraan sertifikasi elektronik, yang operasionalnya berada di bawah pengelolaan Direktorat Keamanan Informasi pada Kementerian Komunikasi dan Informatika Republik Indonesia.[94]

Peran Penyelenggara Sertifikasi Elektronik (PSrE) di Indonesia memiliki signifikansi besar dalam konteks kebebasan berpendapat, terutama di ranah digital, karena PSrE menjadi bagian integral dari infrastruktur keamanan siber yang memengaruhi cara komunikasi online diatur. Berbeda dengan Singapura, di mana

[93] Sari Tri Suprapto and Dona Budi Kharisma, 'Problematika Implementasi Standar Nasional Indonesia (Sni) Wajib Pada Mainan Anak Di Kota Jakarta Timur', *Jurnal Privat Law*, 8.2 (2020), p. 222, doi:10.20961/privat.v8i2.48413.

[94] Gladhi Guarddin and Jundi Ahmad Alwan, 'Implementasi Sistem Registration Authority Dan Personal Security Environment Menggunakan Smart Card', Techno.Com, 20.4 (2021), pp. 623–35, doi:10.33633/tc.v20i4.5284.

sistem seperti SingPass mendukung pengawasan ketat terhadap ujaran digital, Indonesia masih dalam tahap pengembangan ekosistem sertifikasi elektronik, sehingga dampaknya terhadap kebebasan berpendapat belum sekuat, namun tetap penting untuk dibahas. PSrE, sebagaimana diatur dalam UU No. 11/2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dan Peraturan Pemerintah No. 71/2019, bertugas menyediakan layanan sertifikasi elektronik, seperti tanda tangan digital dan autentikasi identitas, yang digunakan untuk memastikan keamanan dan keabsahan transaksi atau komunikasi digital.

Dalam konteks kebebasan berpendapat, PSrE berperan dalam menciptakan lingkungan digital yang lebih terverifikasi. Misalnya, tanda tangan digital atau sertifikat elektronik dapat digunakan untuk mengidentifikasi pelaku komunikasi online, termasuk dalam platform media sosial atau situs web. Di Indonesia, di mana kebebasan berpendapat dijamin oleh UUD 1945, tetapi dibatasi oleh pasal-pasal UU ITE seperti pencemaran nama baik atau ujaran kebencian, PSrE dapat membantu aparat penegak hukum melacak identitas pengguna yang dianggap melanggar aturan. Namun, karena infrastruktur PSrE di Indonesia, seperti yang dikelola oleh *Badan Siber dan Sandi Negara (BSSN) atau penyedia swasta, belum sepenuhnya terintegrasi seperti di Singapura, penggunaannya dalam pengawasan ujaran masih bersifat reaktif, bukan proaktif. Artinya, pelacakan biasanya terjadi setelah ada laporan, seperti kasus penghinaan di media sosial, bukan melalui pemantauan sistematis.

Signifikansi PSrE juga terlihat dari potensinya untuk meningkatkan kepercayaan dalam komunikasi digital, yang secara tidak langsung memengaruhi kebebasan berpendapat. Dengan adanya sertifikasi elektronik, individu atau organisasi dapat memastikan bahwa komunikasi mereka sah dan terlindungi dari manipulasi, seperti penyadapan atau pemalsuan identitas. Namun, ini juga berarti pemerintah memiliki alat untuk memverifikasi sumber ujaran, yang dapat digunakan untuk menegakkan regulasi seperti UU ITE. Berbeda dengan Singapura, di mana sistem digital terpusat memungkinkan kontrol ketat terhadap ujaran yang dianggap mengganggu stabilitas, pendekatan Indonesia lebih longgar, tetapi tetap menimbulkan

kekhawatiran akan potensi penyalahgunaan, misalnya dalam kasus kriminalisasi aktivis atau jurnalis.

Selain itu, PSrE memiliki peran strategis dalam mendukung ekosistem digital yang lebih luas, seperti e-government dan e-commerce, yang secara tidak langsung memengaruhi ruang kebebasan berpendapat. Dengan sistem identitas digital yang lebih kuat, pemerintah dapat mendorong transparansi dalam layanan publik, tetapi juga meningkatkan kemampuan untuk mengawasi aktivitas warga, termasuk dalam menyuarakan pendapat. Meski demikian, tantangan di Indonesia, seperti rendahnya literasi digital dan akses teknologi yang tidak merata, membuat dampak PSrE terhadap kebebasan berpendapat belum sebesar di negara seperti Singapura, di mana teknologi digital sudah sangat maju dan terintegrasi. Penyelenggara Sertifikasi Elektronik (PSrE), yang berperan sebagai *Trusted Third Party* (TTP), merujuk pada entitas yang ditetapkan sebagai PSrE berdasarkan Peraturan Pemerintah No. 82 Tahun 2012 [4]. PSrE tergolong sebagai penyelenggara sistem elektronik yang masuk dalam kategori strategis dan kritikal, sehingga diwajibkan untuk menerapkan sistem manajemen keamanan informasi.[95]

Dibandingkan dengan Singapura, di mana sertifikasi elektronik mendukung pengawasan yang ketat dan efisien untuk menjaga ketertiban, Indonesia masih menghadapi kendala dalam implementasi PSrE, seperti koordinasi antarlembaga dan infrastruktur yang belum matang. Hal ini membuat kebebasan berpendapat di Indonesia lebih terbuka, tetapi juga rentan terhadap penegakan hukum yang tidak konsisten, seperti penggunaan UU ITE secara selektif. Ke depan, seiring pengembangan PSrE, Indonesia perlu menyeimbangkan antara keamanan digital dan perlindungan kebebasan berpendapat agar tidak meniru model pengawasan ketat seperti Singapura, yang mengorbankan kebebasan demi stabilitas.

[95] Edmon Makarim, 'Kajian Hukum Terhadap Kemungkinan Cybernotarydi Indonesia'.

Kurangnya sinergi dapat menyebabkan interpretasi regulasi yang bervariasi, terutama terkait UU ITE 2024 dan PP Nomor 71 Tahun 2019. Misalnya, pengawasan PSrE oleh Kemenkominfo dan audit keandalan oleh BSSN kadang-kadang tidak selaras, menghambat implementasi yang konsisten. Kapasitas sumber daya manusia (SDM) dalam pengelolaan sertifikasi elektronik di Indonesia masih terbatas. Meskipun BSSN dan PSrE swasta memiliki tenaga teknis, kurangnya pelatihan dan kesadaran publik tentang sertifikasi elektronik menghambat adopsi. Misalnya, banyak pengguna sistem elektronik, terutama di sektor swasta, belum memahami pentingnya tanda tangan elektronik tersertifikasi. Selain itu, SDM di PSrE swasta sering kali lebih terlatih, negara Singapura memenuhi standar ini dengan struktur kelembagaan yang ramping, koordinasi yang karena Singapura adalah negara dengan populasi sekitar 5,7 juta jiwa dan wilayah yang kecil, memungkinkan pengelolaan kelembagaan yang terpusat dan terkoordinasi. *Infocomm Media Development Authority* (IMDA) bertindak sebagai regulator utama yang mengawasi Penyelenggara Sertifikasi Elektronik (Certification Authorities/CA) berdasarkan Electronic Transactions Act (ETA) 2021 dan Electronic Transactions (Certification Authority) Regulations 2010. [96]

Pasal 28 dalam Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 mengenai Perlindungan Data Pribadi dalam Sistem Elektronik menetapkan sejumlah kewajiban bagi penyelenggara sistem elektronik. Kewajiban tersebut meliputi kewajiban untuk mendaftarkan dan melakukan sertifikasi sistem elektronik, menjaga keamanan serta kerahasiaan data pribadi pengguna, memberi pemberitahuan kepada pemilik data apabila terjadi pelanggaran atau kegagalan dalam perlindungan data, memiliki kebijakan internal terkait perlindungan data, menyediakan catatan audit, memberikan pilihan kepada pemilik data atas penggunaan

[96] Rista Maharani and Andria Luhur Prakoso, 'Perlindungan Data Pribadi Konsumen Oleh Penyelenggara Sistem Elektronik Dalam Transaksi Digital', *Jurnal Usm Law Review*, 7.1 (2024), p. 333, doi:10.26623/julr.v7i1.8705.

datanya, memungkinkan pemutakhiran data pribadi, serta melakukan pemusnahan data sesuai dengan ketentuan yang berlaku.

Government Technology Agency (GovTech) mendukung implementasi teknologi, seperti SingPass, dalam satu ekosistem terintegrasi. Dengan sedikitnya lembaga yang terlibat, koordinasi menjadi lebih cepat dan minim birokrasi. Faktor kelembagaan memainkan peran penting dalam menentukan kualitas tata kelola, efisiensi pemerintahan, dan perkembangan ekonomi suatu negara, di Indonesia, negara yang merupakan demokrasi terbesar ketiga di dunia dengan sistem pemerintahan presidensial. Namun, tata kelola pemerintahan sering kali dihambat oleh kompleksitas birokrasi, desentralisasi yang belum sepenuhnya efektif, dan koordinasi antarlembaga yang lemah. Menurut *Worldwide Governance Indicators* (WGI) 2023, skor efektivitas pemerintahan Indonesia berada di sekitar persentil 50, menunjukkan bahwa masih ada tantangan dalam hal stabilitas kebijakan dan implementasi. Berbeda dengan Singapura yang dikenal sebagai salah satu negara dengan tata kelola terbaik di dunia. Sistem pemerintahannya yang meritokratis dan terpusat memungkinkan pengambilan keputusan yang cepat dan efisien. Skor WGI untuk efektivitas pemerintahan Singapura berada di persentil 90 ke atas, mencerminkan stabilitas, kejelasan kebijakan, dan implementasi yang kuat.

Sistem hukum di Indonesia masih menghadapi tantangan seperti inkonsistensi penegakan hukum, korupsi di sektor peradilan, dan akses terbatas ke keadilan bagi masyarakat tertentu. Indeks Rule of Law dari World Justice Project (2023) menempatkan Indonesia pada peringkat 63 dari 142 negara, dengan skor rendah di bidang keadilan sipil dan penegakan kontrak. Birokrasi di Indonesia sering dikritik karena lambat, rumit, dan rentan terhadap praktik korupsi. Meskipun ada reformasi birokrasi dalam beberapa tahun terakhir, seperti penyederhanaan perizinan melalui OSS (Online Single Submission), efisiensi masih terhambat oleh regulasi yang tumpang tindih dan kapasitas SDM yang bervariasi. Indeks Ease of Doing Business (sebelum dihentikan pada 2021) menempatkan Indonesia di peringkat 73. Faktor kelembagaan mencerminkan cara institusi negara mengatur tata kelola, hukum, dan

efisiensi sistem untuk mendukung pembangunan. Perbandingan Indonesia dan Singapura menunjukkan kontras signifikan akibat perbedaan skala, sejarah, dan pendekatan pemerintahan.

