KERTAS KEBIJAKAN

Regulasi Siber dan Demokrasi Digital: Menilai Ulang Pasal 32 UU ITE

Lembaga Kajian & Advokasi Independensi Peradilan
LeIP
LBH PERS
SAFEnet

Kertas Kebijakan

Regulasi Siber dan Demokrasi Digital: Menilai Ulang Pasal 32 UU ITE

Lembaga Kajian dan Advokasi Independensi Peradilan (LeIP)
Lembaga Bantuan Hukum Pers (LBH Pers)
Southeast Asia Freedom of Expression Network (SAFEnet)

Tim Penulis:
Johanna G. S. D. Poerba
Mentari A. Ramadhianty
Raynov Tumorang Pamintori
Chikita Edrini Marpaung
Mustafa Layong
Gema Gita Persada
Balqis Zakiyyah

Penelaah Sejawat:
Alia Yofira Karunian

Desain Sampul dan Tata Letak:
Ach. Ridlo Ilwafa

Daftar Tabel

Daftar Gambar

Glosarium

Data Interference	Perbuatan yang tanpa hak dan sengaja mengganggu integritas data komputer dengan merusak, menghapus, menurunkan kualitas, mengubah, atau menghapus data komputer.
Dekriminalisasi	Proses menghapus status tindak pidana dari suatu perbuatan melalui perubahan peraturan perundang-undangan sehingga perbuatan tersebut tidak lagi dikenai sanksi pidana.
Efek menakutkan/ *Chilling effect*	Konsep untuk menjelaskan kekhawatiran masyarakat yang bersumber dari ambiguitas norma hukum.
Illegal access	Perbuatan mengakses sistem elektronik, jaringan, atau data tanpa hak atau tanpa izin yang sah dari pemilik atau pengelola sistem, termasuk dengan melampaui batas kewenangan yang diberikan.
Komentar Umum/ *General Comment*	Dokumen yang disusun oleh pakar independen PBB sebagai pedoman terperinci bagi negara dalam melaksanakan suatu hak.
Kriminalisasi	Proses menjadikan suatu perbuatan atau keadaan tertentu sebagai tindak pidana melalui peraturan perundang-undangan sehingga dapat dikenai sanksi pidana. Istilah ini juga secara populer digunakan untuk menggambarkan penggunaan hukum pidana secara tidak proporsional atau represif terhadap individu atau kelompok tertentu.
Pasal karet	Ketentuan dalam peraturan perundang-undangan yang dirumuskan secara samar, multitafsir, atau terlalu luas sehingga penerapannya mudah disalahgunakan terhadap subjek hukum.
System interference	Perbuatan yang tanpa hak dan sengaja menghambat fungsi sistem komputer dengan memasukkan, mengirimkan, merusak, menghapus, memperburuk, mengubah, atau memperkecil data komputer.
Timpa teks	Perbuatan mengganti atau menimpa teks yang sudah ada dengan teks baru sehingga isi sebelumnya hilang, berubah, atau tidak lagi dapat diakses dalam bentuk aslinya.

1

PENDAHULUAN

1.1 SEJARAH SINGKAT PEMBENTUKAN UU ITE DAN LATAR BELAKANG PERMASALAHAN PASAL 32 UU ITE

Pembentukan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) pada awalnya dilatarbelakangi oleh kebutuhan negara untuk menyesuaikan sistem hukum dengan perkembangan teknologi informasi dan komunikasi, khususnya dalam memberikan kepastian hukum terhadap transaksi elektronik, dokumen digital, tanda tangan elektronik, serta pengakuan bukti elektronik dalam proses hukum. Sehingga, peraturan ini dimaksudkan sebagai instrumen untuk mendukung pertumbuhan ekonomi digital, hak cipta dan paten teknologi, serta mendorong pelayanan publik di era globalisasi informasi.[1] Seiring perkembangan waktu, kebutuhan tersebut bergeser pada munculnya kekhawatiran penggunaan ruang siber sebagai media baru kejahatan. Beberapa perbuatan yang menjadi dasar kekhawatiran tersebut seperti *carding, hacking, cracking, phishing, booting, viruses, cybersquatting,* pornografi, perjudian, penipuan, terorisme, penyebaran informasi destruktif yang telah menjadi bagian dari aktivitas perbuatan pelaku kejahatan internet dan *information and communication technology* (ICT).[2]

Dalam naskah akademik pengaturan mengenai Informasi dan Transaksi Elektronik, pengaturan delik siber secara fundamental menjadi perlu karena cara manusia berkomunikasi, bertransaksi, dan menyimpan data yang bisa melahirkan bentuk-bentuk perbuatan melawan hukum yang tidak lagi dapat dijangkau secara

---

1 Departemen Komunikasi dan Informatika Republik Indonesia, *Naskah Akademik Rancangan Undang-Undang tentang Informasi dan Transaksi Elektronik,* hal. 2-3.

2 *Ibid.*, hal. 4.

memadai oleh konstruksi hukum pidana konvensional. Dokumen ini menjelaskan bahwa karakteristik kejahatan siber, seperti penggunaan sistem elektronik sebagai objek maupun sarana tindak pidana, sifatnya yang tidak mengenal batas wilayah, kecepatan dan skala kerugian yang ditimbulkan, serta kompleksitas pembuktian digital, menuntut perumusan delik yang lebih teknis, spesifik, dan berbasis pada perlindungan terhadap kerahasiaan, keutuhan, dan ketersediaan data dan sistem elektronik.[3] Dalam kerangka ini, delik yang berkaitan dengan perusakan integritas data (*data interference*), termasuk yang diatur dalam Pasal 32 UU ITE, seharusnya dibatasi pada perbuatan yang sengaja dan tanpa hak mengganggu atau merusak integritas data pada komputer, bukan pada penggunaan atau penyebaran informasi sebagai bagian dari ekspresi.

Namun demikian, dalam implementasinya, orientasi penerapan norma UU ITE mengalami pergeseran yang cukup signifikan. Alih-alih berfokus pada penguatan infrastruktur hukum di bidang ekonomi digital sebagaimana mandat awalnya, penggunaan pasal-pasal dalam UU ini justru banyak mengarah pada pengaturan perilaku sosial di ruang siber. Pasal 27A mengenai pencemaran nama baik, Pasal 28 ayat (2) mengenai ujaran kebencian, dan Pasal 28 ayat (3) mengenai berita bohong menjadi pasal-pasal yang paling sering digunakan dalam praktik penegakan hukum.[4] Hingga yang terbaru, penjeratan ekspresi yang sah menggunakan Pasal 32 pada konteks satir atau bahkan pelaporan pelanggaran hukum yang menggunakan informasi rahasia.[5] Pergeseran fokus ini menandai adanya perluasan fungsi hukum dari ranah ekonomi menuju ranah moral dan sosial yang justru menimbulkan pelanggaran hak-hak asasi manusia dan juga tidak sejalan dengan prinsip-prinsip demokrasi.

Penerapan Pasal 32 UU ITE yang melenceng dari tujuan awalnya tersebut membawa dampak serius pada jaminan kepastian hukum dan perlindungan kebebasan berekspresi dan berpendapat. Perumusan unsur yang ambigu dalam tingkat pembuatan undang-undang dan interpretasi yang inkonsisten dalam tingkat penerapan unsur oleh aparat penegak hukum (APH) menyebabkan ruang-ruang

---

3 Badan Pembinaan Hukum Nasional Departemen Hukum dan Hak Asasi Manusia Republik Indonesia, *Naskah Akademik Rancangan Peraturan Pemerintah Tentang Transaksi Elektronik 2005*, hal. 21-27, diakses melalui https://bphn.go.id/data/documents/15na%20ITE.pdf

4 Southeast Asia Freedom of Expression Network, *Laporan Situasi Hak-Hak Digital Indonesia 2024: Tergencet Estafet Represi di Internet,* ed. Anton Muhajir, (Denpasar: SAFEnet, 2025), hal. 21-25.

5 Southeast Asia Freedom of Expression Network, *Laporan Pemantauan Hak-Hak Digital di Indonesia Triwulan II 2025*, ed. Anton Muhajir, (Denpasar: SAFEnet, 2025), hal. 21-22.

rawan kriminalisasi bagi pelaku kebebasan berekspresi dan berpendapat, yang seharusnya dilindungi dalam negara demokratis. Dalam banyak kasus, APH gagal membedakan antara tindakan yang menyerang integritas data (*data interference*), tindakan *illegal access*, dan aktivitas di ruang siber sebagai bentuk kebebasan berekspresi dan berpendapat itu sendiri. Misalnya, dalam kasus putusan pengadilan No. 175/Pid.Sus/2016/PN.Jkt.Pst. dengan terdakwa Ita Suaria Diberty. Dalam dakwaannya, jaksa menggunakan Pasal 30 UU ITE yang berkaitan dengan *illegal access*, alternatif terhadap Pasal 32 UU ITE, kepada terdakwa yang berdasarkan bukti di persidangan tidak melakukan *illegal access*, sebab pihak yang mengakses data atau sistem komputer dalam kasus tersebut adalah orang yang berotoritas dan pengaksesan tersebut tidak didasarkan pada niat atau tujuan buruk. Berdasarkan contoh kasus ini, APH gagal membedakan basis tindakan penyerangan integritas data dengan *illegal access*.

