Jurnal Pengabdian West Science
Vol. 03, No. 04, April, 2024, pp. 429 -442

Sosialisasi Perbandingan Hukum Pidana: Tindak Pidana ITE di Indonesia dan Singapura

Yuni Priskila Ginting[1], Anastasia C.G. Tumbelaka[2], Alunuah Yogeta[3], Bertylla Deva Octania Tjahaja[4], Bintang Fardiansyah Hambran[5], Maria Athena Gani[6], Natanael[7], Raja Farras Nasution[8], Zahwa Naila Firliyani[9], Victoria Kimberly[10]
[1,2,3,4,5,6,7,8,9,10] Universitas Pelita Harapan
**Corresponding author*
E-mail: yuni.ginting@uph.edu[1], 01051220169@student.uph.edu[2], 01051220191@student.uph.edu[3], 01051220145@student.uph.edu[4], 01051220203@student.uph.edu[5] , 01051220168@student.uph.edu[6] 01051220157@student.uph.edu[7], 01051220161@student.uph.edu[8], 01051220138@student.uph.edu[9], 01051220115@student.uph.edu[10]

Article History:
Received: April, 2024
Revised: April, 2024
Accepted: April, 2024

Abstract: *Penelitian ini bertujuan untuk mengetahui perbandingan, tantangan keamanan dan regulasi penggunaan teknologi. Studi ini bertujuan untuk memahami pendekatan legislatif kedua negara dalam menghadapi isu keamanan siber dan penyalahgunaan teknologi informasi. Melalui analisis komparatif, penelitian ini mengungkap bahwa Singapura mengambil pendekatan yang lebih spesifik terhadap perlindungan infrastruktur kritikal dan keamanan nasional, sementara Indonesia mengadopsi pendekatan yang lebih luas yang mencakup berbagai aspek penggunaan teknologi informasi, dari transaksi elektronik hingga perlindungan privasi online. Hasil analisis menunjukkan perbedaan dalam prioritas keamanan dan fokus regulasi yang mencerminkan kebutuhan dan tantangan lokal. Penelitian ini memberi wawasan penting bagi pembuat kebijakan, industri, dan akademisi tentang pentingnya kerangka hukum adaptif dan responsif terhadap dinamika keamanan siber dan teknologi informasi di kawasan.*

Keywords:
Keamanan Siber, Regulasi Teknologi Informasi, Kerangka Hukum, Singapura, Indonesia, Analisis Perbandingan

Pendahuluan

Era digital telah membawa kemajuan pesat dalam teknologi informasi dan komunikasi, yang secara signifikan mempengaruhi berbagai aspek kehidupan sosial, ekonomi, dan politik masyarakat global.[1] Kemudahan akses dan pertukaran informasi

1 Kemajuan teknologi informasi dan komunikasi telah membentuk ciri khas era digital dengan dampak yang luas terhadap kehidupan manusia, baik secara individu maupun kolektif.

yang ditawarkan oleh internet dan teknologi digital telah menumbuhkan inovasi dan kolaborasi tanpa batas, namun juga memunculkan tantangan baru dalam bentuk ancaman siber dan penyalahgunaan teknologi informasi. Tantangan ini mencakup, namun tidak terbatas pada, serangan siber terhadap infrastruktur kritikal, penyebaran konten ilegal dan berbahaya, pelanggaran privasi, dan kejahatan siber lainnya. Dalam upaya mengatasi tantangan tersebut, negara-negara di seluruh dunia telah mengembangkan dan menerapkan kerangka hukum yang dirancang untuk melindungi masyarakat dan infrastruktur mereka dari dampak negatif teknologi informasi, sekaligus memastikan penggunaan teknologi yang aman, etis, dan bertanggung jawab. Baik Indonesia maupun Singapura telah mengakui pentingnya mengatasi tantangan hukum yang timbul dari perkembangan teknologi informasi dan komunikasi. Kedua negara telah mengembangkan lex specialis, atau peraturan khusus, untuk mengatur aspek-aspek tertentu dari teknologi, memastikan bahwa kebutuhan keamanan, privasi, dan keadilan terpenuhi dalam lingkungan digital yang semakin kompleks.[2]

Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) Indonesia[3]

Di Indonesia, Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) No. 19 Tahun 2016 merupakan peraturan kunci yang mengatur penggunaan dan penyalahgunaan teknologi informasi dan elektronik (Mahfi, 2020). UU ITE mendefinisikan kerangka kerja hukum untuk transaksi elektronik, penyebaran informasi digital, dan aspek-aspek lain dari interaksi sosial dalam ruang siber. Tujuan UU ITE untuk menciptakan lingkungan digital yang aman dengan memberikan perlindungan terhadap hak-hak individu dan entitas, sambil juga menetapkan sanksi bagi pelanggaran terhadap ketentuan-ketentuan tersebut (Sidik, 2013). UU ITE undang-undang yang cukup luas yang dirancang untuk mengatur penggunaan teknologi informasi di Indonesia. Fokusnya mencakup berbagai aspek, mulai dari transaksi elektronik, penyebaran konten di internet, hingga perlindungan data pribadi. Meskipun UU ITE mencakup berbagai aspek teknologi informasi, pendekatannya lebih umum, menyediakan kerangka kerja yang luas untuk pengaturan aktivitas digital di Indonesia.

2 Lex specialis adalah peraturan hukum yang mengatur aspek-aspek tertentu dari suatu bidang hukum yang lebih luas, dan sering kali digunakan untuk menangani isu-isu yang kompleks dan berkembang pesat seperti teknologi informasi dan komunikasi. [3] UU No. 19 Tahun 2016

***CyberLaw* Singapura**

Singapura merespons tantangan keamanan siber sejak awal dengan mengesahkan undang-undang khusus, seperti Computer Misuse Act 1993[3]. Undang-undang tersebut menegaskan komitmen Singapura dalam membangun kerangka hukum untuk melawan kejahatan siber, seperti akses tidak sah dan penyebaran malware (Marita, 2015). Pengesahan undang-undang ini mencerminkan pengakuan terhadap risiko teknologi informasi dan internet sejak dini. Seiring dengan perkembangan teknologi, Singapura memperkuat kerangka hukumnya dengan pengesahan Cybersecurity Act 2018. Undang-undang ini memperluas perlindungan terhadap infrastruktur informasi kritikal dan meningkatkan kerja sama antar sektor dalam menghadapi ancaman siber. Langkah-langkah ini menetapkan Singapura sebagai negara terdepan dalam kebijakan dan praktik keamanan siber global, serta memungkinkannya untuk tetap responsif terhadap tantangan yang terus berkembang di dunia digital (Dutta et al., 2022). Singapura telah mengembangkan undang-undang yang lebih spesifik untuk mengatur berbagai aspek teknologi informasi, mencerminkan pendekatan yang lebih tersegmentasi dalam menghadapi tantangan keamanan siber dan privasi data. Pendekatan ini memungkinkan Singapura untuk menangani masalah spesifik dalam keamanan siber dan privasi data dengan lebih terfokus, memberikan perlindungan yang lebih kuat dan terperinci untuk individu dan entitas bisnis.

Dari perspektif sosiologis, pengembangan dan penerapan UU ITE dan *Cyber Law* Singapura mencerminkan respons masyarakat terhadap perubahan dan tantangan yang dibawa oleh revolusi digital. Kedua undang-undang ini mengakui pentingnya teknologi informasi dalam kehidupan sehari-hari sambil juga menggarisbawahi kebutuhan untuk membatasi risiko dan dampak negatif yang dapat muncul dari penyalahgunaan teknologi. Dengan demikian, UU ITE dan *Cyber Law* tidak hanya berfungsi sebagai alat pengaturan hukum tetapi juga sebagai cerminan dari dinamika sosial, ekonomi, dan politik yang lebih luas dalam era digital.