Indonesia, sebagai negara kepulauan besar dengan demokrasi presidensial, menghadapi tantangan kompleks dalam tata kelola. Sistem desentralisasi sejak 2001 memberikan otonomi daerah, tetapi sering kali memunculkan ketimpangan kapasitas antarwilayah dan koordinasi yang lemah antarlembaga pusat-daerah. Efektivitas pemerintahan, berdasarkan data Worldwide Governance Indicators 2023, berada di kisaran persentil 50, menunjukkan implementasi kebijakan yang inkonsisten dan rentan terhadap perubahan politik. Penegakan hukum juga menjadi isu, dengan skor Rule of Law dari World Justice Project 2023 menempatkan Indonesia di peringkat 63 global, terhambat oleh korupsi di sistem peradilan, akses keadilan yang terbatas di daerah terpencil, dan lambatnya penegakan kontrak bisnis. Birokrasi Indonesia, meskipun telah direformasi melalui sistem seperti OSS, masih dianggap lambat dan rumit karena regulasi tumpang tindih dan kapasitas aparatur yang bervariasi. Soal korupsi, Indonesia berada di peringkat 115 dalam Corruption Perceptions Index 2023 dengan skor 34/100, meskipun KPK telah berhasil menangani beberapa kasus besar. Kapasitas kelembagaan di daerah sering kali lemah karena pelatihan SDM yang tidak merata dan kurangnya teknologi pendukung.

Sebaliknya, Singapura, dengan sistem pemerintahan semi-otoriter dan terpusat, menunjukkan keunggulan dalam efisiensi kelembagaan. Tata kelola Singapura mendekati ideal, dengan skor WGI di atas persentil 90, didukung oleh pengambilan keputusan yang cepat, kebijakan yang stabil, dan digitalisasi layanan publik. Sistem hukumnya sangat kuat, menempati peringkat 4 dunia dalam Rule of Law 2023, dengan peradilan independen, perlindungan hak kepemilikan yang jelas, dan penegakan hukum yang konsisten. Birokrasi Singapura adalah salah satu yang paling efisien global, dengan proses perizinan yang transparan dan cepat, menjadikannya peringkat teratas dalam Ease of Doing Business hingga indeks tersebut dihentikan. Korupsi hampir tidak ada, dengan peringkat 5 dunia dalam (skor

83/100), didukung oleh CPIB yang efektif dan budaya akuntabilitas yang kuat. Kapasitas kelembagaan Singapura diperkuat oleh meritokrasi ketat, di mana pegawai publik direkrut dan dilatih berdasarkan kompetensi tinggi, ditambah investasi besar dalam teknologi dan inovasi.[97]

Perbedaan mendasar terletak pada skala dan konteks. Indonesia menghadapi tantangan mengelola populasi besar dan wilayah yang luas, sementara Singapura, sebagai kota-negara kecil, memiliki keunggulan dalam koordinasi dan kontrol. Indonesia telah menunjukkan kemajuan, seperti digitalisasi perizinan dan penguatan KPK, tetapi masih tertinggal dalam hal konsistensi hukum dan efisiensi birokrasi. Singapura, dengan sumber daya terbatas, memaksimalkan kelembagaan melalui disiplin, teknologi, dan hukuman tegas terhadap pelanggaran.

Di Singapura, Kebebasan diatur lebih ketat demi stabilitas sosial. Misalnya, kebebasan berpendapat dibatasi oleh undang-undang seperti Internal Security Act atau Public Order Act, dan media dikontrol ketat. Menurut Pasal 8(1) dari Internal Security Act (ISA), sebelum seseorang dapat ditahan tanpa pengadilan berdasarkan ISA, Presiden harus merasa yakin bahwa penahanan tersebut diperlukan "dengan tujuan untuk mencegah orang tersebut bertindak dengan cara yang merugikan keamanan Singapura atau bagian mana pun darinya, atau merugikan pemeliharaan ketertiban umum atau layanan penting di dalamnya." Presiden tidak bertindak atas kebijaksanaan pribadinya, melainkan harus mengikuti nasihat Kabinet dalam hal ini. Dengan kata lain, Kabinetlah yang memutuskan apakah seseorang dianggap sebagai ancaman terhadap keamanan.[98]

Setelah Presiden menyatakan kepuasannya secara resmi, Menteri Dalam Negeri memiliki kewenangan untuk mengeluarkan perintah penahanan terhadap orang yang bersangkutan untuk jangka waktu tidak melebihi dua tahun. Sebagai alternatif, alih-alih menahan orang tersebut, Menteri dapat mengeluarkan perintah

[97] K. Shanmugam, 'The Rule of Law in Singapore', *Singapore Journal of Legal Studies*, no. 12 (2012), pp. 357–65, doi:10.2139/ssrn.2255270.

[98] Jack Tsen-Ta Lee, 'The Past, Present and Future of the Internal Security Act', *SSRN Electronic Journal*, 2012, doi:10.2139/ssrn.2075475.

yang membatasi aktivitas dan tempat tinggal serta tempat kerja orang tersebut; memberlakukan jam malam; mewajibkan orang tersebut untuk memberi tahu pihak berwenang mengenai pergerakannya; serta melarang orang tersebut untuk berbicara dalam pertemuan umum; memegang jabatan, ikut serta dalam kegiatan, atau bertindak sebagai penasihat dari organisasi atau asosiasi apa pun; terlibat dalam aktivitas politik; atau bepergian ke bagian mana pun dari Singapura atau ke luar negeri.

Untuk informasi, Internal Security Act (ISA): Memungkinkan penahanan tanpa pengadilan untuk alasan keamanan nasional, termasuk ujaran yang dianggap mengancam stabilitas. Warga Singapura tetap dapat menyuarakan pendapat, tetapi dalam batas-batas tertentu, terutama melalui saluran resmi seperti dialog dengan pemerintah atau di Speakers' Corner. Namun, kritik tajam terhadap pemerintah atau isu sensitif seperti ras dan agama sering kali dihindari karena risiko hukuman. Menurut laporan Freedom House (2024), Singapura mendapat skor rendah dalam hal kebebasan berpendapat, meskipun tetap dianggap sebagai salah satu negara paling stabil dan makmur. Singapura pernah mengalami kerusuhan rasial pada 1960-an, yang membuat pemerintah sangat waspada terhadap ujaran yang dapat memicu konflik. Pengalaman ini membentuk kebijakan ketat untuk mencegah polarisasi masyarakat. Oleh karena itu, pemerintah Singapura membentuk aturan Internal Security Act. Singapura memiliki undang-undang seperti *Protection from Online Falsehoods and Manipulation Act* (POFMA) yang mengatur penyebaran informasi di internet. Sertifikasi elektronik, seperti autentikasi identitas digital, dapat digunakan untuk melacak sumber konten online, termasuk postingan media sosial atau artikel yang dianggap melanggar aturan. Sistem seperti *SingPass* (identitas digital nasional Singapura) atau sertifikat elektronik lainnya memungkinkan pemerintah memverifikasi identitas pengguna internet, sehingga memudahkan pelacakan individu yang dianggap menyebarkan ujaran yang dilarang (misalnya, ujaran kebencian atau informasi palsu). Pemerintah Singapura mewajibkan platform digital untuk mematuhi

regulasi ketat. Sertifikasi elektronik digunakan untuk memastikan bahwa platform atau penyedia layanan internet memiliki sistem keamanan yang memenuhi standar pemerintah, termasuk untuk memantau konten yang dianggap sensitif. Misalnya, pihak berwenang dapat meminta platform untuk menghapus konten berdasarkan POFMA, dan sertifikasi elektronik memastikan bahwa perintah ini dikirim dan diterima dengan aman serta sah.

Di Indonesia, sertifikasi elektronik juga digunakan (misalnya, melalui Badan Siber dan Sandi Negara atau penyedia seperti BSrE), tetapi pengawasan terhadap kebebasan berpendapat tidak seketat Singapura. Indonesia memiliki UU ITE (Informasi dan Transaksi Elektronik) yang mengatur konten online, tetapi penegakannya cenderung kurang konsisten dan lebih dipengaruhi oleh dinamika politik atau sosial. Akan tetap, Indonesia menjamin kebebasan berpendapat sebagaimana diatur dalam Undang-Undang Dasar 1945, khususnya Pasal 28E ayat (3) yang menyatakan bahwa setiap orang berhak atas kebebasan berserikat, berkumpul, dan mengeluarkan pendapat. Namun, meskipun kebebasan berpendapat diakui secara konstitusional, ada beberapa perbedaan signifikan dengan Singapura dalam hal implementasi, pengawasan, dan pembatasan, terutama dalam konteks sertifikasi elektronik atau pengaturan ruang digital.

C. Faktor Teknologi dan Infrastruktur

teknologi dan infrastruktur yang menjadi fondasi implementasi kebijakan dan regulasi di kedua negara. Adopsi teknologi di Indonesia masih menghadapi tantangan seperti kesenjangan digital antar wilayah, keterbatasan literasi digital, dan kerentanan data elektronik terhadap manipulasi atau penyadapan. Infrastruktur teknologi informasi di Indonesia cenderung lebih berfokus pada aspek luas, mencakup transaksi elektronik hingga perlindungan privasi online, namun kurang spesifik pada perlindungan infrastruktur kritis dibandingkan Singapura.

Pada 2020, ndonesia mengalami peningkatan penggunaan tanda tangan elektronik, terutama selama pandemi Covid-19, dengan lonjakan pengguna baru

sebesar 61% pada 2020, sebagaimana dilaporkan oleh penyedia layanan seperti PrivyID. Badan Siber dan Sandi Negara (BSSN) menerbitkan Peraturan BSSN Nomor 7 Tahun 2024 tentang Penilaian Kesesuaian Kriteria Umum untuk Evaluasi Keamanan Teknologi Informasi, yang menetapkan standar seperti SNI ISO/IEC 15408 untuk keamanan siber, alasan adanya komparasi ialah Singapura dikenal dengan sistem keamanan siber yang kuat, fokus pada perlindungan infrastruktur kritis, dan investasi besar dalam teknologi mutakhir seperti smart nation initiatives. Ini memungkinkan implementasi sertifikasi elektronik yang lebih efisien dan aman dibandingkan Indonesia. Selama ini, Singapura telah menerapkan Cybersecurity Act atau Undang-Undang Keamanan Siber yang mengatur pemberian lisensi bagi penyedia layanan keamanan siber. Tujuannya adalah untuk menjamin keamanan dan kenyamanan pengguna, meningkatkan kualitas serta standar penyedia jasa, sekaligus mengevaluasi kinerja mereka secara berkala.[99]

Berbeda dengan Indonesia, infrastruktur TIK di Indonesia masih berkembang, dengan tantangan seperti kesenjangan digital antar wilayah dan kerentanan infrastruktur kritis terhadap serangan siber, seperti insiden ransomware pada Pusat Data Nasional (PDN). Regulasi seperti UU ITE dan PP PSTE berfokus pada penguatan keamanan, namun implementasinya masih terhambat oleh keterbatasan infrastruktur dan sumber daya. Akan tetapi, Indonesia mulai membangun kerja sama internasional, seperti melalui BSSN dan forum seperti Indonesia Cyber Security Forum (ICSF).

Teknologi infrastruktur di Indonesia dan Singapura menunjukkan perbedaan signifikan akibat tingkat pembangunan ekonomi, skala wilayah, dan prioritas kebijakan masing-masing negara. Berikut penjelasan mengenai teknologi infrastruktur kedua negara dalam aspek fisik (seperti transportasi dan energi) dan non-fisik (seperti teknologi informasi dan komunikasi/TIK), serta konteks kerja sama dan tantangan yang dihadapi.