Dalam perkembangannya, UU ITE telah mengalami banyak sekali pengujian melalui *legislative review* maupun *judicial review*. Dalam proses *legislative review,* UU ITE mengalami revisi sebanyak dua kali, yakni pada 2016 dan 2024.[6] Pasal-pasal karet yang sering menjerat korban telah diperketat dengan penambahan unsur-unsur pidana dan semakin mendekati standar HAM internasional.[7] Begitu pun melalui *judicial review,* UU ITE telah melalui 18 pengujian, baik uji materiil maupun uji formil di Mahkamah Konstitusi.[8] Namun, proses pengujian pasal ini tidak dilakukan secara menyeluruh. Pasal 32 UU ITE tidak diperbaiki sejak pembentukan UU ITE pada 2008, bahkan *judicial review* melalui Mahkamah Konstitusi pada 2021 juga tidak memberikan hasil yang memuaskan terkait pengaturan Pasal 32 UU ITE.[9] Padahal, pengujian dan perbaikan ini perlu, sebab Pasal 32 UU ITE memiliki banyak sekali ruang kekeliruan dalam penafsiran dan penerapan pasal, seperti perumusan unsur-unsur pidana ambigu dan multitafsir yang bisa digunakan untuk mengkriminalisasi, sanksi pidana yang sangat tinggi, hingga perumusan norma yang belum disesuaikan dengan perkembangan hukum.

1.2 RUMUSAN MASALAH

---

6 Southeast Asia Freedom of Expression, *Dari Kriminalisasi hingga Moderasi: Catatan Implementasi Revisi Kedua UU ITE pada Kebebasan Berekspresi dan Pemilihan Umum 2024*, ed. Ika Ningtyas, (Denpasar: Safenet, 2024), hal. 7-10.

7 *Ibid.*

8 Penelusuran riwayat *judicial review* UU ITE ini dapat diakses melalui tautan berikut: https://tracking.mkri.id/index.php?id=1&jenis=2&menu=4&page=web.home

9 Putusan Mahkamah Konstitusi Nomor 17/PUU-XIX/2021

Berdasarkan latar belakang tersebut, kajian ini menggarisbawahi masalah utama bahwa rancangan Pasal 32 UU ITE sebagai instrumen perlindungan data dan sistem atau program komputer bergeser menjadi alat pemidanaan terhadap ekspresi yang sah di ruang siber. Oleh sebab itu, rumusan masalah yang hendak dijawab melalui kajian ini adalah:

1. Bagaimana peraturan internasional merespons fenomena *data interference* dan kaitannya dengan hak sipil atas kebebasan berekspresi dan berpendapat?
2. Bagaimana situasi penerapan Pasal 32 UU ITE di Indonesia dan apa saja masalahnya terhadap kebebasan berekspresi dan berpendapat?
3. Bagaimana menerapkan Pasal 32 UU ITE dengan ideal?

1.3 TUJUAN KAJIAN

1. Mengidentifikasi peraturan internasional tentang *data interference* dan kaitannya dengan hak sipil atas kebebasan berekspresi dan berpendapat.
2. Mengidentifikasi situasi dan masalah penerapan Pasal 32 UU ITE di Indonesia terhadap kebebasan berekspresi dan berpendapat.
3. Mengidentifikasi cara ideal dalam menafsirkan dan menerapkan Pasal 32 UU ITE di Indonesia.

1.4 RUANG LINGKUP KAJIAN DAN METODE PENGUMPULAN DATA

Pada dasarnya, tindak pidana siber dapat dikategorikan ke dalam dua jenis yakni *cyber-dependent crimes* dan *cyber-enabled crimes*. *Cyber-dependent crimes* adalah tindak pidana yang hanya bisa dilakukan menggunakan komputer, jaringan komputer/internet, atau bentuk lain dari teknologi informasi dan komunikasi. Tindak pidana seperti ini umumnya menyasar pada teknologi informasi dan komunikasi dan ditandai dengan peretasan dan/atau menggunakan perangkat lunak berbahaya termasuk *ransomware.* Sedangkan, *cyber-enabled crimes* adalah tindak pidana tradisional yang difasilitasi atau menggunakan internet dan teknologi digital. Tindak pidana semacam ini berevolusi dalam bentuk dan skala akibat meningkatnya penggunaan teknologi komunikasi. Tindak pidana ini mencakup penipuan secara daring, pembajakan, pemalsuan, dan sebagainya.[10]

10 Colin Murphy, *Understanding Cybercrime*, https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/760356/EPRS_BRI(2024)760356_EN.pdf, hal. 2.

Beberapa instrumen hukum internasional mengkategorikan beberapa tindak pidana yang termasuk ke dalam *cyber-dependent crime*, seperti *illegal access, illegal interception, data interference, system interference, misuse of device* (penyalahgunaan gawai), dan *computer related forgery* (pemalsuan terkait komputer).[11] Kajian ini hanya akan berfokus pada keselarasan bangunan konsep tindak pidana *data interference* dengan unsur tindakan dalam Pasal 32 UU ITE. Keselarasan ini berguna dalam melihat dampak pengaturan Pasal 32 UU ITE terhadap kebebasan berekspresi dan berpendapat, khususnya ekspresi dan pendapat di ruang siber. Dengan demikian, ruang lingkup kajian ini secara berurutan terdiri dari pengertian, praktik, dan pengaturan tentang *data interference*; analisis penafsiran dan penerapan Pasal 32 UU ITE saat ini yang berlaku di Indonesia; dan penyusunan tawaran alternatif dalam menafsirkan dan menerapkan Pasal 32 UU ITE di Indonesia.

Berdasarkan ruang lingkup tersebut, kajian ini disusun berdasarkan studi literatur, catatan pendampingan kasus di lapangan, penelusuran putusan pengadilan, dan *focused group discussion* (FGD).

- **Studi literatur**

Studi literatur dilakukan untuk menelusuri konsep dan kerangka hukum, baik internasional maupun nasional, tentang jenis-jenis kejahatan siber, seperti *data interference*, *system interference*, dan *illegal access*, dan konsep kebebasan berekspresi dan berpendapat. Telusur literatur ini dilakukan terhadap dokumen peraturan internasional, seperti *Universal of Declaration of Human Rights* (UDHR), *International Covenant Civil and Political Rights* (ICCPR), *The Convention on Cybercrime* (Budapest Convention), dan *UN Convention on Cybercrime* (UNCC). Sedangkan telusur literatur terhadap dokumen peraturan nasional dilakukan pada Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 (UUD 1945), Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) beserta Naskah Akademik dan risalah pembahasannya, dan putusan Mahkamah Konstitusi (MK). Selain itu, studi literatur juga dilakukan terhadap literatur *data interference* di negara lain, serta literatur akademik dalam dan luar negeri.

Beberapa negara yang diambil sebagai contoh adalah Inggris, Amerika Serikat, Irlandia, dan Filipina. Negara-negara tersebut dipilih secara acak namun setidaknya tiga negara yakni Inggris, Amerika Serikat, dan Filipina telah meratifikasi Budapest

11 *Convention on Cybercrime/*Konvensi Tindak Pidana Siber, *Council of Europe No. Budapest 23.XI.2001*, Section 1.

Convention. Sedangkan, Irlandia baru menandatangani Budapest Convention dan belum meratifikasinya, namun menggunakannya sebagai panduan kerangka hukum penyusunan undang-undang di negaranya.

Dua negara, Inggris dan Amerika Serikat, telah memiliki undang-undang yang mengatur tindak pidana yang serupa dengan *illegal access* dan *data interference* sebelum Budapest Convention disahkan. Terlepas dari itu, baik Computer Misuse Act 1990 yang dimiliki oleh Inggris maupun Computer Fraud and Abuse Act 1986 milik Amerika Serikat cukup sejalan dengan Budapest Convention. Lebih lanjut, pada 2011, Inggris juga meratifikasi Budapest Convention.[12] Begitu juga dengan Amerika Serikat yang telah menandatangani Budapest Convention pada 2001 dan meratifikasinya pada 2006.[13]

Selain Inggris dan Amerika Serikat, dua negara lain yang diambil sebagai contoh telah mengesahkan undang-undang terkait tindak pidana siber setelah Budapest Convention diterbitkan. Sebagai contoh, Irlandia telah menandatangani Budapest Convention pada 2001 lalu mengesahkan Criminal Justice (Offences Relating to Information Systems) Act pada 2017. Meskipun undang-undang tersebut disahkan terlebih dulu, kerangka hukum yang digunakan dalam perumusan undang-undang tersebut mengacu pada Budapest Convention.[14] Kemudian, Filipina baru meratifikasi Budapest Convention pada 2018[15] dan sebetulnya telah memiliki RA 10175 (2012) yang mengatur tindak pidana siber sebelum meratifikasi Budapest Convention. Namun, dalam laporan Council of Europe, Budapest Convention memiliki pengaruh besar dalam penyusunan RA 10175 (2012) tersebut.[16]

---

12 John Leyden, "UK finally ratifies Cybercrime Convention during Obama visit", https://www.theregister.com/2011/05/25/uk_ratifies_cybercrime_convention/#:~:text=The%20UK%20underlined%20this%20commitment,still%20relevant%20today%20(PDF), diakses pada Jumat, 20 Februari 2026.