Metode

Metode yang digunakan dalam penelitian ini adalah pendekatan hukum normatif, yaitu melalui literatur atau data sekunder. Sumber hukum yang didapat berasal dari hasil penelitian dan karya para ahli hukum, yaitu sebagai bahan-bahan

3 Computer Misuse Act 1993

yang menggambarkan dan menafsirkan sumber hukum primer dan sekunder menjadi sumber hukum tersier. Sehingga dapat diambil kesimpulan teknik analisis deduksi silogisme dalam penelitian hukum ini adalah menganalisis ketentuan dan peraturan perundang-undangan mengenai tindak pidana ITE di Indonesia dan Inggris.

Hasil

A. Definisi

1) Singapura:

   a) Computer Misuse Act 1993: Fokus pada kejahatan siber, melarang akses tidak sah ke sistem komputer, penyebaran virus, dan aktivitas ilegal lainnya yang berkaitan dengan komputer.
   b) Cybersecurity Act 2018: Mengatur tentang keamanan siber nasional, terutama perlindungan infrastruktur informasi kritikal terhadap ancaman siber.
   c) Personal Data Protection Act 2012 (PDPA): Mengatur tentang pengumpulan, penggunaan, dan pemberian data pribadi oleh organisasi, serta memberikan individu hak atas data pribadi mereka.
   d) Electronic Transaction Act (ETA): ETA Singapura dirancang untuk memberikan kejelasan hukum bagi transaksi elektronik dan untuk memfasilitasi perdagangan elektronik. Ini termasuk pengakuan sah terhadap tanda tangan elektronik dan catatan.

2) Indonesia:

   a) UU ITE mendefinisikan berbagai istilah terkait teknologi informasi, termasuk informasi elektronik, transaksi elektronik, dan dokumen elektronik, dengan fokus pada transaksi dan komunikasi dalam ruang digital.

B. Subjek dan Objek

1) Singapura: Subjek utama adalah "critical information infrastructure", sedangkan objek meliputi perlindungan dari ancaman cyber.
2) Indonesia: Subjek meliputi individu dan entitas yang terlibat dalam penyelenggaraan sistem elektronik, sedangkan objeknya mencakup informasi elektronik dan dokumen elektronik.

C. Tujuan Teoritis dan Praktis

1) Singapura: Bertujuan untuk melindungi infrastruktur informasi kritik dari ancaman cyber, memastikan keamanan nasional, dan menjaga kesejahteraan ekonomi.
2) Indonesia: Bertujuan untuk mengatur transaksi elektronik, meningkatkan keamanan dan kepercayaan digital, serta melindungi hak-hak pribadi dan publik dalam ruang digital.

D. Dasar Hukum

1) Singapura: Cybersecurity Act 2018, Computer Misuse Act 1993, 2) Indonesia: UU ITE No. 19 Tahun 2016.

E. Jurisdiksi

1) Singapura: Cyber Security Agency (CSA).
2) Indonesia: Kementerian Komunikasi dan Informatika, dengan penegakan hukum oleh kepolisian dan kejaksaan.

F. Spesifikasi Tindak Pidana

1) Singapura: Termasuk tindakan tidak sah terhadap infrastruktur informasi kritik. Berfokus pada tindakan yang mengancam cybersecurity.
2) Indonesia: Tindakan tidak sah mencakup penyebaran konten ilegal, pencemaran nama baik, dan penipuan elektronik. UU ITE Indonesia lebih luas, mencakup tindakan yang merugikan pengguna internet, penyebaran konten ilegal, dan pelanggaran privasi.

G. Jenis Tindak Pidana

Indonesia

Pasal 27	Larangan mendistribusikan, mentransmisikan, membuat dapat diaksesnya informasi elektronik dan/atau dokumen elektronik, Bermuatan: Asusila (ayat (1)); Perjudian (ayat (2)); Pencemaran nama baik (ayat (3)); Pemerasan dan/atau pengancaman (ayat (4)).
Pasal 28	Berita Bohong: Kepada konsumen (ayat (1)); Terkait suku, agama, ras, dan antargolongan (SARA) (ayat (2)).
Pasal 29	Ancaman kekerasan atau menakut-nakuti
Pasal 30	Mengakses sistem elektronik milik orang lain: Dengan cara apapun (ayat (1)); Mengakses dan mengambil (ayat (2)); Menerobos (ayat (3)).