---

[99] 'J*anuary 2019', Journal of Business & Management (Coes&Rj-Jbm), 7.1 (2019), doi:10.25255/jbm.2019.7.1.*

Indonesia, sebagai negara kepulauan terbesar di dunia dengan populasi lebih dari 270 juta, fokus pada pembangunan infrastruktur untuk meningkatkan konektivitas antarwilayah, daya saing ekonomi, dan pemerataan pembangunan. Infrastruktur fisik, seperti jalan, pelabuhan, bandara, dan waduk, menjadi prioritas utama pemerintah melalui Proyek Strategis Nasional (PSN). Contohnya, proyek Palapa Ring, yaitu jaringan serat optik broadband yang menghubungkan lebih dari 514 kabupaten/kota, bertujuan meningkatkan akses internet di seluruh wilayah, termasuk daerah terpencil seperti Maluku dan Papua. Proyek ini didukung oleh Satelit Multifungsi Satria dengan kapasitas 150 Gb/detik untuk memperkuat jaringan backbone. Selain itu, pembangunan infrastruktur transportasi, seperti jalan tol, MRT di Jakarta, dan bandara baru, bertujuan menurunkan biaya logistik yang masih tinggi, yaitu sekitar 14,29% dari PDB pada 2023, jauh lebih tinggi dibandingkan Singapura yang di bawah 10%.

Di bidang teknologi informasi, Indonesia berupaya mempercepat transformasi digital melalui pengembangan data center, seperti di KEK Nongsa, Batam, yang diharapkan menghemat devisa hingga Rp30 triliun per tahun. Namun, tantangan besar meliputi rendahnya kualitas bandwidth, infrastruktur kabel yang belum memadai, dan disharmonisasi regulasi antara pusat dan daerah yang menyebabkan biaya internet tinggi. Indeks Pembangunan TIK (IP-TIK) Indonesia pada 2022 mencapai 5,85 dari skala 10, menunjukkan kemajuan tetapi masih tertinggal dibandingkan Singapura. Selain itu, rendahnya literasi digital masyarakat dan keterbatasan daya beli memperumit aksesibilitas teknologi digital. Untuk mendukung transformasi digital, pemerintah mendorong pengembangan talenta digital di bidang AI dan IoT, serta menerapkan sistem transportasi cerdas (Intelligent Transportation Systems) dan pembayaran elektronik.

Pembangunan infrastruktur di Indonesia melibatkan kolaborasi pemerintah, swasta, dan BUMN, dengan pendanaan dari APBN dan investasi asing. Lembaga seperti LMAN dan KPPIP dibentuk untuk mempercepat proyek infrastruktur, tetapi keterbatasan anggaran (misalnya, Rp240 triliun diperlukan untuk jalan nasional)

mendorong keterlibatan investor swasta. Namun, regulasi yang tumpang tindih dan kurangnya koordinasi antarpihak sering menghambat efisiensi.

Berbeda hal-nya dengan Singapura, sebagai negara kota dengan populasi sekitar 5,7 juta, memiliki infrastruktur teknologi yang sangat maju, menjadikannya salah satu pusat finansial dan teknologi terkemuka di dunia. Infrastruktur fisik Singapura, seperti transportasi massal (MRT, bus), pelabuhan, dan bandara, didukung oleh teknologi canggih seperti manajemen lalu lintas real-time dan pembayaran elektronik tanpa kontak. Sistem Common Service Tunnel dan Utility Service Ducts, yang mengintegrasikan utilitas seperti air, listrik, dan telekomunikasi di bawah tanah, menjadi contoh inovasi yang efisien dan ramah lingkungan. Pengelolaan limbah, air, dan sampah juga menggunakan teknologi mutakhir, mendukung visi "Smart Nation" yang mengintegrasikan teknologi digital untuk meningkatkan kualitas hidup.

Di bidang TIK, Singapura unggul dengan infrastruktur jaringan internet yang inklusif, mencatat skor 86,8 pada indeks akses internet 2021, jauh di atas Indonesia (67,8). Infrastruktur ini didukung oleh jaringan serat optik yang luas, data center canggih, dan keamanan siber yang kuat. Singapura juga menjadi pusat startup teknologi dan inovasi, dengan ekosistem yang mendukung pengembangan cryptocurrency dan teknologi blockchain, berkat infrastruktur internet yang mumpuni dan tingkat edukasi digital yang tinggi. Program seperti GovTech, di bawah Perdana Menteri, mengoordinasikan transformasi digital dengan pendekatan n-helix, melibatkan pemerintah, swasta, dan akademisi.

Singapura juga fokus pada teknologi hijau, seperti pengembangan energi terbarukan dan transportasi rendah emisi, serta kolaborasi internasional untuk proyek seperti kabel listrik bawah laut dengan Indonesia. Infrastruktur ini mendukung daya saing global Singapura, dengan peringkat pertama di ASEAN menurut Global Competitiveness Index 2019.

Kedua negara telah menjalin kerja sama di bidang teknologi infrastruktur untuk saling melengkapi keunggulan masing-masing. Singapura membantu Indonesia dalam pengembangan Palapa Ring dengan teknologi dan keahlian, serta berkontribusi

pada pembangunan Nongsa Digital Park di Batam, yang menjadi pusat data dan inovasi. Indonesia, dengan pasar besar dan sumber daya manusia yang melimpah, menawarkan peluang ekspansi bagi perusahaan teknologi Singapura. Contoh kerja sama lainnya termasuk pelatihan SDM teknologi, pengembangan startup, dan keamanan siber untuk melawan kejahatan digital. Pada 2023, kedua negara menandatangani 20 letter of intent untuk investasi di IKN, termasuk di bidang energi, kesehatan, dan digital. Benchmarking infrastruktur oleh Otorita IKN di Singapura pada 2024 menunjukkan upaya Indonesia untuk mengadopsi teknologi hijau dan digital Singapura, seperti pengelolaan limbah dan utilitas. Indonesia menghadapi tantangan dalam kesenjangan infrastruktur digital, terutama di daerah terpencil, serta regulasi yang belum selaras. Singapura, meski unggul, memiliki keterbatasan lahan dan populasi, sehingga bergantung pada pasar regional seperti Indonesia. Kerja sama kedua negara menawarkan peluang untuk mengatasi tantangan ini, seperti meningkatkan literasi digital di Indonesia dan memperluas pasar teknologi Singapura.

Namun, harmonisasi regulasi, investasi dalam SDM, dan penerapan teknologi yang sesuai dengan konteks lokal menjadi kunci keberhasilan. Seperti disebutkan dalam pertanyaan awal, rendahnya daya saing dan kepatuhan terhadap SNI di Indonesia menunjukkan perlunya regulasi daerah yang mendukung standar dan penilaian kesesuaian. Regulasi ini dapat mengintegrasikan upaya pemerintah daerah, BSN, swasta, dan BUMN untuk menerapkan standar teknologi infrastruktur, seperti dalam proyek TIK dan transportasi, guna mendukung pembangunan yang lebih terarah dan komprehensif. Singapura, dengan pendekatan terpusatnya, dapat menjadi inspirasi bagi Indonesia dalam menyusun regulasi yang efisien.

Akses infrastruktur TIK berdampak positif dan signifikan terhadap PDRB di Indonesia bagian barat maupun timur. Namun, dampaknya lebih besar di Indonesia bagian timur, mencapai 0,4110%, dibandingkan bagian barat sebesar 0,2647%. Perbedaan ini mencerminkan tahap pembangunan TIK yang berbeda. Bagian barat, yang telah lebih dulu memiliki infrastruktur dan akses TIK yang lebih baik, menunjukkan dampak ekonomi yang relatif lebih rendah. Sebaliknya, bagian timur

sedang mengalami pembangunan infrastruktur TIK yang pesat, dengan akses internet yang semakin meningkat, menjadi hal baru bagi provinsi-provinsi di wilayah ini. Karenanya, masih terdapat potensi besar untuk memanfaatkan TIK guna mendorong pertumbuhan ekonomi di kawasan timur.[100] Berbeda dengan penggunaan TIK, hanya Indonesia bagian barat yang merasakan dampak positif dan signifikan terhadap pertumbuhan ekonomi. Setiap peningkatan 1% dalam penggunaan TIK berkontribusi pada kenaikan pertumbuhan ekonomi sebesar 0,0376%, dengan asumsi ceteris paribus. Provinsi-provinsi di wilayah ini telah mengintegrasikan TIK dalam berbagai sektor, seperti ekonomi, pendidikan, kesehatan, dan pemerintahan.

Keberadaan sistem pembayaran digital seperti QRIS dan maraknya belanja online mendorong peningkatan penggunaan TIK. Selain itu, sejumlah perusahaan di kawasan ini telah menerapkan berbagai perangkat lunak dan perangkat keras TIK untuk mendukung operasional mereka. Peningkatan penggunaan Quick Response Code Indonesian Standard (QRIS) di Indonesia menunjukkan perkembangan pesat dalam transformasi pembayaran digital, sejalan dengan upaya Bank Indonesia (BI) dan Asosiasi Sistem Pembayaran Indonesia (ASPI) untuk mendorong masyarakat tanpa tunai (cashless society). QRIS, yang diluncurkan pada 17 Agustus 2019 dan diterapkan secara nasional mulai 1 Januari 2020, telah menjadi alat pembayaran yang populer dan efisien, terutama di kalangan Usaha Mikro, Kecil, dan Menengah (UMKM). Penggunaan QRIS telah meningkat secara signifikan sejak peluncurannya.

Berdasarkan data, pada Oktober 2023, QRIS telah diadopsi oleh 29,6 juta merchant dan 43,44 juta pengguna, dengan 92% di antaranya adalah UMKM. Hingga 2024, jumlah pengguna QRIS mencapai 50,5 juta dengan 32,71 juta merchant, dan nilai transaksi tahunan mencapai Rp42 triliun (setara $2,57 miliar), dengan pertumbuhan transaksi sebesar 226,54% dibandingkan tahun sebelumnya. Pada Januari 2025, transaksi QRIS mencatatkan nilai Rp80 triliun dengan 790 juta

[100] David Richardo Sibarani and others, 'Pertumbuhan Ekonomi Indonesia (The Impact of Information and Communications Technology Access Use and Expertise on Indonesia's Economic Growth)', *Jurnal Resolusi Konflik*, 8.2 (2023), pp. 32–42.

transaksi, menunjukkan akselerasi adopsi yang luar biasa, penggunaan QRIS (Quick Response Code Indonesian Standard) dalam konteks sertifikasi elektronik merujuk pada integrasi teknologi pembayaran digital berbasis kode QR dengan sistem sertifikasi elektronik untuk mendukung transaksi yang aman, efisien, dan terverifikasi secara digital. Sertifikasi elektronik, sebagaimana diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) serta Peraturan Pemerintah Nomor 71 Tahun 2019, melibatkan penggunaan Sertifikat Elektronik yang dikeluarkan oleh Penyelenggara Sertifikasi Elektronik (PSrE) untuk memastikan keabsahan identitas dan keamanan transaksi elektronik, QRIS menggunakan standar keamanan berbasis teknologi enkripsi dan autentikasi yang selaras dengan prinsip sertifikasi elektronik. Penyelenggara Jasa Sistem Pembayaran (PJSP) wajib memenuhi standar keamanan yang ditetapkan BI, termasuk sertifikasi keamanan siber yang diakui nasional dan internasional. Ini memastikan bahwa transaksi QRIS memiliki keabsahan hukum dan perlindungan terhadap penipuan, seperti pemalsuan kode QR.[101]