13 U.S. Department of State, "Mulitlateral (13174): - Convention on Cybercrime", https://www.state.gov/13174, diakses pada Jumat, 20 Februari 2026.

14 Hal ini terlihat dari jawaban Ireland Minister of Justice atas pertanyaan Deputy Roderic O'Gorman dalam diskusi Cybersecurity Policy. Minister of Justice menegaskan bahwa Criminal Justice (Offences Relating to Information System) Act 2017 telah mengatur kerangka penegakkan hukum untuk tindak pidana siber yang mengacu pada Budapest Convention. Minister of Justice juga menegaskan komitmennya untuk meratifikasi Budapest Convention. (Lihat https://www.oireachtas.ie/en/debates/question/2025-03-25/546/)

15 Daftar negara-negara yang telah menandatangani dan/atau meratifikasi Budapest Convention dapat dilihat melalui tautan berikut: https://www.coe.int/en/web/cybercrime/the-budapest-convention

16 Jose Midas P. Marquez, "From accession to action: The Philippines cybercrime strategy's progress", https://www.coe.int/fr/web/cybercrime/philippines?utm_source=chatgpt.com, diakses pada Jumat, 20 Februari 2026.

- **Catatan dan analisis pendampingan kasus di lapangan**

Tujuan dari metode ini adalah mengidentifikasi dan menguraikan temuan di lapangan atas kaitan antara kebebasan sipil dengan kejahatan di ruang siber berupa *data interference* yang dihukum pidana dengan Pasal 32 UU ITE. Temuan kasus ini berdasarkan aduan yang diterima oleh Lembaga Bantuan Hukum (LBH). Kasusnya dikelompokkan menjadi tiga berdasarkan sasaran pemidanaannya, yaitu pemidanaan terhadap *whistleblower*, pemidanaan korban kekerasan dalam rumah tangga (KDRT), dan pemidanaan pada timpa *text* digital.

- **Penelusuran dan analisis putusan pengadilan**

Dalam proses pengumpulan putusan, tim penulis mengakses database putusan seperti situs web Direktori Putusan Mahkamah Agung (https://putusan3.mahkamahagung.go.id/) dan Hukumonline (https://www.hukumonline.com/). Tujuan dari metode ini adalah melihat penafsiran dan penerapan Pasal 32 UU ITE oleh APH, khususnya jaksa melalui dakwaannya dan hakim melalui pertimbangan hukumnya. Untuk memfokuskan pengumpulan putusan pada perkara-perkara dengan dakwaan dan amar putusan yang menggunakan Pasal 32 UU ITE, tim peneliti menggunakan kata kunci sebagai berikut:

a. "mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan" untuk mencari putusan yang menggunakan Pasal 32 ayat (1) UU ITE; dan

b. "memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang lain" untuk mencari putusan yang menggunakan Pasal 32 ayat (2) UU ITE.

Dari pencarian putusan tersebut, ditemukan 112 nomor putusan untuk perkara menggunakan Pasal 32 ayat (1) UU ITE dan 39 nomor putusan untuk perkara Pasal 32 ayat (2) UU ITE di direktori putusan Mahkamah Agung. Tim peneliti hanya membaca dan menganalisis beberapa putusan sebagai sampel untuk membaca fenomena dalam penerapan pasal-pasal tersebut.

Selain putusan-putusan yang ada dalam situs web Direktori Putusan Mahkamah Agung dan Hukumonline, tim peneliti juga menggunakan putusan-putusan perkara yang didampingi atau telah dikurasi oleh LBH Pers dalam database milik LBH Pers yakni sejumlah 56 putusan. Dengan demikian terdapat total sekitar 207 putusan Pasal 32 ayat (1) dan/atau ayat (2) UU ITE yang dibaca oleh tim peneliti. Dari keseluruhan

putusan tersebut, mayoritas putusan yang ditemukan adalah terkait tindak pidana dalam sektor perbankan, telekomunikasi, data pribadi, dan sebagainya. Namun, terdapat juga sedikit putusan yang memiliki karakteristik perbuatan yang berbeda jauh dari mayoritas putusan yang ditemukan.

- **Focused group discussion (FGD)**

Kajian ini melakukan pengambilan data melalui wawancara mendalam melalui mekanisme *focused group discussion* (FGD). FGD dilakukan sebanyak 3 (tiga) kali, dengan peserta yang terdiri dari kelompok korban, Koalisi SERIUS Revisi UU ITE, dan PAKU ITE. Adapun beberapa narasumber ahli terdiri dari dosen hukum pidana dan dosen hukum tata negara yang memberikan paparan terkait *data interference* dan irisannya dengan kebebasan berekspresi dan berpendapat.

2

PERATURAN INTERNASIONAL DALAM MERESPONS FENOMENA *DATA INTERFERENCE* DAN KAITANNYA DENGAN HAK SIPIL ATAS KEBEBASAN BEREKSPRESI DAN BERPENDAPAT

2.1 KEBEBASAN BEREKSPRESI PADA INSTRUMEN HAM INTERNASIONAL DAN PRAKTIK DI BERBAGAI NEGARA

Hak atas kebebasan berekspresi telah dijamin dalam berbagai instrumen hak asasi manusia (HAM) internasional, yakni pada *Article 19 Universal Declaration of Human Rights* (UDHR)[17] dan juga *Article 19 (1)* dan (2) *International Covenant on Civil and Political Rights* (ICCPR) yang telah diratifikasi melalui Undang-Undang No. 12 Tahun 2005.[18] Hak kebebasan berekspresi adalah hak yang penting dilindungi untuk menjamin penikmatan hak-hak lainnya di dalam kerangka HAM serta untuk menjamin berjalannya negara yang demokratis. Di sisi lain, pelaksanaan hak kebebasan berekspresi memiliki batasan-batasan.

Adapun pembatasan tersebut seharusnya sejalan dengan *three-part test* yang dijelaskan dalam Komentar Umum No. 34[19] yakni, diatur melalui undang-undang

---

17 Lebih lengkapnya berbunyi "*Setiap orang berhak atas kebebasan mempunyai dan mengeluarkan pendapat; dalam hal ini termasuk kebebasan menganut pendapat tanpa mendapat gangguan, dan untuk mencari, menerima dan menyampaikan keterangan-keterangan dan pendapat dengan cara apa pun dan dengan tidak memandang batas-batas*".

18 Lebih lengkapnya berbunyi "*(1) Setiap orang berhak berpendapat tanpa ada yang mengganggunya. (2) Setiap orang berhak atas kebebasan berekspresi; hak ini mencakup kebebasan untuk mencari, menerima, dan menyampaikan informasi serta gagasan apa pun, terlepas dari batas-batas negara, baik secara lisan, tertulis, atau dalam bentuk cetakan, dalam bentuk karya seni, atau melalui media lain sesuai pilihannya*".

19 Komentar Umum No. 34 merupakan dokumen penjelasan dari Pasal 19 ICCPR tentang hak kebebasan berpendapat.

dengan rumusan yang jelas dan dapat dipahami (prinsip legalitas), berdasarkan kebutuhan dan proporsional, dan memiliki tujuan yang sah.[20] Tujuan sah dari pembatasan yang dimaksud telah disebut dalam Pasal 19 (3) ICCPR bahwa pelaksanaan hak atas kebebasan berekspresi tunduk pada batasan: untuk menghormati hak atau reputasi orang lain; atau untuk perlindungan keamanan nasional atau ketertiban umum (*ordre public)*, atau kesehatan atau moralitas publik.

Selain pada *Article 19 (3)* ICCPR, terdapat juga prinsip-prinsip yang penting untuk menjadi batu uji dalam pembatasan hak dan juga ekspresi di internet. Prinsip-prinsip itu tertuang pada *Siracusa Principles* dan juga *The Johannesburg Principles.* Dari berbagai instrumen HAM dan dokumen-dokumen penjelas tersebut, dapat ditarik kesimpulan bahwa hak atas kebebasan berekspresi adalah hak yang wajib dilindungi oleh negara dan hanya dapat dibatasi secara ketat berdasarkan tujuan yang sah dan dilakukan secara proporsional.

Jaminan perlindungan hak kebebasan berekspresi serta syarat-syarat pembatasannya juga dituangkan pada Undang-Undang Dasar Negara Republik Indonesia 1945 (UUD NRI 1945). Jaminan hak atas kebebasan berpendapat dan berekspresi dituangkan pada Pasal 28E ayat (3) UUD NRI 1945[21]. Selain itu, Pasal 28F UUD NRI 1945[22] mengatur mengenai hak atas informasi. Sementara itu, syarat-syarat pembatasan hak, termasuk di dalamnya yaitu untuk menghormati hak dan kebebasan orang lain, diatur dalam Pasal 28J UUD NRI 1945[23].

Salah satu cara bagi negara untuk melakukan pembatasan hak adalah melalui pengaturan ketentuan pidana dalam undang-undang. Salah satu undang-undang yang memiliki hubungan erat dengan pembatasan hak atas kebebasan berekspresi adalah UU ITE. Beberapa pasal dalam UU ITE acapkali digunakan untuk mendakwa

---

20 *General Comment No. 34 Article 19: Freedoms of opinion and expression*/Komentar Umum No. 34 Pasal 19: Kebebasan Berpendapat dan Berekspresi, *Human Rights Committee No. CCPR/C/GC/34*, 11-29 July 2011, Pasal/Art 22.