Pasal 31	Melakukan intersepsi atau penyadapan: Sistem elektronik milik orang lain (ayat (1)); Dari publik ke privat dan/atau sebaliknya (termasuk mengubah dan/atau tidak mengubah) (ayat (2)).
Pasal 32	Larangan perubahan informasi elektronik dan/atau dokumen elektronik: Pengubahan, pengrusakkan, memindahkan, menyembunyikan (ayat (1)); Memindahkan ke tempat yang tidak berhak (ayat (2)); Membuka dokumen atau informasi rahasia (ayat (3)).
Pasal 33	Mengganggu sistem elektronik
Pasal 34	Larangan menyediakan atau memfasilitasi: a. Perangkat keras atau perangkat lunak untuk memfasilitasi pelanggaran pasal 27 sampai dengan pasal 33 b. Sandi lewat komputer, kode akses atau sejenisnya untuk memfasilitasi pelanggaran pasal 27 sampai dengan pasal 33.
Pasal 35	Pemalsuan dokumen elektronik dengan cara: manipulasi, penciptaan, perubahan, penghilangan, pengrusakan.

Singapura

Cybersecurity Act

Pasal 7-16	Infrastruktur Informasi kritikal. Kewajiban untuk melaporkan insiden keamanan siber, melakukan audit dan penilaian, serta terlibat dalam latihan
Pasal 19-23	Tanggapan terhadap Ancaman dan Insiden Keamanan Siber:
Pasal 24-35	Penyedia Layanan Keamanan Siber: Larangan dan persyaratan untuk lisensi bagi penyedia layanan keamanan siber
Pasal 36-41	Pelanggaran Umum: Pelanggaran oleh perusahaan, asosiasi, atau kemitraan, bersama dengan penyalahgunaan kekuasaan dan masuk tanpa izin
Pasal 31-35	Denda Keuangan dan Banding: Pasal 31 hingga 35 untuk denda keuangan dan Pasal 35 untuk banding ke Menteri.

Computer Misuse Act 1993

Pasal 3 (1) Hacking, Phishing, Melakukan pengujian penetrasi tanpa diminta	Siapa pun yang dengan sengaja menyebabkan komputer melakukan fungsi apa pun untuk tujuan mengamankan akses tanpa otoritas, ke program atau data apa pun yang disimpan dalam komputer mana pun, akan bersalah melakukan tindak pidana. Pada penghukuman pertama, pelaku dapat dikenai denda hingga $5.000; penjara untuk jangka waktu hingga dua tahun; atau keduanya.
Pasal 7 (1) Denial Of Service (DOS ATTACK)	Setiap orang yang, dengan sengaja dan tanpa otoritas atau alasan yang sah: (a) mengganggu, atau menghentikan atau menghalangi penggunaan yang sah dari, sebuah komputer; atau (b) menghambat atau mencegah akses ke, atau merusak kegunaan atau efektivitas dari, program atau data yang disimpan dalam komputer (Denial of Service/ DOS A ack)
Pasal 5 Penyisipan malware	Pelanggaran bagi siapapun yang melakukan tindakan yang dia tahu akan menyebabkan modifikasi yang tidak sah terhadap isi dari komputer mana pun. (malware, ransomware, spyware, worm, trojan, dan virus) ke dalam sistem TI
Pasal 4 Pencurian identitas atau penipuan identitas	Merupakan suatu pelanggaran bagi seseorang untuk menyebabkan komputer melakukan fungsi apapun dengan tujuan memperoleh akses ke program atau data yang disimpan dalam komputer tersebut, dengan maksud untuk melakukan sejumlah pelanggaran, termasuk beberapa pelanggaran yang melibatkan penipuan atau ketidakjujuran.