QRIS dalam sertifikasi elektronik berperan sebagai alat pembayaran digital yang terintegrasi dengan sistem keamanan dan verifikasi identitas berbasis Sertifikat Elektronik. Melalui standar yang ditetapkan BI dan PSrE, QRIS mendukung transaksi yang cepat, aman, dan terjangkau, dengan dampak positif pada inklusi keuangan dan pertumbuhan ekonomi. Namun, tantangan seperti keamanan siber dan literasi digital perlu diatasi melalui regulasi daerah yang selaras, edukasi, dan investasi infrastruktur TIK. Dengan harmonisasi ini, QRIS dan sertifikasi elektronik dapat menjadi pilar utama transformasi digital di Indonesia. Bank Indonesia, sebagai lembaga negara dan badan hukum publik, memiliki wewenang untuk menetapkan peraturan sesuai dengan batas kewenangannya. Pembentukan peraturan di Bank Indonesia wajib mematuhi prinsip pembentukan peraturan perundang-undangan serta asas umum pemerintahan yang baik. Untuk mendukung proses ini, diperlukan prosedur dan metode standar

[101] Dinda Shafira Maharani and others, 'Peran Infrastruktur Teknologi Dalam Meningkatkan The Role Of Technology Infrastructure In Enhancing', 4.1 (2025), pp. 15–22.

sebagai pedoman. Dalam hal ini, Bank Indonesia telah menerbitkan Peraturan Bank Indonesia Nomor 18/42/PBI/2016 tentang Pembentukan Peraturan di Bank Indonesia (PBI Pembentukan Peraturan di Bank Indonesia).[102]

Terdapat kerja sama lintas batas (cross-border QR payment linkage) antara Indonesia dan Singapura yang memungkinkan pengguna QRIS dari Indonesia untuk melakukan pembayaran di merchant Singapura yang mendukung NETS QR/SGQR, dan sebaliknya. Kerja sama ini resmi diluncurkan pada 17 November 2023 oleh Bank Indonesia dan Monetary Authority of Singapore (MAS), Dalam konteks sertifikasi elektronik, QRIS dan NETS QR/SGQR menggunakan standar keamanan berbasis teknologi enkripsi yang selaras dengan EMVCo, standar internasional untuk pembayaran QR.

Di Indonesia, QRIS diatur oleh BI dan memenuhi persyaratan keamanan yang diawasi oleh Penyelenggara Jasa Sistem Pembayaran (PJSP). Sertifikasi elektronik, seperti yang dikeluarkan oleh Penyelenggara Sertifikasi Elektronik (PSrE) di bawah UU ITE, dapat digunakan untuk memverifikasi identitas merchant atau transaksi QRIS, terutama dalam pembayaran lintas batas, untuk memastikan keabsahan dan keamanan. Di Singapura, NETS QR juga menerapkan protokol keamanan serupa untuk melindungi data pengguna, melalui kerja sama lintas batas yang dimulai pada November 2023, QRIS dapat digunakan di Singapura untuk membayar di merchant yang mendukung NETS QR, dan sebaliknya. Integrasi ini memperkuat ekosistem pembayaran digital di kedua negara, didukung oleh standar keamanan yang selaras dengan sertifikasi elektronik untuk memastikan transaksi aman dan terverifikasi. Untuk memastikan kelancaran, pengguna disarankan memeriksa kompatibilitas aplikasi pembayaran dan merchant yang tergabung dalam kerja sama ini.

Kartu prabayar yang bersifat proprietary (seluruh transaksi dilakukan dalam sistem tertutup) tampak sebagai kandidat logis karena tidak melibatkan biaya antar

[102] Qurotul Aini, Untung Rahardja, and Anggy Fatillah, 'Penerapan Qrcode Sebagai Media Pelayanan Untuk Absensi Pada Website Berbasis Php Native', *Sisfotenika*, 8.1 (2018), p. 47, doi:10.30700/jst.v8i1.151.

bank (interchange), sehingga memungkinkan Merchant Discount Rate (MDR) yang lebih rendah. Kartu prabayar juga memerlukan pembayaran di muka. Pengelolaan dana pembayaran di muka ini (sering disebut escrow) diatur oleh Bank Sentral dan harus disimpan dalam rekening bank melalui hubungan kustodian. Pembayaran di muka ini memungkinkan penyedia kartu prabayar memperoleh pendapatan bunga dari dana tersebut, yang pada gilirannya mengurangi biaya operasional bisnis. Tidak ada kewajiban hukum untuk membayar bunga kepada pelanggan atas pembayaran di muka ini, sehingga semakin menekan biaya operasional. Pendapatan dari breakage (dana yang tidak digunakan) juga merupakan bagian penting dari model bisnis kartu prabayar. Di Singapura, NETS dan EZLink menjadi kandidat alami karena keduanya adalah kartu prabayar proprietary. Secara keseluruhan, kartu prabayar merupakan metode pembayaran ideal untuk langkah berikutnya dalam perjalanan menuju pembayaran tanpa tunai.[103] Perjalanan menuju masyarakat tanpa tunai memerlukan pertimbangan berbagai faktor. Fokus pada kategori pedagang dengan nilai transaksi rendah, tingkat diskon pedagang (Merchant Discount Rate), ukuran pasar domestik, antarmuka pembayaran, peran kartu transportasi umum, dan intervensi strategis pemerintah merupakan beberapa isu kunci yang perlu diperhatikan.

Menggembirakan bahwa pemerintah Singapura memimpin upaya ini melalui inisiatif Smart Nation. Inisiatif ini akan mengoordinasikan pembangunan infrastruktur akuisisi nasional berbasis kode QR. Kepemimpinan pemerintah dalam menetapkan standar dan mengoordinasikan platform bersama di antara penyedia pembayaran komersial yang berbeda demi kepentingan masyarakat juga menjadi poin pembelajaran utama. Kepemimpinan pemerintah kali ini mungkin menjadi kunci keberhasilan menuju masyarakat tanpa tunai di Singapura.

Puncak integrasi sistem pembayaran regional di Asia Tenggara terjadi saat KTT ASEAN ke-42 di Labuan Bajo, di bawah kepemimpinan Indonesia pada tahun

[103] Dennis Ng, 'Evolution of Digital Payments: Early Learnings from Singapore's Cashless Payment Drive', *Journal of Payments Strategy & Systems*, 11.4 (2018), p. 306, doi:10.69554/qohg1171.

2023. Dalam Pertemuan Para Menteri Keuangan dan Gubernur Bank Sentral ASEAN (AFMGM), komitmen mereka ditegaskan melalui sebuah komunike untuk mendorong konektivitas pembayaran regional dan mempromosikan kerangka penyelesaian transaksi menggunakan mata uang lokal dalam transaksi intra-regional (ASEAN, 2023a). Pernyataan ini memberikan kerangka politik dan hukum bagi kerja sama, koordinasi, dan integrasi lebih lanjut atas sistem pembayaran digital lintas batas seperti sistem berbasis kode QR di seluruh kawasan. Selain itu, hal ini berpotensi memperkuat keberlangsungan Masyarakat Ekonomi ASEAN (MEA) yang mendorong dan memfasilitasi masyarakatnya untuk secara aktif berpartisipasi dalam pasar keuangan regional demi keuntungan mereka sendiri.[104]

Dengan demikian, teknologi infrastruktur Indonesia sedang berkembang pesat namun masih menghadapi tantangan akses dan regulasi, sedangkan Singapura telah mencapai tingkat kemajuan tinggi dengan fokus pada efisiensi dan inovasi. Kerja sama kedua negara menjadi jembatan untuk mempercepat transformasi digital dan pembangunan berkelanjutan.

[104] Azza Bimantara, Rangga Tri Nugraha, and Universitas Muhammadiyah Malang, 'The Politics of International Cooperation in Cross-Border Digital Payment Connectivity: A Case Study of QR Payment System in Asean Azza Bimantara 1* , Rangga Tri Nugraha 2', 8090.246 (2025), pp. 82–99, doi:10.22219/jurnalsospol.v11i1.38367.

Bab IV

Perbandingan Sistem Hukum Dan Analisis Faktor Yang Mempengaruhi

Bab ini menyajikan hasil dan pembahasan dari penelitian yang dilakukan terkait Analisis komparasi sistem hukum di bidang Sertifikasi Elektronik antara Indonesia dan Singapura. Pembahasan ini diarahkan untuk menjawab dua rumusan masalah utama yang telah dirumuskan sebelumnya, yaitu: (1) Bagaimana kedudukan sistem hukum di bidang Sertifikasi Elektronik antara Indonesia dan Singapura? (2) Apa faktor yang mempengaruhi adanya perbandingan sistem hukum di bidang Sertifikasi Elektronik antara Indonesia dengan Singapura?

A. Perbandingan kedudukan sistem hukum di bidang Sertifikasi Elektronik antara Indonesia dan Singapura

1. Persamaan

Pasal 5 Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas UU ITE:[105]

(1) Informasi Elektronik dan/ atau Dokumen Elektronik dan/ atau hasil cetaknya merupakan alat bukti hukum yang sah.

(2) Informasi Elektronik dan/ atau Dokumen Elektronik dan/ atau hasil cetaknya sebagaimana dimaksud pada ayat (1) merupakan perluasan dari alat bukti yang sah sesuai dengan Hukum Acara yang berlaku di Indonesia.

[105] Pasal 5, Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, ‘.

(3) Informasi Elektronik dan/ atau Dokumen Elektronik dinyatakan sah apabila menggunakan Sistem Elektronik sesuai dengan ketentuan yang diatur dalam Undang-Undang ini.

(4) Ketentuan mengenai Informasi Elektronik dan/atau Dokumen Elektronik sebagaimana dimaksud pada ayat (l) tidak berlaku dalam hal diatur lain dalam Undang-Undang.

Cap. 88 Electronic Transaction Signatures, PART II ELECTRONIC RECORDS, SIGNATURES AND CONTRACTS, Section 8.[106]

Requirement for signature 8. Where a rule of law requires a signature, or provides for certain consequences if a document or a record is not signed, that requirement is satisfied in relation to an electronic record if —

(a) a method is used to identify the person and to indicate that person's intention in respect of the information contained in the electronic record;

and (b) the method used is either —

(i) as reliable as appropriate for the purpose for which the electronic record was generated or communicated, in the light of all the circumstances, including any relevant agreement; or

(ii) proven in fact to have fulfilled the functions described in paragraph (a), by itself or together with further evidence.

[106] *Cap. 88 Section 8 T H E Law and others, 'The Statutes of the Republic of Singapore - COPYRIGHT ACT', 2008.March 2008 (2015).*

Terjemahan;

Apabila suatu ketentuan hukum mensyaratkan adanya tanda tangan, atau menetapkan konsekuensi tertentu jika suatu dokumen atau catatan tidak ditandatangani, maka persyaratan tersebut dianggap terpenuhi dalam kaitannya dengan catatan elektronik apabila:

(a) digunakan suatu metode untuk mengidentifikasi orang tersebut dan menunjukkan niat orang tersebut terhadap informasi yang terkandung dalam catatan elektronik; dan

(b) metode yang digunakan adalah:

(i) seandal yang sesuai untuk tujuan catatan elektronik tersebut dibuat atau dikomunikasikan, dengan mempertimbangkan seluruh keadaan, termasuk perjanjian yang relevan; atau

(ii) terbukti secara faktual telah memenuhi fungsi-fungsi sebagaimana dijelaskan dalam paragraf (a), baik secara mandiri maupun bersama dengan bukti tambahan.