21 Lebih lengkapnya berbunyi *"Setiap orang berhak atas kebebasan berserikat, berkumpul, dan mengeluarkan pendapat."*

22 Lebih lengkapnya berbunyi *"Setiap orang berhak untuk berkomunikasi dan memperoleh informasi untuk mengembangkan pribadi dan lingkungan sosialnya, serta berhak untuk mencari, memperoleh, memiliki, menyimpan, mengolah, dan menyampaikan informasi dengan menggunakan segala jenis saluran yang tersedia."*

23 Lebih lengkapnya berbunyi *"(1) Setiap orang wajib menghormati hak asasi manusia orang lain dalam tertib kehidupan bermasyarakat, berbangsa, dan bernegara. (2) Dalam menjalankan hak dan kebebasannya, setiap orang wajib tunduk kepada pembatasan yang ditetapkan dengan undang-undang dengan maksud semata-mata untuk menjamin pengakuan serta penghormatan atas hak dan kebebasan orang lain dan untuk memenuhi tuntutan yang adil sesuai dengan pertimbangan moral, nilai-nilai agama, keamanan, dan ketertiban umum dalam suatu masyarakat demokratis."*

ekspresi individu yang dianggap melanggar hukum, di antaranya yaitu Pasal 27A dan Pasal 28 ayat (2). Pengaturan Pasal 27A UU ITE adalah bentuk pembatasan hak kebebasan berekspresi berhubungan dengan perlindungan kehormatan atau martabat orang lain. Pasal semacam ini (pencemaran nama baik) sebetulnya telah lama direkomendasikan oleh Komite PBB untuk didekriminalisasi.[24] Pasal 28 ayat (2) UU ITE mengandung konteks perlindungan ketertiban umum dan moral publik sebagai tujuan pembatasan kebebasan berekspresi.[25] Selain kedua pasal tersebut, belakangan ini Pasal 32 UU ITE juga sering digunakan sebagai pasal dakwaan terhadap ekspresi warga negara. Apabila dibaca secara seksama, rumusan Pasal 32 tersebut sejatinya tidak memiliki konteks tujuan pembatasan hak kebebasan berekspresi yang sejalan dengan *Article 19 (3)* ICCPR. Tetapi, merujuk kepada UUD 1945, pembatasan yang terkandung dalam Pasal 32 UU ITE dapat dikategorikan bertujuan untuk melindungi hak orang lain, khususnya hak atas perlindungan terhadap harta benda di bawah kekuasaannya dan hak atas rasa aman sebagaimana diatur dalam Pasal 28G ayat (1) UUD NRI 1945.[26] Uraian lebih lanjut mengenai konteks Pasal 32 UU ITE sebagai perlindungan terhadap harta benda serta hak atas rasa aman dapat dilihat pada bagian di bawah ini.

2.2 *DATA INTERFERENCE* SEBAGAI KEJAHATAN SIBER DALAM PERATURAN INTERNASIONAL

2.2.1 Perbandingan Pengaturan Kejahatan Siber dalam Budapest Convention dan UU ITE

Pemerintah menyusun ketentuan Pasal 32 UU ITE dengan mengacu kepada substansi dari *The Convention on Cybercrime, Budapest,* 23.XI.2001 (*Budapest Convention*) agar negara dapat menangani tindak pidana siber secara efektif[27]. Beberapa materi

---

24 General Comment No. 34…, *Op. Cit.*, Pasal/Art. 47.

25 Beberapa pasal dalam UU ITE sebelum direvisi pada 2024 seringkali digunakan untuk mengancam maupun mempidanakan orang-orang yang menggunakan haknya untuk berekspresi. Pasca revisi pun, masih terdapat kritik terhadap beberapa pasal tersebut maupun potensi ancaman terhadap kebebasan berekspresi dari pasal-pasal tertentu dalam UU ITE baru (Lihat: https://www.hukumonline.com/berita/a/pasal-karet-dalam-uu-ite-terbaru-masih-mengancam-masyarakat-yang-kritis-lt6597e40be9b8c/). Data mengenai penyalahgunaan pasal-pasal ini tidak akan dijabarkan secara rinci dalam tulisan ini mengingat fokus tulisan ini adalah pada Pasal 32 UU ITE. Namun, tim peneliti tidak menjustifikasi praktik pemidanaan ekspresi menggunakan Pasal 27A maupun Pasal 28 ayat (2) UU ITE yang keliru atau dipaksakan.

26 Lebih lengkapnya berbunyi *"Setiap orang berhak atas pelindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang ada di bawah kekuasaannya, serta berhak atas rasa aman dan pelindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi"*

27 Putusan Mahkamah Konstitusi No. 78/PUU-XVII/2019, hal. 74.

yang diatur dalam *Budapest Convention* adalah mengenai *illegal access (Article 2), illegal interception (Article 3), data interference (Article 4), system interference (Article 5), misuse of device (Article 6), dan computer related forgery (Article 7)*. Tiga ketentuan yang dianalisis dalam tulisan ini adalah mengenai *illegal access, data interference,* dan *system interference* karena secara konteks pengaturan memiliki kesamaan atau hubungan dengan Pasal 32 UU ITE.

Tabel 2.1: Perbandingan Rumusan Ketentuan *Illegal Access, Data Interference,* dan *System Interference* Budapest Convention dan UU ITE

Kejahatan Siber	Budapest Convention	UU ITE
Illegal Access	Pasal 2: Tiap pihak (negara peserta) wajib membuat suatu peraturan perundangan atau melakukan tindakan lain yang diperlukan berdasarkan hukum domestiknya untuk mengatur suatu perbuatan, yang dilakukan dengan sengaja dan tanpa hak, mengakses ke seluruh atau sebagian dari sistem komputer. Negara peserta dapat mengatur dalam aturan tersebut bahwa perbuatan pidana tersebut mencakup perbuatan yang dilakukan dengan melanggar langkah-langkah keamanan, dengan maksud untuk memeroleh data komputer atau disertai niat tidak baik lainnya, atau berkaitan dengan sistem komputer yang terhubung ke sistem komputer lainnya.	Pasal 30: (1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apapun. (2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apapun dengan tujuan untuk memperoleh Informasi Elektronik dan/ atau Dokumen Elektronik. (3) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apapun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

Kejahatan Siber	Budapest Convention	UU ITE
Data Interference	Pasal 4: (1) Setiap Pihak wajib membuat suatu peraturan perundanga dan tindakan lain yang diperlukan untuk mengatur perbuatan, yang dilakukan dengan sengaja dan tanpa hak, merusak, menghapus menurunkan kualitas, mengubah, atau menghapus data komputer sebagai tindak pidana. (2) Suatu Pihak dapat mengatur ketentuan agar tindakan yang dijelaskan dalam paragraf 1 harus mengakibatkan kerugian serius.	Pasal 32: (1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/ atau Dokumen Elektronik milik Orang lain atau milik publik. (2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang lain yang tidak berhak.
System Interference	Pasal 5: Tiap Pihak harus membuat suatu peraturan perundangan dan mengambil tindakan lain yang diperlukan untuk menetapkan suatu tindakan serius, jika dilakukan dengan sengaja dan tanpa hak, menghambat tanpa hak fungsi sistem komputer dengan memasukkan,	Pasal 33: Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apapun yang berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya

Kejahatan Siber	Budapest Convention	UU ITE
	mengirimkan, merusak, menghapus, memperburuk, mengubah, atau memperkecil data komputer sebagai tindak pidana.	

2.2.2 Perbedaan Konsep Illegal Access, Data Interference, dan System interference

Dalam kerangka *Budapest Convention*, rumusan Pasal 32 ayat (1) dan (2) UU ITE sebetulnya mengatur larangan atas perbuatan yang dikenal dengan istilah "*data interference*". Pasal 4 Budapest Convention mengartikan *data interference* sebagai perbuatan yang dilakukan dengan sengaja dan tanpa hak untuk merusak, menghapus, mengurangi, mengubah, atau menyamarkan data komputer. Dalam *Budapest Convention* perbuatan ini diatur terpisah dengan perbuatan lain yang juga dilarang, yaitu "*system interference*". Pasal 5 *Budapest Convention* mendefinisikan "*system interference*" sebagai perbuatan yang dilakukan dengan sengaja, tanpa hak, dan secara serius menghambat fungsi dari sistem komputer dengan cara memasukkan, mentransmisikan, merusak, menghapus, mengurangi, mengubah, atau menyamarkan data komputer. Baik "*data interference*" maupun "*system interference*" memiliki unsur perbuatan yang mirip, dan pengaturan tentang keduanya, termasuk pelarangan tindakannya, ditujukan untuk melindungi kerahasiaan, integritas, dan ketersediaan sistem maupun data komputer, dan mencegah kriminalisasi atas aktivitas yang sah dan normal dilakukan dalam proses merancang jaringan elektronik maupun proses mengoperasikan jaringan dan praktik-praktik komersial lainnya.[28] Namun, objek dan kepentingan hukum yang dilindungi dalam kedua ketentuan ini berbeda.