H. Sistem Pemeriksaan, Tata Cara Penangkapan, dan Penanganan

1) Singapura

Diatur dalam Criminal Procedure Code 2010.

a) Penyelidikan Awal: Ketika suatu kejahatan dilaporkan atau dideteksi, polisi akan memulai penyelidikan. Ini bisa termasuk pengumpulan bukti, interogasi saksi, dan, jika perlu, penahanan tersangka.
b) Penangkapan: Tersangka dapat ditangkap jika ada alasan yang cukup untuk meyakini bahwa mereka telah terlibat dalam kejahatan. Penangkapan dilakukan berdasarkan waran atau, dalam kasus tertentu, tanpa waran jika situasinya mendesak atau jika individu tersebut tertangkap tangan.
c) Pengajuan Ke Pengadilan: Setelah penyelidikan, jika cukup bukti

ditemukan, kasus akan diajukan ke pengadilan. Tersangka akan dihadapkan ke pengadilan, dan dakwaan akan dibacakan.

d) Pleidoi: Tersangka diminta untuk memberikan pleidoi (bersalah atau tidak bersalah). Jika tersangka mengaku bersalah, pengadilan akan melanjutkan ke tahap penentuan hukuman. Jika tersangka mengaku tidak bersalah, pengadilan akan menetapkan tanggal untuk persidangan.
e) Persidangan: Selama persidangan, jaksa penuntut dan pembela tersangka akan mempresentasikan bukti dan argumen mereka di hadapan hakim (dan kadang-kadang juri, tergantung pada jenis kasusnya). Setelah mendengar semua bukti, hakim (atau juri) akan membuat keputusan mengenai kebersalahan tersangka.
f) Penentuan Hukuman: Jika tersangka dinyatakan bersalah, pengadilan akan melanjutkan ke fase penentuan hukuman, di mana hukuman yang sesuai akan ditetapkan berdasarkan keparahan kejahatan dan faktor lain yang relevan.
g) Banding: Tersangka memiliki hak untuk mengajukan banding terhadap keputusan atau hukuman ke pengadilan yang lebih tinggi.

2) Indonesia

Tata cara penangkapan terhadap pelaku tindak pidana diatur dalam Pasal 17 KUHAP harus dilakukan atas bukti permulaan yang cukup, yaitu:

a) Penangkapan dilakukan oleh penyidik atau penyidik pembantu dengan surat perintah penangkapan yang mencantumkan identitas tersangka dan alasan penangkapan serta pasal yang diduga dilanggar;
b) Penyidik atau penyidik pembantu harus menunjukkan surat perintah penangkapan kepada tersangka dan memberikan salinannya kepada tersangka atau keluarganya;
c) Penyidik atau penyidik pembantu harus segera memberitahukan alasan penangkapan secara jelas dan benar kepada tersangka;
d) Penyidik atau penyidik pembantu harus segera mengirimkan berita acara penangkapan kepada penuntut umum melalui kepala kepolisian;
e) Penyidik atau penyidik pembantu harus segera memeriksa tersangka dan membuat berita acara pemeriksaan;
f) Penyidik atau penyidik pembantu harus segera menyerahkan tersangka beserta barang bukti dan berkas perkara kepada penuntut umum paling lama dalam waktu 20 hari sejak tanggal penangkapan

I. Sanksi

1) Singapura:

a) Akses Tidak Sah ke Komputer: Hukuman maksimum penjara 2 tahun, denda, atau keduanya, untuk akses tidak sah tanpa motif kejahatan tambahan.
b) Akses dengan Tujuan Menipu atau Melakukan Kejahatan: Jika akses tidak sah tersebut dilakukan dengan tujuan untuk melakukan atau memfasilitasi komisi kejahatan lain, hukumannya bisa meningkat menjadi maksimum 10 tahun penjara dan denda.
c) Penggunaan Komputer untuk Mencuri atau Menipu: Tindakan menggunakan komputer untuk melakukan pencurian atau penipuan dapat dihukum dengan penjara maksimum 10 tahun, denda, atau keduanya.
d) Penggunaan Komputer untuk Menyebarkan Materi yang Tidak Pantas atau Ilegal: Mereka yang menggunakan komputer untuk menyebarkan materi pornografi atau terlarang lainnya bisa menghadapi hukuman penjara dan denda, dengan keparahan hukuman tergantung pada materi yang disebarkan.
e) Pembuatan atau Penyebaran Malware: Individu yang terlibat dalam pembuatan atau penyebaran virus komputer, malware, atau perangkat lunak jahat lainnya bisa dihukum dengan penjara dan/atau denda, tergantung pada dampak dari tindakan mereka.
f) Serangan Cyber terhadap Infrastruktur Kritikal: Serangan terhadap infrastruktur kritikal, yang dapat membahayakan keamanan nasional atau keselamatan publik, dianggap sebagai pelanggaran yang sangat serius dan dapat mengakibatkan hukuman penjara yang panjang dan denda besar.

2) Indonesia:

a) Menyebarkan Video Asusila (Pasal 27 ayat 1) : Orang yang dengan sengaja dan tanpa hak menyebarkan video atau informasi yang melanggar kesusilaan dapat dikenai sanksi pidana penjara paling lama 6 tahun dan/atau denda paling banyak Rp1.000.000.000,00.
b) Judi Online (Pasal 27 ayat 2): Melakukan perjudian online dapat mengakibatkan sanksi pidana penjara paling lama 6 tahun dan/atau denda paling banyak Rp1.000.000.000,00.
c) Pencemaran Nama Baik (Pasal 27 ayat 3): Pencemaran nama baik dapat

berujung pada pidana penjara paling lama 4 tahun dan/atau denda paling banyak Rp750.000.000,00.

d) Pemerasan dan Pengancaman (Pasal 27 ayat 4): Pelaku pemerasan dan pengancaman dengan menggunakan media elektronik dapat dikenai pidana penjara paling lama 6 tahun dan/atau denda paling banyak Rp1.000.000.000,00.
e) Berita Bohong (Pasal 28 ayat 1): Menyebarkan berita bohong yang merugikan konsumen dapat mengakibatkan pidana penjara paling lama 6 tahun dan/atau denda paling banyak Rp1.000.000.000,00.
f) Ujaran Kebencian (Pasal 28 ayat 2): Menyebarluaskan informasi dengan tujuan menimbulkan rasa kebencian berdasarkan SARA dapat dikenai pidana penjara paling lama 6 tahun dan/atau denda paling banyak Rp1.000.000.000,00.
g) Teror Online (Pasal 29): Mengirimkan ancaman kekerasan atau menakut-nakuti melalui media elektronik dapat berujung pada pidana penjara paling lama 4 tahun dan/atau denda paling banyak Rp750.000.000,00.

J. Pembelaan

1) Singapura:

a) Pleidoi Tidak Bersalah dan Pembuktian: Terdakwa memiliki hak untuk mengaku tidak bersalah terhadap tuduhan yang diajukan, yang memicu proses persidangan di mana jaksa penuntut harus membuktikan kesalahan terdakwa "di luar keraguan yang wajar".
b) Pembelaan di Pengadilan: Selama persidangan, terdakwa (melalui pengacara pembelanya) berhak untuk menyajikan bukti dan argumen pembelaan. Ini bisa termasuk menyebutkan saksi, menyajikan bukti fisik, dan memberikan alibi.
c) Pembelaan Spesifik: Terdakwa bisa menggunakan pembelaan spesifik tergantung pada sifat kejahatan, seperti pembelaan diri dalam kasus kekerasan atau kegilaan pada saat melakukan tindak pidana. Pembelaan semacam itu memerlukan bukti dan argumentasi yang mendukung.
d) Prosedur Praperadilan: Hak untuk Tidak Memberatkan Diri Sendiri: Terdakwa memiliki hak untuk tidak memberatkan diri sendiri, yang berarti mereka tidak diwajibkan untuk memberikan kesaksian atau bukti yang bisa menginkriminasikan diri sendiri.
e) Ajuan Banding: Jika terdakwa dinyatakan bersalah, mereka memiliki hak untuk mengajukan banding terhadap keputusan atau hukuman ke

pengadilan yang lebih tinggi. Proses banding bisa mencakup argumen baru mengenai pembelaan atau penilaian ulang bukti yang ada.