Article 5 UNCITRAL Model Law On Electronic Signatures 2001

Article 5. Variation by agreement

"The provisions of this Law may be derogated from or their effect may be varied by agreement, unless that agreement would not be valid or effective under applicable law." [107]

Terjemahan:

Pasal 5. Perubahan Berdasarkan Kesepakatan

[107] *UNCITRAL model law on Electronic Signatures, Article 5.*

> Ketentuan dalam Undang-Undang ini dapat dikesampingkan atau diubah efektivitasnya melalui kesepakatan, kecuali jika kesepakatan tersebut tidak sah atau tidak berlaku menurut hukum yang berlaku.

Undang-Undang No. 1 Tahun 2024, memiliki kesamaan mendasar dengan UNCITRAL Model Law Pasal 5 dalam pengakuan hukum terhadap informasi dan dokumen elektronik sebagai alat bukti yang sah. Dalam Pasal 5 UU ITE, dinyatakan bahwa informasi elektronik, dokumen elektronik, dan hasil cetaknya diakui sebagai alat bukti hukum yang sah, sejalan dengan Hukum Acara yang berlaku di Indonesia. Demikian pula, ETA Cap. 88, pada Section 8, menetapkan bahwa dokumen elektronik tidak boleh ditolak keabsahannya hanya karena bentuknya elektronik, selama memenuhi persyaratan tertentu seperti keandalan dan integritas. Persamaan ini menjadi dasar bagi PSrE di Indonesia dan Certification Authorities (CAs) di Singapura untuk memastikan bahwa sertifikat elektronik, seperti tanda tangan digital, memiliki kekuatan hukum dalam transaksi, baik untuk keperluan bisnis, pemerintahan, maupun hukum. Ini selaras dengan prinsip inti UNCITRAL Model Law on Electronic Commerce, khususnya Pasal 5, yang menetapkan bahwa data elektronik tidak boleh ditolak keabsahannya hanya karena bersifat elektronik, selama memenuhi persyaratan tertentu. Kedua regulasi ini bertujuan memberikan kepastian hukum terhadap penggunaan dokumen elektronik dalam transaksi, termasuk dalam konteks PSrE, yang memastikan keabsahan tanda tangan elektronik atau sertifikat digital untuk autentikasi.

Pasal 13 Undang-Undang Nomor 1 Tahun 2024 Perubahan Kedua dari Undang-Undang ITE:[108]

(1) Setiap Orang berhak menggunakan Penyelenggara Sertifikasi Elektronik pembuatan Tanda Tangan Elektronik.

(2) Penyelenggara Sertilikasi Elektronik harus memastikan keterkaitan suatu Tanda Tangan Elektronik dengan pemiliknya.

(3) Penyelenggara Sertifikasi Elektronik yang beroperasi di Indonesia harus berbadan hukum Indonesia dan berdomisili di Indonesia.

Pasal 13A Undang-Undang Nomor 1 Tahun 2024 Perubahan Kedua dari Undang-Undang ITE:[109]

(1) Penyelenggara Sertifikasi Elektronik dapat menyelenggarakan layanan berupa:

a. Tanda Tangan Elektronik;

b. segel elektronik;

c. penanda waktu elektronik;

d. layanan pengiriman elektronik tercatat; e. autentikasi situs web;

f. preservasi Tanda Tangan Elektronik dan/ atau segel elektronik;

g. identitas digital; dan/atau h. layanan lain yang menggunakan Sertifikat Elektronik.

[108] Pasal 13 Undang-undang Nomor 1 Tahun 2024 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik,

[109] Pasal 13A Undang-undang Nomor 1 Tahun 2024 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik

Cap. 88 Electronic Transaction Signatures PART III SECURE ELECTRONIC RECORDS AND SIGNATURES, Section 17 Secure electronic record[110]

17.—(1) If a specified security procedure, or a commercially reasonable security procedure agreed to by the parties involved, has been properly applied to an electronic record to verify that the electronic record has not been altered since a specific point in time, such record shall be treated as a secure electronic record from such specific point in time to the time of verification.

(2) For the purposes of this section and section 18, whether a security procedure is commercially reasonable shall be determined having regard to the purposes of the procedure and the commercial circumstances at the time the procedure was used, including —

(a) the nature of the transaction;

(b) the sophistication of the parties;

(c) the volume of similar transactions engaged in by either or all parties;

(d) the availability of alternatives offered to but rejected by any party;

(e) the cost of alternative procedures; and

(f) the procedures in general use for similar types of transactions

Terjemahan;

Pasal 17.—

(1) Jika suatu prosedur keamanan tertentu, atau prosedur keamanan yang secara komersial wajar dan disepakati oleh para pihak yang terlibat, telah diterapkan dengan tepat pada suatu catatan elektronik untuk memverifikasi bahwa catatan

[110] *Cap. 88 Section 8* Law and others, 'The Statutes of the Republic of Singapore - Copyright Act'.

elektronik tersebut tidak mengalami perubahan sejak waktu tertentu, maka catatan tersebut akan dianggap sebagai catatan elektronik yang aman sejak waktu tertentu tersebut hingga waktu verifikasi dilakukan.

(2) Untuk keperluan pasal ini dan pasal 18, apakah suatu prosedur keamanan dapat dianggap secara komersial wajar ditentukan dengan mempertimbangkan tujuan dari prosedur tersebut serta kondisi komersial pada saat prosedur digunakan, termasuk:

(a) jenis transaksi yang dilakukan;

(b) tingkat kecanggihan para pihak yang terlibat;

(c) jumlah transaksi serupa yang dilakukan oleh salah satu atau semua pihak;

(d) ketersediaan alternatif yang ditawarkan namun ditolak oleh salah satu pihak;

(e) biaya dari prosedur alternatif tersebut; dan

(f) prosedur yang lazim digunakan dalam jenis transaksi serupa.

.

Article 6, UNCITRAL Model Law On Electronic Signatures

Article 6. Compliance with a requirement for a signature

1. Where the law requires a signature of a person, that requirement is met in relation to a data message if an electronic signature is used that is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.

2. Paragraph 1 applies whether the requirement referred to therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature.

3. An electronic signature is considered to be reliable for the purpose of satisfying the requirement referred to in paragraph 1 if:

(a) The signature creation data are, within the context in which they are used, linked to the signatory and to no other person; UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001 3

(b) The signature creation data were, at the time of signing, under the control of the signatory and of no other person;

(c) Any alteration to the electronic signature, made after the time of signing, is detectable; and

(d) Where a purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable.

4. Paragraph 3 does not limit the ability of any person:

(a) To establish in any other way, for the purpose of satisfying the requirement referred to in paragraph 1, the reliability of an electronic signature; or

(b) To adduce evidence of the non-reliability of an electronic signature.

5. The provisions of this article do not apply to the following: [...].

Terjemahan:

Pasal 6 Kepatuhan terhadap Persyaratan Tanda Tangan

1. Apabila hukum mensyaratkan adanya tanda tangan dari seseorang, persyaratan tersebut dianggap terpenuhi terhadap suatu pesan data apabila digunakan tanda tangan elektronik yang tingkat keandalannya sesuai dengan

tujuan pesan data tersebut dibuat atau dikomunikasikan, dengan mempertimbangkan seluruh keadaan, termasuk perjanjian yang relevan.

2. Ayat (1) berlaku baik jika persyaratan tanda tangan tersebut berbentuk kewajiban hukum maupun jika hukum hanya menetapkan konsekuensi atas tidak adanya tanda tangan.
3. Suatu tanda tangan elektronik dianggap andal untuk memenuhi persyaratan sebagaimana dimaksud dalam ayat (1) apabila:

   (a) Data pembuat tanda tangan, dalam konteks penggunaannya, terkait dengan penanda tangan dan tidak dengan pihak lain;

   (b) Data pembuat tanda tangan, pada saat penandatanganan, berada di bawah kendali penanda tangan dan tidak ada orang lain yang mengendalikannya;

   (c) Setiap perubahan terhadap tanda tangan elektronik setelah waktu penandatanganan dapat terdeteksi; dan

   (d) Jika tujuan dari persyaratan hukum atas tanda tangan adalah untuk menjamin integritas informasi yang ditandatangani, maka setiap perubahan terhadap informasi tersebut setelah waktu penandatanganan dapat terdeteksi.
4. Ayat (3) tidak membatasi hak siapa pun:

   (a) Untuk membuktikan dengan cara lain bahwa suatu tanda tangan elektronik andal guna memenuhi persyaratan sebagaimana dimaksud dalam ayat (1); atau

   (b) Untuk mengajukan bukti bahwa tanda tangan elektronik tersebut tidak andal.
5. Ketentuan dalam pasal ini tidak berlaku untuk hal-hal berikut: [...].[111]

[111] Article 6, Uncitral Model Law On Electronic Signatures

Selanjutnya, UU ITE mengatur PSrE dalam Pasal 13 dan Pasal 13A, yang menguraikan tugas PSrE dalam menerbitkan sertifikat elektronik untuk menjamin keaslian dan integritas transaksi elektronik. ETA Cap. 88, pada Section 17 mengatur tugas serupa untuk CAs, yang bertanggung jawab menerbitkan sertifikat elektronik untuk memverifikasi identitas dan keaslian tanda tangan elektronik, dengan standar teknis yang ketat untuk menjamin kepercayaan. Baik PSrE maupun CAs diharuskan mematuhi persyaratan teknis dan hukum, seperti penggunaan teknologi kriptografi, untuk memastikan integritas transaksi digital.

Ini selaras dengan UNCITRAL Model Law on Electronic Signatures, khususnya Pasal 6, yang mengatur peran otoritas sertifikasi (Certification Service Providers) dalam memverifikasi identitas pihak yang menggunakan tanda tangan elektronik dan memastikan keamanan melalui teknologi seperti Public Key Infrastructure (PKI). Kedua kerangka hukum ini menekankan bahwa PSrE atau otoritas sertifikasi harus memenuhi standar teknis dan prosedur untuk menjamin kepercayaan, meskipun UU ITE lebih spesifik dengan mewajibkan registrasi PSrE di bawah Kementerian Komunikasi dan Informatika, sedangkan UNCITRAL memberikan panduan yang lebih umum.

2. Perbedaan

Sifat Hukum pada kedua negara seperti Undang-Undang No. 1 Tahun 2024 adalah undang-undang nasional yang mengikat di Indonesia, dengan cakupan luas meliputi tanda tangan elektronik, kejahatan siber, dan perlindungan konsumen. ETA Singapura juga mengikat, tetapi lebih fokus pada transaksi elektronik dan perdagangan, dengan infrastruktur teknologi yang lebih matang seperti otoritas sertifikasi. UNCITRAL Model Law bersifat non-binding, berfungsi sebagai pedoman internasional yang diadopsi oleh Indonesia dan Singapura dengan penyesuaian sesuai konteks nasional.