Larangan atas "*data interference*" ditujukan untuk melindungi integritas dan fungsi data dan program komputer sebagaimana melindungi benda-benda fisik pada umumnya dari kerusakan yang disengaja.[29] Dalam *Explanatory Report to*

---

28 *Explanatory Report to the Convention on Cybercrime Budapest*/Laporan Penjelasan atas Konvensi Tindak Pidana Siber Budapest *23.XI.2001, European Treaty Series - No. 18*, Pasal/Art 43.

29 *Ibid*, par. 60.

the Convention on Cybercrime Budapest, terdapat penjelasan tentang definisi masing-masing perbuatan yang dilarang, seperti "mengubah", "mengurangi", "menghapus", dan sebagainya. Meskipun demikian, laporan ini memberikan penekanan penting pada kapan perbuatan-perbuatan tersebut dilarang, yaitu ketika perbuatan-perbuatan tersebut dilakukan secara sengaja[30] dan "tanpa hak". Ketentuan yang demikian telah masuk pada rumusan Pasal 32 ayat (1) dan ayat (2) UU ITE. Artinya, aktivitas yang pada umumnya dilakukan dan melekat pada desain jaringan elektronik atau praktik operasional maupun komersial tidak dapat dipidana. Aktivitas yang pada umumnya dilakukan tersebut misalnya kegiatan pengujian keamanan sistem komputer yang diotorisasi oleh pemilik sistem, modifikasi data untuk tujuan keamanan komunikasi, atau modifikasi data untuk memfasilitasi komunikasi anonim.[31]

Di samping itu, larangan "*system interference*" yang diatur dalam *Budapest Convention* bertujuan untuk menjerat perbuatan-perbuatan yang menghalangi atau menghambat penggunaan komputer, termasuk jaringan telekomunikasi, yang sah. Kepentingan hukum yang dilindungi melalui pelarangan "*system interference*" adalah kepentingan operator dan pengguna dalam menggunakan fungsi komputer atau jaringan telekomunikasi.[32] Perbuatan dalam "*system interference*" dapat dilakukan melalui beberapa cara yang mirip dengan yang diatur dalam ketentuan "*data interference*" pada *Budapest Convention*. Hanya saja, perbedaan mendasar dari pelarangan keduanya adalah istilah "*hindering*" atau kondisi menghambat sebagai konsekuensi dari "*system interference*". Perbuatan yang ditujukan untuk menghambat sistem komputer ini harus memiliki dampak serius agar dapat dikenakan sanksi pidana. Kriteria dampak serius tersebut harus ditentukan oleh negara. Selain itu, "*system interference*" ini juga harus dilakukan secara sengaja dan "tanpa hak", yaitu secara sengaja bertujuan untuk menghambat penggunaan fungsi sistem komputer maupun jaringan telekomunikasi.

Berdasarkan penjelasan "*data interference*" dan "*system interference*" dalam *Budapest Convention* tersebut, dapat disimpulkan bahwa meski beberapa unsur serupa, tujuan dari kedua ketentuan ini berbeda. Larangan "*data interference*" berfokus pada pelindungan integritas data dan program komputer dari kerusakan,

30 *Ibid*, par. 63.

31 *Ibid*, par. 62.

32 *Ibid*, par. 65.

sedangkan larangan "*system interference*" berfokus pada pelindungan kepentingan pengguna atau operator dari suatu sistem komputer agar mereka dapat menggunakan sistem komputer tanpa gangguan. Objek dari pengaturan di kedua ketentuan ini pun jelas berbeda sesuai dengan nama dari kedua ketentuan tersebut.

Selain dengan *system interference*, penting juga untuk melihat perbandingan konteks antara *data interference* dengan *illegal access*. Dalam *Budapest Convention,* pasal *illegal access* dan *data interference* melindungi kepentingan hukum yang berbeda. *Illegal access* menitikberatkan pada pelanggaran terhadap kontrol akses suatu sistem komputer, yakni perbuatan mengakses seluruh atau sebagian sistem komputer tanpa hak. Inti deliknya adalah masuknya pihak yang tidak berwenang, terlepas dari apakah setelah masuk tersebut pelaku merusak, mengubah, atau menghapus data. Dengan demikian, fokus utama pasal ini adalah perlindungan atas kerahasiaan dan eksklusivitas akses terhadap sistem komputer. Sedangkan *data interference,* berfokus pada gangguan terhadap data komputer. Perbuatan yang dipidana mencakup penghapusan, perusakan, pengubahan, atau penekanan data komputer tanpa hak, baik perbuatan tersebut didahului oleh *illegal access* maupun tidak. Artinya, seseorang bisa saja melakukan *data interference* meskipun ia memiliki akses ke sistem, selama tindakan terhadap data dilakukan tanpa kewenangan. Di sini, yang dilindungi bukan lagi pintu masuk ke sistem, melainkan keutuhan dan keberfungsian data tersebut. Sehingga, pada prinsipnya pengaturan ini untuk melindungi data yang harus dilihat secara kesatuan kerahasiaannya, integritasnya, dan keberadaan data di jaringan komputer. Pengaturan ini juga mensyaratkan bahwa harus terdapat akses terlebih dahulu ke dalam sistem ataupun komputer, sehingga integritas data tersebut terancam.

Selain *Budapest Convention*, kejahatan siber juga diatur dalam *UN Convention on Cybercrime* (UNCC). *Illegal Access* diatur dalam Pasal 7 (1), yang menyatakan "*Setiap Negara Pihak wajib mengadopsi langkah-langkah legislatif dan tindakan lain yang diperlukan untuk menetapkan sebagai tindak pidana dalam hukum nasionalnya, apabila dilakukan dengan sengaja, perbuatan mengakses seluruh atau sebagian sistem teknologi informasi dan komunikasi tanpa hak".* Sementara ayat 2 dari pasal ini memberikan ketentuan opsional yang dapat diadopsi oleh negara: *"Suatu Negara Pihak dapat mensyaratkan bahwa tindak pidana tersebut dilakukan dengan cara melanggar langkah-langkah keamanan, dengan maksud untuk memperoleh data elektronik atau dengan niat tidak jujur atau niat jahat lainnya,*

atau berkaitan dengan sistem teknologi informasi dan komunikasi yang terhubung dengan sistem teknologi informasi dan komunikasi lainnya". Ketentuan opsional ini menekankan pada pentingnya kesengajaan dan niat jahat dalam *illegal access* yang terjadi yang mana sejalan dengan pengaturan dalam Budapest Convention.

Pasal 9 Konvensi ini mengatur soal *data interference* dengan menyatakan *"Setiap Negara Pihak harus mengadopsi undang-undang atau langkah-langkah lain yang diperlukan untuk menetapkan sebagai tindak pidana dalam hukum nasionalnya, apabila dilakukan dengan sengaja dan tanpa hak, tindakan merusak, menghapus, menurunkan kualitas, mengubah, atau menekan (menyembunyikan) data elektronik".* Ayat (2) dari pasal tersebut menyebutkan: *"Negara Pihak dapat mensyaratkan bahwa perbuatan sebagaimana dimaksud pada ayat (1) hanya dianggap tindak pidana jika mengakibatkan kerugian serius."* Aspek "kerugian serius" di sini perlu digaris bawahi karena artinya harus ada dampak yang terukur dari tindakan yang dilakukan.

Selain melihat perbandingan antara Budapest Convention dengan UNCC, penting juga untuk melihat contoh bagaimana negara lain (Amerika dan Inggris) mengatur dan mengimplementasikan ketentuan terkait illegal access dan data interference. Beberapa pengaturan dan praktik tersebut adalah sebagai berikut:

Tabel 2.2: Pengaturan dan Implementasi Ketentuan *Illegal Access* dan *Data Interference* di Beberapa Negara

Negara	Pengaturan Negara Lain	Catatan Pasal	Contoh Implementasi
Inggris **Computer Misuse Act (CMA)**[33]	**Section 1: Unauthorised access to computer material.** Pasal 1: Akses tidak sah terhadap komputer[34] (1) Seseorang dinyatakan melakukan pelanggaran jika— (a) ia membuat komputer melakukan suatu fungsi dengan maksud untuk memperoleh akses ke suatu program atau data yang tersimpan di dalam komputer tersebut atau untuk memungkinkan akses tersebut diperoleh olehnya]; (b) akses yang ia maksudkan untuk diperoleh [atau untuk memungkinkan diperoleh] adalah tidak sah; dan (c) ia mengetahui pada saat ia menyebabkan komputer melakukan fungsi tersebut bahwa hal itu memang akan terjadi.	CMA merumuskan struktur tindak pidana *illegal access* cukup jelas, ada tindakan yang menyebabkan komputer menjalankan fungsi tertentu, ada niat, dan harus disertai pengetahuan bahwa tindakan itu tidak sah. Kombinasi ini penting karena mencegah pemidanaan atas kesalahan yang bersifat tidak disengaja, seperti kesalahan teknis atau akses yang terjadi karena kelalaian sistem. Unsur-unsur pokoknya: 1. tindakan menjalankan fungsi pada komputer; 2. dengan maksud memperoleh akses ke data atau program; 3. akses tersebut tidak berwenang; 4. pelaku mengetahui bahwa akses tersebut tidak berwenang.	Dalam Putusan DPP v Jones [1997] 2 CR App R 155 sebuah komputer didefinisikan sebagai perangkat untuk menyimpan, memproses, dan mengambil informasi Berdasarkan ketentuan Pasal 1(2) CMA maksud untuk mengamankan akses tidak perlu diarahkan pada program atau data tertentu, program atau data jenis tertentu atau program atau data yang tersimpan di komputer tertentu. Niat baik juga tidak akan mempengaruhi penerapan Pasal 1 CMA. Kasus R v Cuthbert [2005] (Tidak dilaporkan, Pengadilan Magistrat Horseferry Road, 6 Oktober 2006) menunjukkan bahwa peretasan yang etis dapat dinyatakan bersalah atas akses tidak sah