f) Pleidoi Tidak Bersalah dan Pembuktian: Terdakwa memiliki hak untuk mengaku tidak bersalah terhadap tuduhan yang diajukan, yang memicu proses persidangan di mana jaksa penuntut harus membuktikan kesalahan terdakwa "di luar keraguan yang wajar".
g) Pembelaan di Pengadilan: Selama persidangan, terdakwa (melalui pengacara pembelanya) berhak untuk menyajikan bukti dan argumen pembelaan. Ini bisa termasuk menyebutkan saksi, menyajikan bukti fisik, dan memberikan alibi.
h) Pembelaan Spesifik: Terdakwa bisa menggunakan pembelaan spesifik tergantung pada sifat kejahatan, seperti pembelaan diri dalam kasus kekerasan atau kegilaan pada saat melakukan tindak pidana. Pembelaan semacam itu memerlukan bukti dan argumentasi yang mendukung.
i) Prosedur Praperadilan: CPC juga mengatur prosedur praperadilan yang bisa memberi kesempatan kepada terdakwa untuk menantang legalitas penangkapan atau perlakuan sebelum sidang dimulai, yang bisa mempengaruhi jalannya persidangan.
j) Hak untuk Tidak Memberatkan Diri Sendiri: Terdakwa memiliki hak untuk tidak memberatkan diri sendiri, yang berarti mereka tidak diwajibkan untuk memberikan kesaksian atau bukti yang bisa menginkriminasikan diri sendiri.
k) Ajuan Banding: Jika terdakwa dinyatakan bersalah, mereka memiliki hak untuk mengajukan banding terhadap keputusan atau hukuman ke pengadilan yang lebih tinggi. Proses banding bisa mencakup argumen baru mengenai pembelaan atau penilaian ulang bukti yang ada.

Tidak ada perundangan spesifik untuk pembelaan UU ITE.

2) Indonesia:

Pembelaan dalam KUHAP:

Dalam pembelaan hukum, tersangka atau terdakwa dapat mengajukan alasan-alasan pembelaan yang dapat menghapus, mengurangi atau memperberat pertanggungjawaban pidananya. Alasan-alasan pembelaan tersebut dapat berupa:

a) Alasan pembenar *(justification)*, yaitu alasan yang menyatakan bahwa perbuatan yang dilakukan oleh tersangka atau terdakwa tidak melanggar hukum, misalnya karena dilakukan dalam keadaan darurat, membela diri,

menurut perintah yang sah, dan sebagainya. (Pasal 48 KUHAP);

b) Alasan pemaaf *(excuse)*, yaitu alasan yang menyatakan bahwa tersangka atau terdakwa tidak dapat dipertanggungjawabkan secara pidana karena tidak memiliki kesalahan, misalnya karena tidak sadar, tidak berdaya, tidak berakal sehat, dipaksa, dan sebagainya. (pasal 49 KUHAP);

c) Alasan-alasan pembelaan tersebut harus didasarkan pada fakta-fakta hukum yang dapat dibuktikan secara sah dan meyakinkan di pengadilan. Pembuktian tersebut dapat dilakukan dengan menggunakan alat bukti yang diatur dalam KUHAP, yaitu Keterangan saksi, Keterangan ahli, Surat, Petunjuk, Keterangan terdakwa.