Untuk Informasi, Indonesia belum sepenuhnya resmi mengadopsi UNCITRAL secara keseluruhan akan tetapi, ada elemen-elemen dari UNCITRAL yang diadopsi dalam hukum nasional.

Rangkuman beberapa perbedaan dalam sistem hukum di Indonesia dan Singapura, yaitu;

1. Di Indonesia, Tanda tangan elektronik didefinisikan sebagai informasi elektronik yang dilekatkan, terasosiasi, atau terkait dengan informasi elektronik lainnya yang digunakan sebagai alat verifikasi dan autentikasi, Tanda tangan elektronik memiliki kekuatan hukum yang sah jika memenuhi syarat, seperti data pembuatan tanda tangan hanya terkait penandatangan, berada dalam kuasa penandatangan, dan perubahan pada tanda tangan atau informasi elektronik dapat terdeteksi, UU ITE juga mengatur perlindungan konsumen dalam transaksi elektronik, termasuk

privasi dan keabsahan kontrak elektronik. UU No. 1 Tahun 2024 memperbarui UU ITE untuk menyesuaikan dengan perkembangan teknologi dan kebutuhan perlindungan data, meskipun detail spesifik perubahan dalam UU ini tidak sepenuhnya tercakup dalam sumber yang tersedia.

2. Di Singapura, pada ETA chap. 88 mengakui tanda tangan elektronik sebagai sah secara hukum, setara dengan tanda tangan basah, asalkan memenuhi persyaratan keandalan dan autentikasi. Tanda tangan elektronik harus dapat diidentifikasi sebagai milik penandatangan dan menunjukkan niat untuk menandatangani. Dan menekankan penggunaan teknologi yang andal untuk memastikan integritas dan keaslian tanda tangan elektronik, seperti penggunaan sertifikat digital dan otoritas sertifikasi (Certification Authorities), ETA tidak membatasi jenis teknologi tertentu untuk tanda tangan elektronik, memungkinkan fleksibilitas dalam penggunaan teknologi seperti blockchain atau kriptografi lainnya, odel Law menetapkan bahwa tanda tangan elektronik memiliki kekuatan hukum yang setara dengan tanda tangan basah jika memenuhi tiga syarat utama:

   a. Identifikasi Penandatangan Tanda tangan dapat diidentifikasi sebagai milik penandatangan.

   b. Keandalan: Metode yang digunakan cukup andal untuk tujuan tanda tangan tersebut.

   c. Kontrol Penandatangan: Data pembuatan tanda tangan berada dalam kendali penandatangan.

3. Tabel Komparasi

Berikut adalah tabel perbandingan aspek hukum sertifikasi elektronik antara Indonesia dan Singapura dari sisi cakupan, persyaratan, dan kekuatan hukumnya.

Aspek	Indonesia	Singapura
Cakupan Hukum	Mengatur informasi dan transaksi elektronik secara luas, termasuk tanda tangan elektronik, perlindungan data, dan kejahatan siber. Berlaku di Indonesia dan transaksi lintas batas yang memengaruhi kepentingan Indonesia.	Mengatur transaksi elektronik, termasuk tanda tangan elektronik kontrak elektronik, dan penyimpanan data, dengan fokus pada perdagangan domestik dan internasional.
Persyaratan Hukum	Harus terkait langsung dengan penandatangan, berada dalam kendali penandatangan, serta perubahan pada informasi dapat terdeteksi.	Mengidentifikasi penanda tangan Melalui sertifikat digital yang diterbitkan oleh otoritas sertifikasi yang diakui.
Kekuatan Hukum	Diakui sah secara hukum apabila memenuhi syarat dan ketentuan dalam UU ITE.	Memiliki kekuatan hukum setara dengan tanda tangan basah jika memenuhi syarat yang ditetapkan.

Aspek	Indonesia	Singapura
Status Hukum	Berlaku secara mengikat di Indonesia, dengan peraturan pelaksana seperti Peraturan Pemerintah dan Peraturan Otoritas Jasa Keuangan.	Berlaku secara mengikat di Singapura, dengan pengaturan yang diatur oleh otoritas sertifikasi yang sesuai ketentuan hukum setempat.
Fokus Perlindungan	Perlindungan konsumen, privasi, dan keamanan data dalam konteks nasional.	Perlindungan konsumen dan pelaku usaha dalam perdagangan elektronik domestik/internasional.

Tabel 4.1

Sumber: Diolah dari Undang-Undang ITE dan Electronic Transactions Act

B. Analisis Implikasi Faktor Faktor Yang Mempengaruhi adanya Perbandingan Terhadap Sistem Hukum di bidang Sertfikasi Elektronik antara Indonesia dan Singapura

Dalam penelitian ini, Perbandingan antara Indonesia dan Singapura dalam konteks hukum, khususnya terkait sertifikasi elektronik, transaksi elektronik, perlindungan data pribadi, atau penyelenggaraan tanda tangan digital mempunyai beberapa faktor strategis dan kontras yang signifikan.

Perbandingan antara Indonesia dan Singapura dalam 3 faktor; (1) standar internasional, (2) kelembagaan, (3) teknologi & infrastuktur. Sering dilakukan karena terdapat perbedaan yang signifikan namun relevan. Meskipun keduanya berada di kawasan yang sama, pendekatan dan kesiapan mereka terhadap transformasi digital berbeda, yang menjadikan keduanya objek perbandingan yang menarik dan strategis.

Dari sisi infrastruktur digital, Singapura memiliki keunggulan yang sangat menonjol. Negara ini sudah lama berinvestasi dalam infrastruktur teknologi informasi dan komunikasi yang canggih, seperti jaringan internet berkecepatan tinggi, cakupan 5G yang luas, serta pusat data yang aman dan terintegrasi dengan standar internasional. Infrastruktur tersebut mendukung terciptanya lingkungan digital yang stabil dan terpercaya, memungkinkan implementasi sistem identitas digital nasional seperti Singpass dan berbagai layanan publik berbasis elektronik yang efisien.

Sementara itu, Indonesia masih menghadapi tantangan besar dalam hal infrastruktur digital, terutama karena wilayah geografisnya yang luas dan kondisi topografi yang beragam. Meskipun pemerintah Indonesia telah menginisiasi berbagai

proyek strategis seperti Palapa Ring untuk memperkuat konektivitas nasional, ketimpangan akses antara daerah perkotaan dan pedesaan masih cukup tinggi. Hal ini berdampak langsung pada kemampuan Indonesia dalam menerapkan sistem elektronik secara merata di seluruh wilayah.

Dari sisi kelembagaan, Singapura menunjukkan koordinasi yang kuat antar lembaga dalam penerapan kebijakan digital. Lembaga seperti Infocomm Media Development Authority (IMDA) memiliki peran sentral dalam merancang regulasi dan memastikan pelaksanaan kebijakan digital berjalan efektif. Kelembagaan yang stabil dan efisien ini memungkinkan Singapura untuk mengadopsi model-model hukum internasional seperti UNCITRAL Model Law dengan cepat dan konsisten. Sebaliknya, di Indonesia, koordinasi kelembagaan dalam isu digital masih kerap menghadapi tantangan birokrasi dan tumpang tindih kewenangan. Misalnya, dalam isu perlindungan data pribadi, sebelumnya terdapat peran yang tumpang tindih antara beberapa kementerian dan lembaga, meskipun kini sudah mulai diarahkan pada pembentukan lembaga pengawas yang khusus setelah disahkannya UU Perlindungan Data Pribadi.

Dari perspektif standar nasional, Singapura telah memiliki kerangka regulasi yang matang dan mengacu pada praktik internasional. Standar yang digunakan, baik untuk keamanan siber, tanda tangan elektronik, maupun pengelolaan data, merujuk pada standar global yang memungkinkan interoperabilitas dan kepercayaan dari pelaku usaha internasional. Standar-standar ini juga diimplementasikan secara konsisten melalui instrumen hukum yang kuat dan kepatuhan yang tinggi dari sektor swasta. Indonesia sendiri sedang dalam tahap pengembangan dan harmonisasi standar nasional. Misalnya, penerapan tanda tangan elektronik dan sistem transaksi

elektronik diatur dalam berbagai peraturan yang masih dalam proses penyesuaian terhadap standar internasional. Kehadiran UU Nomor 1 Tahun 2024 tentang Sistem dan Transaksi Elektronik menunjukkan komitmen Indonesia untuk memperkuat standar hukum nasional di bidang ini. Namun, implementasinya membutuhkan kesiapan lebih lanjut baik dari segi teknologi, sumber daya manusia, maupun kepatuhan pelaku industri.

Dengan mempertimbangkan ketiga aspek tersebut—yakni infrastruktur, kelembagaan, dan standar nasional—perbandingan antara Indonesia dan Singapura menjadi penting. Singapura berfungsi sebagai model ideal yang dapat menjadi acuan bagi Indonesia dalam memperkuat regulasi dan praktik digital. Di sisi lain, Indonesia dapat mengadaptasi pengalaman Singapura dengan mempertimbangkan konteks sosial, ekonomi, dan geografisnya yang berbeda. Perbandingan ini tidak hanya bersifat akademis, tetapi juga praktis untuk perumusan kebijakan nasional yang lebih efektif dan berorientasi pada masa depan digital yang inklusif dan aman.

BAB V

PENUTUP

A. Kesimpulan

Berdasarkan perumusan masalah yang kemudian diuraikan dalam hasil penelitian dan analisa yang disajikan pada bab-bab maka penelitian ini dapat ditarik kesimpulan sebagai berikut:

1. Sertifikat elektronik memiliki kedudukan hukum yang kuat sebagai alat bukti yang sah (Pasal 5 UU ITE), sepanjang memenuhi syarat formil dan materil, seperti autentikasi identitas penandatangan dan keutuhan dokumen. Penyelenggara Sertifikasi Elektronik (PSrE) harus berbadan hukum Indonesia dan terdaftar di Kementerian Komunikasi dan Informatika (Kominfo). Singapura memiliki kerangka hukum untuk untuk sertifikasi elektronik, terutama melalui Electronic Transactions Act (ETA) yang selaras dengan standar internasional seperti UNCITRAL Model Law on Electronic Commerce. Sertifikat elektronik diakui sebagai alat bukti yang sah dengan prosedur penyerahan yang lebih terperinci di pengadilan. Sertifikasi elektronik di Indonesia dan Singapura memiliki kedudukan hukum yang kuat sebagai alat bukti elektronik, tetapi Singapura unggul dalam hal efisiensi, kejelasan prosedur, dan integrasi dengan standar internasional.

2. Faktor-faktor seperti infrastruktur teknologi, kerangka regulasi, kesadaran masyarakat, standar keamanan, dan konteks ekonomi menjadi penyebab utama perbedaan dalam penerapan sertifikasi elektronik antara kedua negara. Indonesia perlu memperkuat harmonisasi regulasi, meningkatkan infrastruktur

teknologi, dan edukasi masyarakat untuk mengejar efektivitas sistem sertifikasi elektronik seperti di Singapura**.**

Adapun, alasan penulis mengambil negara Singapura adalah karena Singapura ialah negara tetangga di kawasan Asia Tenggara, dan rekam jejaknya memiliki kemiripan seperti hal-nya Indonesi. Dahulu, negara Singapura merupakan negara berkembang bahkan lebih rumit dari Indonesia sejak awal kemerdekaan.