33 Inggris, *Computer Misuse Act 1990*/Undang-Undang Penyalahgunaan Komputer, Pasal 1 dan 3.

34 Pasal-pasal dalam tabel ini merupakan terjemahan bebas.

Negara	Pengaturan Negara Lain	Catatan Pasal	Contoh Implementasi
	(2) Niat yang harus dimiliki seseorang untuk melakukan pelanggaran berdasarkan pasal ini tidak perlu dilakukan dengan spesifik menyasar pada— (a) program atau data tertentu; (b) program atau data jenis tertentu; atau (c) program atau data yang tersimpan di dalam komputer tertentu. Pasal 3: Tindakan tidak sah dengan maksud untuk merusak, atau dengan kelalaian dalam merusak, pengoperasian komputer, dll. (1) Seseorang dinyatakan bersalah atas suatu pelanggaran jika— (a) ia melakukan tindakan tidak sah yang berkaitan dengan komputer; (b) pada saat ia melakukan perbuatan tersebut ia mengetahui bahwa perbuatan itu tidak sah; dan (c) salah satu dari ayat (2) atau ayat (3) di bawah ini berlaku.	Pada pasal mengenai data interference mengatur mengenai illegal access terlebih dahulu terhadap perangkat.	ke materi komputer. Cuthbert, seorang konsultan keamanan komputer, melakukan uji penetrasi pada situs web Komite Darurat Bencana (DEC) karena ia curiga bahwa situs web tersebut tidak otentik. Dirinya kemudian diputus bersalah melakukan pelanggaran berdasarkan Pasal 1 dengan sengaja melakukan akses tidak sah terhadap sistem DEC. Pengujian keamanan tanpa izin dianggap sebagai bentuk main hakim sendiri yang jelas melanggar CMA 1990.

Negara	Pengaturan Negara Lain	Catatan Pasal	Contoh Implementasi
	(2) Ayat ini berlaku jika orang tersebut bermaksud dengan melakukan perbuatan tersebut— (a) untuk mengganggu pengoperasian komputer apa pun; (b) untuk mencegah atau menghalangi akses ke program atau data apa pun yang tersimpan di komputer apa pun; (c) untuk mengganggu pengoperasian program tersebut atau keandalan data tersebut; atau (d) untuk memungkinkan salah satu hal yang disebutkan dalam paragraf (a) hingga (c) di atas dilakukan.		
Amerika Serikat	Computer Fraud and Abuse Act (CFAA)[35] 1030. Penipuan dan aktivitas terkait yang berhubungan dengan komputer	CFAA secara eksplisit membedakan antara pelanggaran akses terhadap data pertahanan, data finansial, dan data pemerintahan. Pendekatan ini secara tegas memisahkan	HIQ LABS, INC., Plaintiff-Appellee, v. LINKEDIN CORPORATION United States Supreme Court No. 17-16783 D.C. No. 3:17-cv-03301-EMC, April 2022

35 Amerika Serikat, Computer Fraud & Abuse Act/Undang-Undang Kekerasan dan Penipuan Berbasis Komputer, Pasal 1030.

Negara	Pengaturan Negara Lain	Catatan Pasal	Contoh Implementasi
	(1) dengan sengaja mengakses komputer tanpa izin atau tidak sesuai dengan akses yang diizinkan, dan dengan cara tersebut memperoleh informasi yang telah ditentukan oleh Pemerintah Amerika Serikat berdasarkan perintah Eksekutif atau undang-undang harus dilindungi dari pengungkapan tanpa izin karena alasan pertahanan nasional atau hubungan luar negeri, atau data terbatas apa pun, sebagaimana didefinisikan dalam paragraf y. dari bagian 11 Undang-Undang Energi Atom tahun 1954, dengan maksud atau alasan untuk percaya bahwa informasi yang diperoleh tersebut akan digunakan untuk merugikan Amerika Serikat, atau untuk keuntungan negara asing mana pun; (2) dengan sengaja mengakses komputer tanpa izin atau tidak	kategori data berdasarkan tingkat kepentingan publik atau nasional. Dengan begitu, hukum ini memprioritaskan perlindungan terhadap data yang berimplikasi pada keamanan nasional dan stabilitas ekonomi, bukan hanya sekadar privasi individual.	April 2022 Berdasarkan Putusan ini, tindakan Hiq Labs Inc. melakukan data scraping dari situs web publik (LinkedIn) yang tersedia untuk umum tidak dianggap sebagai pelanggaran 1030 CFAA. Namun, Pengadilan menekankan bahwa analisisnya terbatas pada CFAA dan tidak berlaku untuk potensi klaim melalui regulasi lain seperti pelanggaran hak cipta, pelanggaran kontrak, atau pelanggaran hak privasi. Pertimbangan yang penting untuk analisis ini meliputi (i) sifat data; (ii) dari mana data tersebut dikumpulkan; dan (iii) bagaimana data tersebut dikumpulkan.[36]

36 Erin Hanson, "Web Scraping, Website terms and The CFAA: hiQ's preliminary injuction affirmed again under van buren", https://www.whitecase.com/insight-our-thinking/web-scraping-website-terms-and-cfaa-hiqs-preliminary-injunction-affirmed-again, diakses pada 15 Desember 2025.

Negara	Pengaturan Negara Lain	Catatan Pasal	Contoh Implementasi
	sesuai dengan akses yang diizinkan, dan dengan demikian memperoleh informasi yang terdapat dalam catatan keuangan lembaga keuangan, atau penerbit kartu sebagaimana didefinisikan dalam bagian 1602(n) dari judul 15, atau yang terdapat dalam berkas lembaga pelaporan konsumen tentang konsumen, sebagaimana istilah tersebut didefinisikan dalam Undang-Undang Pelaporan Kredit yang Adil (15 U.S.C. 1681 et seq.); (3) dengan sengaja, tanpa izin untuk mengakses komputer departemen atau lembaga Amerika Serikat, mengakses komputer departemen atau lembaga tersebut yang secara eksklusif digunakan oleh Pemerintah Amerika Serikat atau, dalam hal komputer yang tidak secara eksklusif digunakan untuk tujuan tersebut, digunakan oleh atau untuk Pemerintah Amerika Serikat dan tindakan tersebut memengaruhi penggunaan atau pengoperasian komputer tersebut oleh Pemerintah,		

Negara	Pengaturan Negara Lain	Catatan Pasal	Contoh Implementasi
	(4) dengan sadar dan dengan maksud untuk menipu, mengakses komputer kepentingan Federal tanpa izin, atau melampaui akses yang diizinkan, dan dengan tindakan tersebut memajukan penipuan yang dimaksud dan memperoleh sesuatu yang berharga, kecuali objek penipuan dan hal yang diperoleh hanya terdiri dari penggunaan komputer; (5) dengan sengaja mengakses komputer kepentingan Federal tanpa izin, dan melalui satu atau lebih tindakan tersebut mengubah, merusak, atau menghancurkan informasi dalam komputer kepentingan Federal tersebut, atau mencegah penggunaan yang sah atas komputer atau informasi tersebut, dan dengan demikian (A) menyebabkan kerugian kepada satu atau lebih orang lain dengan nilai total $1.000 atau lebih selama periode satu tahun; atau		

Negara	Pengaturan Negara Lain	Catatan Pasal	Contoh Implementasi
	(B) memodifikasi atau merusak, atau berpotensi memodifikasi atau merusak, pemeriksaan medis, diagnosis medis, pengobatan medis, atau perawatan medis dari satu atau lebih individu; (6) dengan sengaja dan dengan maksud untuk menipu memperdagangkan (sebagaimana didefinisikan dalam pasal 1029) kata sandi atau informasi serupa yang melaluinya komputer dapat diakses tanpa izin, jika (A) perdagangan tersebut memengaruhi perdagangan antar negara bagian atau luar negeri; atau (B) komputer tersebut digunakan oleh atau untuk Pemerintah Amerika Serikat;		