Dalam hal tersangka atau terdakwa dinyatakan bersalah oleh pengadilan atas tindak pidana pemalsuan, maka ia dapat mengajukan upaya hukum sesuai dengan ketentuan dalam KUHAP (Banding, Kasasi dan PK). Sehingga pembelaan disini adalah pembelaan secara umum bukan pembelaan secara khusus di ITE

K. Contoh Kasus

1) Singapura

Dalam kasus Jaksa Penuntut Umum v Muhammad Nuzaihan bin Kamal Luddin [1999] 3 SLR(R) 653, terdakwa ditemukan telah, di antara lain, mengeksploitasi beberapa kerentanan untuk meretas beberapa server korban, guna mendapatkan akses tidak sah ke file komputer yang terdapat pada server korban. Terdakwa dijatuhi hukuman penjara selama dua bulan atas dakwaan di bawah pasal 3(1) dari CMA.[4]

2) Indonesia

Seorang pemuda asal Depok, Jawa Barat, bernama Ahmad Addril Hidayah (22) diringkus polisi usai ketahuan meretas sistem pembayaran isi ulang (top up) kartu multi trip (KMT) kereta rel listrik (KRL). Hanya bermodal handphone dan sejumlah aplikasi, pelaku berhasil memperoleh saldo hingga 12 juta dalam 3 hari. Atas perbuatannya, pelaku dijerat dengan Pasal 33 juncto Pasal 49 dan/atau Pasal 30 juncto Pasal 46 Undang-Undang (UU) Nomor 1 Tahun 2024 tentang Perubahan atas UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE). Pemuda itu pun terancam hukuman 6 tahun sampai maksimal 10 tahun penjara.[6]

4 The Singapore Law Gazzette

Diskusi

Gambar 1. Dokumentasi Pemaparan Materi

Kesimpulan

Perbandingan antara Indonesia dan Singapura dalam hal peraturan teknologi menunjukkan perbedaan dalam pendekatan legislatif kedua negara terhadap tantangan yang ditimbulkan oleh era digital. Indonesia, dengan UU ITE-nya, memberikan kerangka hukum yang lebih umum dan luas yang mencakup berbagai aspek teknologi informasi. Sementara itu, Singapura memilih untuk mengadopsi serangkaian undang-undang spesifik yang menargetkan kejahatan siber, keamanan siber, dan perlindungan data pribadi secara terpisah, mencerminkan pendekatan yang lebih tersegmentasi dan terfokus. Pendekatan Singapura memberikan kejelasan dan perlindungan yang lebih spesifik terhadap tantangan tertentu, sementara pendekatan Indonesia memberikan fleksibilitas yang lebih besar dalam penerapan dan interpretasi hukum.

Pengakuan/Acknowledgements

Tim penulis mengucapkan terima kasih kepada Ibu Yuni Priskila Ginting selaku dosen pengampu mata kuliah Perbandingan Hukum Pidana yang telah memberikan kesempatan untuk kami memaparkan materi “Tindak Pidana ITE di Indonesia dan Singapura”.

Daftar Referensi

Dutta, N., Jadav, N., Tanwar, S., Sarma, H. K. D., Pricop, E., Dutta, N., Jadav, N., Tanwar, S., Sarma, H. K. D., & Pricop, E. (2022). Importance of Cyberlaw. *Cyber Security: Issues and Current Trends*, 159–174.

Harahap, I. R., & Maharani, D. (2020, July). Penerapan dan Pandangan Keagamaan Terhadap Undang-Undang ITE di Indonesia. In Journal of Social Responsibility Projects by Higher Education Forum (Vol. 1, No. 1, pp. 28-31).

Lessig, L. (1999). The Law of the Horse: What Cyberlaw Might Teach. Harvard Law Review, 113(2), 501-549.

Mahfi, M. R. R. (2020). Undang-Undang Informasi Dan Transaksi Elektronik (UU ITE) Dalam Perspektif Hukum Pidana Administrasi (Administrasi Penal Law). *Badamai Law Journal*, *5*(1), 140–149.

Marita, L. S. (2015). Cyber Crime Dan Penerapan Cyber Law Dalam Pemberantasan Cyber Law Di Indonesia. *Cakrawala-Jurnal Humaniora*, *15*(2).

Sidik, S. (2013). Dampak undang-undang informasi dan transaksi elektronik (UU ITE) terhadap perubahan hukum dan sosial dalam masyarakat. *Jurnal Ilmiah Widya*, *1*(1), 1–7.