Namun, seiring berjalannya waktu, Singapura kian berkembang pesat dalam bidang ekonomi, pendidikan, infrastuktur, teknologi, dan lain-lain. Maka dari itu, adanya penulisan ini guna mempelajari sistem hukum dalam bidang teknologi yaitu Sertifikasi Elektronik yang ada di negara Singapura maupun Indonesia dengan metode komparasi.

Indonesia juga tidak tertinggal dari perkembangan teknologi, dengan adanya Startup Digital (TokoPedia, Shopee, Dll.) dan QRIS. juga termasuk nilai tambah tersendiri untuk Indonesia.

Penulis menyadari bahwa penulisan ini murni dibuat untuk kepentingan internal dan pengembangan pengetahuan, bahwa perbandingan Indonesia dan Singapura tidak bersifat *apple to apple* mengingat adanya perbedaan signifikan dalam hal luas wilayah, jumlah penduduk, serta kapasitas sumber daya masing-masing negara. Namun, perbandingan ini tetap relevan untuk memberikan perspektif yang lebih luas, khususnya dalam pendekatan kebijakan dan praktik yang diterapkan oleh negara masing-masing. Penulis sangat menyadari bahwa kedua negara memiliki karakteristik yang berbeda, oleh sebab itu, penulisan ini guna untuk memberikan wawasan komperatif yang dapat menjadi bahan refleksi dan pembelajaran kebijakan.

B. Saran

Adapun beberapa saran dari peneliti untuk pemerintah Indonesia agar lebih berkembang, yaitu sebagai berikut;

1. Meningkatkan kapasitas lembaga otoritas sertifikasi (CA) lokal melalui pembaruan teknologi dan pengawasan yang ketat;

2. Pemerintah Indonesia dapat mempercepat pembangunan infrastruktur teknologi informasi, terutama di daerah-daerah terpencil, untuk mengatasi kesenjangan digital. Program seperti Palapa Ring (proyek pembangunan infrastuktur untuk memperluas akses internet ke seluruh wilayah Indonesia, termasuk daerah-daerah terpencil) dapat dioptimalkan untuk mendukung keandalan sistem sertifikasi elektronik;

3. Mendorong adopsi sertifikasi elektronik di sektor publik dan swasta secara luas, melalui insentif, edukasi, dan integrasi sistem;

4. Membentuk ekosistem digital yang mendukung keamanan siber, agar kepercayaan publik terhadap TTD E meningkat;

5. Pemerintahan sebaiknya melalukan sosialisasi agar masyarakat dapat mengetahui lebih banyak tentang hal-hal berbau elektronik, di-karenakan masyarakat di pedalaman biasanya lebih awam mengenai digital.

DAFTAR PUSTAKA

Agustika, Fitriah, and others, 'Telaah Teknologi Informasi Dan Sistem Informasi Dalam Organisasi Dengan Lingkungan', *Jurnal Bisnis Kolega*, 9.1 (2023), doi:10.57249/jbk.v9i1.104

Agustina, Ditha Cindy, 'Fakultas Ekonomi Dan Bisnis Universitas Muhammadiyah', *Riset*, no. 02 (2020)

Ahadi, Lalu M. Alwin, 'Efektivitas Hukum Dalam Perspektif Filsafat Hukum: Relasi Urgensi Sosialisasi Terhadap Eksistensi Produk Hukum', *Jurnal Usm Law Review*, 5.1 (2022), p. 110, doi:10.26623/julr.v5i1.4965

Aini, Qurotul, Untung Rahardja, and Anggy Fatillah, 'Penerapan Qrcode Sebagai Media Pelayanan Untuk Absensi Pada Website Berbasis Php Native', *Sisfotenika*, 8.1 (2018), p. 47, doi:10.30700/jst.v8i1.151

Arkhan, Muhammad, and others, 'Jurnal Hukum Mimbar Justitia (JHMJ) Evaluasi Efektivitas Undang-Undang No . 1 Tahun 2024 Tentang Informasi Dan Transaksi Elektronik Dalam Pencegahan Cyberterrorism Evaluation of the Effectiveness of Law No . 1 of 2024 on Information and Electronic Trans', 5681.2 (2024),

Bambang Warsita, Bambang Warsita, 'Landasan Teori Dan Teknologi Informasi Dalam Pengembangan Teknologi Pembelajaran', *Jurnal Teknodik*, XV (2014), doi:10.32550/teknodik.v0i0.91

Bimantara, Azza, Rangga Tri Nugraha, and Universitas Muhammadiyah Malang, 'The Politics of International Cooperation in Cross-Border Digital Payment Connectivity: A Case Study of QR Payment System in ASEAN Azza Bimantara 1* , Rangga Tri Nugraha 2', 8090.246 (2025), doi:10.22219/jurnalsospol.v11i1.38367

Damayanti, Adelina, and Rina Arum Prastyanti, 'Kajian Hukum Dan Regulasi Terkait Serangan Hacking Pada Platform Digital Di Indonesia', *Multidisciplinary Indonesian Center Journal (MICJO)*, 1.2 (2024), doi:10.62567/micjo.v1i2.117

Dari, Ditinjau, and others, 'Pertanggungjawaban Pidana Terhadap Pelaku Hacking Hukum Dalam Tindak Pidana Cyber Crime Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik)', 4307.May (2025).

Dewisari, Wita, and Tasya Author, 'Analisis Keamanan Penyelenggara Sertifikasi Elektronik Indonesia : PT Privy Identitas Digital', 18218037 (2022)

Dopo, Gianluca Fredrick Wou, I Nyoman Putu Budiartha, and Ida Ayu Putu Widiati, 'Kebebasan Berpendapat Dalam Hubungannya Dengan Tindak Pidana Ujaran Kebencian (Studi Putusan Pengadilan Tinggi Denpasar Nomor 72/ Pid.Sus/2020/Pt.Dps)', *Jurnal Analogi Hukum*, 5.2 (2023),

Dr. Zainal Said, M.H., *Polemik Undang-Undang Perbankan Indonesia Tinjauan Sosio Yuridis)*, *Sustainability (Switzerland)*, 2019, XI <http://scioteca.caf.com/bitstream/handle/123456789/1091/RED2017-Eng-8ene.pdf?sequence=12&isAllowed=y%0Ahttp://dx.doi.org/10.1016/j.regsciurbeco.2008.06.005%0Ahttps://www.researchgate.net/publication/305320484_Sistem_Pembetungan_Terpusat_Strategi_Melestari>

Elektronik, Penyelenggaraan Sistem, and Pribadi D I Indonesia, 'Aktual Justice', 5.2,

Fadhal, Soraya, and Lestari Nurhajati, 'Identifikasi Identitas Kaum Muda Di Tengah Media Digital (Studi Aktivitas Kaum Muda Indonesia Di Youtube)', *Jurnal Al Azhar Indonesia Seri Pranata Sosial*, 1.3 (2012), <http://main.makeuseoflimited.netdna-cdn.com/>

Fahza Alfaizi, Faldin, Yesi Airohmah, and Bakti Fatwa Anbiya, 'Analisis Konsep, Teori Teknologi Informasi Dan Implikasinya Dalam Pengembangan Teknologi Pembelajaran PAI Di Indonesia: Sistematik Literatur Riview', *Jurnal Sosial Teknologi*, 3.11 (2023), doi:10.59188/jurnalsostech.v3i11.985

Fathurrahman, M A, and L Husna, 'Perbandingan Hukum Indonesia Dan India Terhadap Penyelesaian Sengketa Arbitrase Secara Online', *UNES Law Review*, 5.4 (2023), <https://review-unes.com/index.php/law/article/view/758>

Fayza, Yasmina, Muhamad Amirulloh, and Mustofa Haffas, 'BERDASARKAN Peraturan Perundang-Undangan Terkait Sales Of Covid-19 Vaccine Certificate By Facebook Users Based On Related Law Indonesia Menjamin Hak Komunikasi Warga Negara Melalui Pasal 28F Undang- Undang Dasar Negara Republik Indonesia Tahun 1945 Yang M', no. 42 (2022)

Guarddin, Gladhi, and Jundi Ahmad Alwan, 'Implementasi Sistem Registration Authority Dan Personal Security Environment Menggunakan Smart Card', *Techno.Com*, 20.4

(2021), pp. 623–35, doi:10.33633/tc.v20i4.5284

H. Syafa'at Anugrah, and Rustam Magun Pikahulan, 'Mulawarman LawReview', *Mulawarman Law Review*, 4.1 (2019),

Hasananuddin Hasan, 'Hierarki Peraturan Perundang-Undangan Negara Republik Indonesia Sebagai Suatu Sistem', *Madani Legal Review*, 1.2 (2017), doi:10.31850/malrev.v1i2.32

Hasim, Hasanuddin, 'Hubungan Hukum Internasional Dan Hukum Nasional Perspektif Teori Monisme Dan Teori Dualisme', *Mazahibuna Jurnal Perbandingan Mazhab*, 1.2 (2019),

Hidayah, Syarifaatul, 'Tantangan Dan Peluang Sertifikat Elektronik Dalam Reformasi Pendaftaran Tanah Di Era Digital .', 1.6 (2024),

Infocomm, 'Consultation Paper Issued by the Infocomm Media Development Authority on Embedded SIM Technology', *Consultation Paper*, no. June (2018), p. <https://www.imda.gov.sg/-/media/imda/files/inner/pcdg/consultations/consultation-paper/public-consultation-on-embedded-sim-technology/consultation-document-for-esim.pdf?la=en>

International, uncitral model law on internarional commercial arbitration, '06-54671_Ebook.Pdf'

'January 2019', *Journal of Business & Management (COES&RJ-JBM)*, 7.1 (2019), doi:10.25255/jbm.2019.7.1

Kusuma, Ersa, 'Kebebasan Berpendapat Dan Kaitannya Dengan Hak Asasi Manusia (HAM)', *Sanskara Hukum Dan HAM*, 1.03 (2023), doi:10.58812/shh.v1i03.63

Laia, Pesman, 'Analisis Perspektif Komparatif Regulasi Hukum Dagang Nasional Dengan Standar Internasional', *Jurnal Kajian Hukum Dan Kebijakan Publik*, 1.2 (2024), pp. 174–79

Law, T H E, and others, 'The Statutes of the Republic of Singapore - copyright act', 2008.March 2008 (2015)

Lee, Jack Tsen-Ta, 'The Past, Present and Future of the Internal Security Act', *ssrn Electronic Journal*, 2012, doi:10.2139/ssrn.2075475

Maharani, Dinda Shafira, and others, 'Peran Infrastruktur Teknologi Dalam Meningkatkan The Role Of Technology Infrastructure In Enhancing', 4.1 (2025),

Maharani, Rista, and Andria Luhur Prakoso, 'Perlindungan Data Pribadi Konsumen Oleh Penyelenggara Sistem Elektronik Dalam Transaksi Digital', *Jurnal Usm Law Review*,

7.1 (2024), p. 333, doi:10.26623/julr.v7i1.8705

Maisarah, Siti, 'Fungsi Sertifikasi Elektronik Bagi Pelaku Usaha Dalam Transaksi Perdagangan Elektronik', *Badamai Law Journal*, 4.1 (2019), doi:10.32801/damai.v4i1.9233

Makarim, Edmon, 'Kajian Hukum Terhadap Kemungkinan Cybernotarydi Indonesia'