Negara	Pengaturan Negara Lain	Catatan Pasal	Contoh Implementasi
Irlandia **Criminal Justice (Offences Relating to Information Systems) Act 2017**	Pasal 2: Akses tidak sah Seseorang dinyatakan bersalah apabila, tanpa otoritas atau alasan yang sah, dengan sengaja mengakses sistem informasi dengan cara melanggar ketentuan keamanan Pasal 3: Intervensi terhadap sistem informasi Seseorang dinyatakan bersalah apabila, tanpa otoritas yang sah, dengan sengaja menghalangi atau mengganggu fungsi dari sistem informasi dengan cara: (a) Memasukkan data ke dalam sistem, (b) Melakukan transmisi, merusak, menghapus, mengubah atau memperkecil, atau menyebabkan berkurangnya, data pada sistem, atau	Pasal 3 dari UU ini memiliki rumusan yang mirip dengan unsur perbuatan pada Pasal 32 ayat (1) UU ITE (terutama dengan adanya unsur transmisi). Namun, unsur transmisi ini hanya terdapat pada Pasal 3 yang mengatur tindak pidana *system interference* dan bukan *data interference*. Transmisi dalam hal ini adalah perbuatan mentransmisi data dengan tujuan membuat terganggunya fungsi sistem informasi. Unsur transmisi tidak terdapat pada Pasal 4 UU ini yang mengatur tentang *data interference*.	Terdapat satu contoh putusan yang menggunakan Pasal 2 dan 3 dari UU ini yakni kasus David Young. Ia diadili di Cork District Court atas perbuatan mengakses sistem informasi terkait sistem parkir milik Vodafone Data Centre di Clonshaugh Business and Technology Park, Dublin pada 2019. Young juga terbukti melakukan pengancaman terhadap Park Magic Mobile Solutions dengan tujuan mendapatkan informasi akun pelanggan.[37]

37 Oliver Kelleher, "Man (28) charged under anti-computer crime legislation", https://www.thejournal.ie/man-28-charged-under-anti-computer-crime-legislation-5349146-Feb2021/, diakses pada 20 Februari 2026.

Negara	Pengaturan Negara Lain	Catatan Pasal	Contoh Implementasi
	(c) Membuat data pada sistem menjadi tidak bisa diakses. Pasal 4: Intervensi terhadap data Seseorang dinyatakan bersalah apabila, tanpa otoritas yang sah, dengan sengaja menghapus, merusak, mengubah atau memperkecil, atau membuat tidak dapat diaksesnya, atau menyebabkan berkurangnya, data pada sistem informasi.		
Filipina **Cybercrime Prevention Act 2012 (Republic Act 10175)**	Section 4: Tindak Pidana Siber (a)(1) Illegal Access – akses tanpa hak terhadap keseluruhan atau suatu bagian dari sistem komputer. (a)(3) Data Interference — dengan sengaja atau secara lalai melakukan perubahan, merusak, menghapus, atau mengurangi data komputer, dokumen elektronik, atau pesan elektronik, secara tanpa hak, termasuk memasukkan atau mentransmisikan virus. Section 8: Sanksi	Pasal *data interference* dalam UU ini memuat salah satunya unsur perbuatan mentransmisikan namun secara spesifik mentransmisikan virus yang dapat mengancam integritas data.	Tim peneliti belum mendapatkan contoh putusan menggunakan pasal *data interference* ini mengingat tidak semua putusan tingkat pengadilan regional dipublikasikan. Namun, dalam Putusan Mahkamah Agung Filipina pada kasus Disini v. Secretary of Justice (GR No. 203335,February 11, 2014), beberapa pasal dalam UU ini diajukan untuk uji materil.

Negara	Pengaturan Negara Lain	Catatan Pasal	Contoh Implementasi
	Setiap orang yang terbukti bersalah atas tindak pidana yang diatur dalam Section 4(a) dan 4(b) dari UU ini dihukum dengan pidana penjara mayor (rentang 6-12 tahun) dan/atau denda minimum ₱ 200,000.00 dan maksimum yang dapat menggantikan kerugian yang disebabkan oleh tindakannya Sanksi tambahan dikenakan apabila sasaran dari perbuatan pidana adalah infrastruktur yang penting.		Salah satunya adalah pasal *illegal access* dan *data interference* yang dinilai berpotensi melanggar HAM. Mahkamah Agung Filipina memutus bahwa kedua pasal tersebut tidak berpotensi melanggar hak konstitusional maupun HAM, khususnya kebebasan berekspresi sehingga tidak perlu diatur prinsip *strict scrutiny* dalam implementasi pasal-pasal ini. Selain itu, Mahkamah Agung Filipina menyatakan bahwa klaim para pemohon bahwa pasal *data interference* membuka ruang tafsir yang terlalu luas berpotensi menimbulkan "chilling effect" tidak tepat karena ketentuan pidana pada umumnya memang dibuat untuk mencegah orang berbuat pidana dan para pemohon dinilai tidak dapat membuktikan klaim bahwa pasal tersebut membuka potensi penafsiran yang luas.[38]

38 Philippines Supreme Court, *Disini, Jr., et al. vs. The Secretary of Justice, et al.*, G.R. No. 203335, 18 February 2014, hal. 35.

Berdasarkan contoh-contoh instrumen internasional yang mengatur tindak pidana siber, dapat dilihat bahwa Budapest Convention dan UN Convention on Cybercrime memiliki pengaturan yang sejalan terkait perbuatan yang termasuk dalam tindakan *illegal access* maupun *data interference.* Kedua instrumen ini banyak dijadikan sebagai acuan negara-negara dalam mengatur *illegal access* dan *data interference.* Namun, mengingat kedua instrumen ini adalah panduan, maka negara-negara yang menjadikannya sebagai panduan tidak perlu mengatur ketentuan yang sama persis dengan instrumen tersebut. Sebagai contoh, Amerika dan Inggris mengatur ketentuan-ketentuan terkait *data interference* yang didahului dengan tindakan *illegal access.* Namun, jika di Inggris tidak secara spesifik mengatur *illegal access* dan *data interference* terhadap data milik Negara atau perbankan, Amerika justru mengatur secara spesifik ketentuan tersebut untuk melindungi integritas data yang terkait pertahanan dan keamanan negara, pemerintah, maupun data fiskal atau perbankan. Berbeda dengan Inggris dan Amerika Serikat, Irlandia dan Filipina memisahkan pasal pidana yang mengatur *illegal access* dari *data interference.*

Terlepas dari perbedaan pengaturan tersebut, dari segi rumusan terlihat kesamaan tujuan dan beberapa unsur antara pasal pidana *data interference* di negara-negara tersebut dengan Budapest Convention. Hal ini menunjukkan, penggunaan instrumen seperti Budapest Convention sebagai acuan dalam menyusun regulasi menjadi penting agar rumusan pasal terkait *illegal access* dan *data interference* tersebut tidak rancu dan sejalan dengan tujuan yang ingin dicapai dari keberadaan pasal *data interference* yakni pelindungan integritas dan fungsi data. Dengan ini, tim peneliti menggunakan Budapest Convention sebagai salah satu alat utama untuk menganalisis rumusan dan implementasi dari Pasal 32 UU ITE. Pasca beberapa kali perubahan pasal-pasal multitafsir, rumusan pasal lain dalam UU ITE digunakan sebagai alat baru untuk membatasi hak masyarakat atas ekspresi dan berpendapat, yaitu Pasal 32 UU ITE. Hal ini teridentifikasi di antaranya dengan kemunculan sejumlah laporan dan pengaduan dari masyarakat sipil kepada LBH Pers dan beberapa organisasi yang fokus dalam memberikan bantuan hukum bagi kelompok minoritas rentan. Berikut penjabaran lebih lanjut terkait beberapa kasus dan pendampingan dengan penggunaan Pasal 32 UU ITE.

3

SITUASI PENERAPAN PASAL 32 UU ITE BERDASARKAN PENDAMPINGAN KASUS DI LAPANGAN

3.1 FENOMENA PENGGUNAAN PASAL 32 UU ITE YANG MENGANCAM EKSPRESI WARGA NEGARA

a. Pemidanaan whistleblower

Pada awal 2025, LBH Bandung menerima pengaduan dari seseorang berinisial TY, seorang mantan pekerja Badan Amil Zakat Nasional (BAZNAS) Provinsi Jawa Barat dan pernah menjabat sebagai Kadiv Penghimpunan, Kepala Pelaksana, Kadiv Pendistribusian dan Pendayagunaan, Kepala Satuan Kepatuhan dan Audit Internal, Kadiv Program dan Development, dan Staf Ahli Ketua Baznas Jabar. Pada Januari 2024, TY melaporkan dugaan penyelewengan dana hibah senilai 11,7 Miliar ke Inspektorat Pemprov Jawa Barat.[39] Pihak Inspektorat meminta TY untuk melengkapi barang bukti. Dalam laporan ke Inspektorat Jawa Barat tersebut, TY melampirkan dokumen bukti berupa laporan pertanggungjawaban dana hibah Belanja Tidak Terduga (BTT) APBD Provinsi Jawa Barat Tahun 2020 yang berisi surat penawaran giro bank, SK pedoman penyaluran, SK struktur panitia penyaluran bantuan COVID-19, nota dinas, dll. Dokumen ini kemudian menjadi alat bukti di Polda Jawa Barat dan dianggap sebagai dokumen rahasia.

---

39 LBH Bandung, "Hentikan Upaya Kriminalisasi Whistleblower Dugaan Korupsi Baznas Jabar Rp13,3 M", https://www.lbhbandung.or.id/baznas-jabar-harus-bertanggung-jawab-atas-kriminalisasi-dan-perlindungan-terhadap-whistleblower/, diakses pada November 2025.