Mason, Stephen, *Electronic Signatures in Law, 3rd Edition*, *Electronic Signatures in Law, 3rd Edition*, 2012, doi:10.1017/CBO9780511998058

Moha, Mohamad Rivaldi, and others, 'The Comparative Law Study: E-Commerce Regulation in Indonesia and Singapore', *Jurnal Legalitas*, 16.2 (2023), doi:10.33756/jelta.v16i2.20463

Musqith, Munadhil Abdul; Tayibnapis, Radita Gora, 'Jurnal Sosial Dan Budaya Syar-I', *Jurnal Sosial Dan Budaya Syar-I*, 9.4 (2022), doi:10.15408/sjsbs.v10i6.38412

Nafisah, Syifaun, 'Electronic Information and Transaction Law, a Means of Information Control in Libraries', *Jurnal Kajian Informasi & Perpustakaan*, 11.1 (2023), doi:10.24198/jkip.v11i1.35354

Ng, Dennis, 'Evolution of Digital Payments: Early Learnings from Singapore's Cashless Payment Drive', *Journal of Payments Strategy & Systems*, 11.4 (2018), doi:10.69554/qohg1171

Nurul, Shinta, Shynta Anggrainy, and Siska Aprelyani, 'Faktor-Faktor Yang Mempengaruhi Keamanan Sistem Informasi: Keamanan Informasi, Teknologi Informasi Dan Network (Literature Review Sim)', *Jurnal Ekonomi Manajemen Sistem Informasi*, 3.5 (2022), doi:10.31933/jemsi.v3i5.992

Ooi, Vincent, and Vincent Ooi, 'Institutional Knowledge at Singapore Management University Adapting Taxation for the Digital Economy in Singapore Singapore Adapting Taxation for the Digital Economy in Singapore', 2021,

Orlando, Galih, 'Efektivitas Hukum Dan Fungsi Hukum Di Indonesia', *Jurnal Pendidikan* AgamaDanSains,6(2022),
<https://www.ejurnal.stita.ac.id/index.php/TBQ/article/download/77/70>

'Part Ii Accreditation Of Certification Authorities 3', 2010

Pradana, H Syafa'at Anugrah, and Muhammad Andri Alvian, 'Kompabilitas Mekanisme Omnibus Law Dalam Pengaturan Perpajakan', *Jurnal Ilmu Hukum AMANNA GAPPA*,

21.1 (2021),

Pradana, Syafa'at Anugrah, and others, 'Regulation of Esports in the Context of the Employment in Indonesia', *Amsir Law Journal*, 4.1 (2022), doi:10.36746/alj.v4i1.98

Pradana, Syafa'at Anugrah, Sunandar, and EMi Asriati Makmur, 'Urgensi Kajian Fiqh Al-Bi'ah Dalam Pemenuhan Urusan Konkuren Bidang Pelayanan Kebersihan Di Kabupaten Luwu Timur', *Gorontalo Law Review*, 5.2 (2022),

Rahayu, Nathania Salsabila Marikar Ssahib., Soesi Idayanti. dan, Kanti, 'Problematika Aturan Penyelenggara Sistem Elektronik (PSE) Di Indonesia', *Pancasakti Law Journal*, 1.1 (2023), <https://fh.pps-upstegal.ac.id/index.php/plj/article/view/8%0Ahttps://fh.pps-upstegal.ac.id/index.php/plj/article/download/8/7>

Rezende, Pedro A D, 'The Possible Laws on Digital / Electronic Signature : On the Proposed uncitral Model Department of Computer Science Classification of Laws'

Richardo Sibarani, David, and others, 'Pertumbuhan Ekonomi Indonesia (The Impact of Information and Communications Technology Access Use and Expertise on Indonesia's Economic Growth)', *Jurnal Resolusi Konflik*, 8.2 (2023),

Safitri, Intan Dila, 'Dinamika Masyarakat Dalam Meningkatkan Efektivitas Penegakan Hukum', *Socius: Jurnal Penelitian Ilmu-Ilmu Sosial*, 1 (2024), <https://ojs.daarulhuda.or.id/index.php/Socius/article/view/145%0Ahttps://ojs.daarulhuda.or.id/index.php/Socius/article/download/145/145>

Said, Zainal, *Politik Hukum Perbankan Nasional*, 2019

Salsabillah, Anggini, and Yudi Kornelis, 'Melalui Media Sosial Menurut Undang Undang Nomor 1 Tahun 2024 Tentang Ite', 2024

Shanmugam, K., 'The Rule of Law in Singapore', *Singapore Journal of Legal Studies*, no. 12 (2012), doi:10.2139/ssrn.2255270

Signatures, Electronic, : ': تمدقلما', 6 (2025),

Suardi, Suardi, Fakhruddin Azmi, and Nurika Khalila Daulay, 'Perkembangan International Standard of Organization', *Jurnal Ilmiah Universitas Batanghari Jambi*, 23.3 (2023), p. 2625, doi:10.33087/jiubj.v23i3.3411

Suhairi, Juli Syahputri, and Fahmi Rizky, 'Strategi & Standarisasi Dalam Pemasaran Global', *Jurnal Masharif Al-Syariah: Jurnal Ekonomi Dan Perbankan Syariah*, 8.1 (2023), <http://journal.um-surabaya.ac.id/index.php/Mas/index>

Suprapto, Sari Tri, and Dona Budi Kharisma, 'Problematika Implementasi Standar Nasional Indonesia (Sni) Wajib Pada Mainan Anak Di Kota Jakarta Timur', *Jurnal Privat Law*, 8.2 (2020), doi:10.20961/privat.v8i2.48413

Syariah, Fakultas, and others, 'Kemelitan Penegakan Hukum Terhadap Hak Kebebasan Berpendapat Syafa ' at Anugrah Pradana Rusdianto Sudirman', *Jurnal Syariah Dan Hukum*, 20 (2022),

Tahir, Hardiyanti, Zainal Said, and Marhani, 'Strategi Marketing Funding Dalam Meningkatkan Jumlah Nasabah Di Bank Bni Syariah Parepare', *BANCO: Jurnal Manajemen Dan Perbankan Syariah*, 3.2 (2022) doi:10.35905/banco.v3i2.2156

Tangan, Tanda, and others, 'INTERNASIONAL', 5.1 (2022), doi:10.28946/slrev.Vol5.Iss1.603.pp71-85.2

Ummah, Masfi Sya'fiatul, 'Implementasi Model Interoperabilitas Pada Sistem Informasi Akademik Berbasis Multi Platform Muhammad Faisal Program Studi Teknik Komputer STMIK Profesional Makassar Muh.Faisal.Art@gmail.Com', *Sustainability (Switzerland)*, 11.1 (2019), <http://scioteca.caf.com/bitstream/handle/123456789/1091/RED2017-Eng-8ene.pdf?sequence=12&isAllowed=y%0Ahttp://dx.doi.org/10.1016/j.regsciurbeco.2008.06.005%0Ahttps://www.researchgate.net/publication/305320484_Sistem_Pembetungan_Terpusat_Strategi_Melestari>

Undang-undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, 'Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik', *Journal of Physics A: Mathematical and Theoretical*, 44.8 (2011),

United Nations, *uncitral Model Law on Electronic Signatures, United Nations Publication*, 2002 <http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2001Model_signatures.html>

Vania, Cindy, and others, 'Tinjauan Yuridis Terhadap Perlindungan Data Pribadi Dari Aspek Pengamanan Data Dan Keamanan Siber', *Jurnal Multidisiplin Indonesia*, 2.3 (2023), pp. 654–66, doi:10.58344/jmi.v2i3.157

Wibowo, Yulianto, and Ida Aryati Dpw, 'Tinjauan Yuridis Tentang Perlindungan Data Pribadi Masyarakat Pada Era Digitalisasi', 18.01 (2025)

Wiwin, H. Syafa'at Anugrah Pradana, and Muhammad Imam Dhiya'ul Haq, 'Regulation of Articles on State Institutional Insults to The Right to Freedom of Expression in Indonesia: A Critical Review', *Mulawarman Law Review* 2023, 2023, doi:10.30872/mulrev.v8i1.1122

Yusuf, Mohd., and others, 'Tinjauan Yuridis Faktor-Faktor Yang Mempengaruhi Efetivitas Penegakan Hukum Di Masyarakat', *JPin: Jurnal Pendidik Indonesia*, 5.2 (2022), <http://jurnal.intancendekia.org/index.php/JPIn/article/view/369>

Zahra, Nabilla, Recca Ayu Hapsari, and Melisa Safitri, 'Perlindungan Hukum Teknologi Identitas Digital Melalui Sistem Verifikasi Identitas Berbasis Biometrik', *Supremasi: Jurnal Pemikiran Dan Penelitian Ilmu-Ilmu Sosial, Hukum, & Pengajarannya*, XIX.1 (2024),

Peraturan Perundang-Undangan

Pasal 5, Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, '.

Pasal 13, Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik"

Pasal 13A, Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik"

Cap. 88 Section 8 T H E Law and others, 'The Statutes of the Republic of Singapore - COPYRIGHT ACT', 2008.March 2008 (2015).

UNCITRAL model law on Electronic Signatures, Article 5.

Cap. 88 Section 8 Law and others, 'The Statutes of the Republic of Singapore - COPYRIGHT ACT'.

Article 6, Uncitral Model Law On Electronic Signatures

LAMPIRAN-LAMPIRAN

THE STATUTES OF THE REPUBLIC OF SINGAPORE

ELECTRONIC TRANSACTIONS ACT

(CHAPTER 88)

(Original Enactment: Act 16 of 2010)

REVISED EDITION 2011

(31st December 2011)

Prepared and Published by

THE LAW REVISION COMMISSION
UNDER THE AUTHORITY OF
THE REVISED EDITION OF THE LAWS ACT (CHAPTER 275)

Informal Consolidation – version in force from 21/11/2021

BIODATA PENULIS

Penulis bernama lengkap Humaerah Hairunnisa, lahir di Pinrang, 02 Juli 2002, penulis merupakan anak pertama dari pasangan Abd. Asis dan Alrmh. Enceng Yang bertempat tinggal di Malimpung, kec. Patampanua, kab. Pinrang. Penulis memulai pendidikan di TK Yapis Manokwari Papua Barat (2006), SDN 41 Manokwari Papua Barat (2007), SMP AL Mazaakhirah Pinrang (2014), dan 1 Tahun menempuh pendidikan di Darul Aman Gombara Makassar (2017), kemudian pindah ke SMA Al Mazaakhirah (2018), setelah itu menempuh pendidikan di Institut Agama Islam Negeri Parepare (2021) sampe penulis menulis skripsi ini dan kemudian terdaftar sebagai mahasiswa Program Studi Hukum Tata Negara, Fakultas Syariah dan Ilmu Hukum Islam. Dengan ketekunan serta motivasi dan doa dari keluarga, bantuan dosen pembimbing akademik, bantuan dosen pembimbing, dan dose penguji, serta tiap tiap orang yang ikut membantu dalam proses penyelasaian. Alhamdulillah, puji syukur kepada Allah Subhanahu Wa Taa'ala penulis dapat menyelesaikan tugas akhir. Semoga skripsi yang berjudul "Analisis Komparasi Sistem Hukum Di Bidang Sertifikasi Elektronik Antara Indonesia dan Singapura" dapat memberikan manfaat.