Akibat tindakan tersebut, pada Jumat, 7 Februari 2025, TY mendapatkan surat undangan klarifikasi dari Dit Ressiber Polda Jabar dengan tuduhan Pasal 48 *jo.* Pasal 32 ayat (1) dan (2) UU ITE perihal tindak pidana *illegal access*. Pada 15 Mei 2025, TY ditetapkan sebagai tersangka dan diperiksa sebagai tersangka karena dianggap menyebarluaskan data BAZNAS JABAR yang bersifat rahasia, sebagaimana Penetapan Ketua BAZNAS JABAR No. 93 tahun 2022 tentang klasifikasi informasi yang dikecualikan, salah satunya dokumen yang dikirim oleh TY.

Mengingat adanya kejanggalan terhadap proses penetapan tersangka tersebut, TY bersama LBH Bandung melayangkan permohonan perlindungan hukum kepada Lembaga Perlindungan Saksi dan Korban (LPSK), sebagaimana diatur dalam Peraturan Lembaga Perlindungan Saksi dan Korban Nomor 2 Tahun 2024 tentang Pengelolaan Pengaduan Pelayanan Publik dan *Whistleblowing System* di Lingkungan Lembaga Perlindungan Saksi dan Korban.[40]

b. Pemidanaan korban kekerasan dalam rumah tangga (KDRT)

Kasus serupa juga dialami oleh seorang dokter gigi berinisial AN yang merupakan korban kekerasan dalam rumah tangga (KDRT) oleh seorang anggota TNI Angkatan Darat. Sebab permasalahan kekerasan dalam rumah tangga tersebut, AN mencari keadilan dengan memberikan kuasa kepada kuasa hukum untuk mengungkap kasus perselingkuhan suaminya. Akan tetapi, niat AN tersebut disalahgunakan oleh kuasa hukum yang menyebabkan AN ditetapkan sebagai tersangka pada April 2024 atas tindak pidana dalam Pasal 48 ayat (1) *jo.* Pasal 32 ayat (1) UU ITE *jo.* Pasal 55 ayat (1) ke-1 KUHP. Sama halnya dengan TY, AN mengajukan permohonan perlindungan dari LPSK dan mendapatkan surat perlindungan hukum tersebut. Hingga kajian ini dibuat, kasus TY dan AN masih menggantung di kepolisian dan keduanya masih berstatus sebagai tersangka.

c. Pemidanaan pada praktik timpa teks digital

Kejanggalan dalam penggunaan Pasal 32 UU ITE kembali ditemukan pada praktik penangkapan dan penahanan[41] yang dilakukan oleh aparat kepolisian sehubungan dengan aksi demonstrasi pada 25 dan 27 Agustus 2025. Salah satu kasus yang

---

40 Disampaikan pada sesi FGD bersama pendamping hukum dan organisasi masyarakat sipil pada 29 September 2025.

41 Ady Thea DA, "Ratusan Demonstran Ditangkap, YLBHI: Pengamanan Aparat Berlebihan dan Represif", https://www.hukumonline.com/berita/a/ratusan-demonstran-ditangkap--ylbhi--pengamanan-aparat-berlebihan-dan-represif-lt66c7f947ea9ab/, diakses pada November 2026.

didampingi oleh Tim Advokasi Untuk Demokrasi (TAUD) adalah KA, seorang jurnalis dan aktivis media sosial dengan akun Instagram @aliansimahasiswapenggugat. Sebagai jurnalis dan aktivis, KA kerap menggunakan platform media sosial untuk membuat konten pendidikan publik perihal isu hak asasi manusia dan demokrasi. Penangkapan dilatarbelakangi oleh konten "timpa teks"[42] KA, yaitu KA melakukan tangkapan layar (*screenshot)* terhadap suatu artikel berita oleh Redaksi Kota yang terbit pada Selasa, 26 Agustus 2025 pada sebuah situs web perusahaan media mengenai salah satu tokoh gerakan yang berjudul "*Said Iqbal Tegaskan agar Anarko, Pelajar & BEM Jangan Gabung Aksi 28 Agustus: Ini Murni Isu Buruh! .....*". KA kemudian melakukan proses penyuntingan judul berita tersebut menjadi "*Said Iqbal Tegaskan agar Anarko, Pelajar & BEM Segera Gabung Aksi 28 Agustus: Ini Murni Gerakan Rakyat Indonesia!"* dengan menggunakan akun penyuntingan komersial, lalu mempublikasikan kembali potongan tangkapan layar tersebut melalui akun Instagramnya. Dalam Putusan Sela Perkara Nomor 757/Pid. Sus/2025/PN Jkt.Pst, Majelis Hakim menyatakan surat dakwaan Penuntut Umum Nomor Register Perkara PDM 84/M.1.10/Eku.2/10/2025 tanggal 10 Desember 2025 batal demi hukum karena dalil Dakwaan Pertama, Kedua dan Ketiga Penuntut Umum tidak cermat dan tidak jelas dalam menguraikan diksi "Aplikasi Canva atau Aplikasi Lainnya" sebagai syarat bagaimana suatu tindak pidana dilakukan. Akan tetapi, Jaksa Penuntut Umum (JPU) melimpahkan Dakwaan Ulang dalam kasus yang sama, namun kali ini menggunakan Pasal 32 ayat (2) UU ITE sebagai dakwaan pertama.[43]

Penerapan Pasal 32 UU ITE pada tindakan KA merupakan kekeliruan dalam menginterpretasikan delik pidana dalam pasal dan dalam menilai tindakan ekspresi warga negara yang sah. Tindakan yang dilakukan KA tersebut merupakan bentuk protes yang sah, yang memuat kekecewaan KA terhadap pernyataan atau

---

42 Praktik timpa teks lazim digunakan dalam ekosistem digital sebagai bentuk ekspresi dan penyebarluasan informasi di masyarakat. Pengunggahan kembali konten yang telah disunting menggunakan metode timpa teks dapat memuat ragam informasi, mulai dari konten humor hingga kritik publik yang bersifat satir terhadap kebijakan dan tindakan para pejabat negara. Metode timpa teks dilakukan dengan berbagai alat dan media yang dapat dioperasikan secara langsung di dalam platform atau melalui aplikasi penyuntingan dari pihak ketiga. Berangkat dari kemunculannya sebagai ruang berekspresi masyarakat di internet (warganet), praktik timpa teks berkaitan erat dengan kultur komunitas yang menciptakan ruang aman bagi warganet dalam berekspresi. Hal ini dapat ditemui salah satunya dalam komunitas *Timpa Teks: Singularity* di Facebook (https://www.facebook.com/groups/SpOotaXxkEerR/?locale=id_ID) yang melahirkan bahasa dan humor baru sebagai ruang berekspresi warganet.

43 Tempo.co, "Khariq Anhar Didakwa Lagi Pekan Depan", https://www.tempo.co/hukum/khariq-anhar-didakwa-lagi-pekan-depan-2112658, diakses pada hari 20 Februari 2026.

seruan dari seorang tokoh gerakan buruh yang mengecualikan kelompok gerakan masyarakat sipil tertentu.

3.2 PENGUJIAN KONSTITUSIONALITAS PASAL 32 UU ITE

Jauh sebelum tiga peristiwa pemidanaan menggunakan Pasal 32 tersebut terjadi, berdasarkan analisis dari dosen hukum tata usaha negara Violla Reininda, masyarakat sipil telah memohonkan uji konstitusionalitas Pasal 32 ayat (1) dan (2) UU ITE ke MK, yaitu sebagai berikut.

Tabel 3.1: Rincian Putusan MK terkait Uji Materil Pasal 32 UU ITE

Permohonan Pertama	
Putusan	Putusan MK Nomor 78/PUU-XVII/2019, 29 September 2020
Pemohon	PT. Nadira Intermedia Nusantara (Lembaga Penyiaran Berlangganan)
Pasal yang Diuji	Pasal 32 ayat (1) UU ITE (transmisi); Pasal 25 ayat (2) huruf a UU 28/2014 tentang Hak Cipta (hak ekonomi lembaga penyiaran untuk melaksanakan sendiri, memberi izin atau melarang pihak lain melakukan, salah satunya penyiaran ulang)
Batu Uji	Pasal 28D Ayat (1) tentang kepastian hukum yang adil Pasal 28F menghilangkan hak atas informasi
Tentang	► Larangan transmisi dalam Pasal 32 ayat (1) UU ITE- ► Larangan untuk menyimpan, mengolah, dan menyampaikan informasi yang dijamin Pasal 28F UUD 1945
Pertimbangan Hukum	Lembaga Penyiaran Berlangganan memiliki IPP tetap berpotensi untuk dikenakan sanksi pidana dan sanksi administrasi. Ada keterputusan pembacaan norma UU ITE dan UU Penyiaran.-Keharusan menyediakan paling sedikit sepuluh per seratus dari kapasitas kanal saluran untuk menyalurkan program dari LPP dan LPS merupakan keharusan menyediakan ruang siar, tidak mencakup makna bahwa program dari LPP dan LPS dapat disiarkan oleh LPB.-Pasal yang diuji tidak menutup hak untuk menyimpan, mengolah, dan menyampaikan informasi.
Amar Putusan	Menolak untuk seluruhnya.

Permohonan Kedua	
Putusan	Putusan MK Nomor 17/PUU-XIX/2021, 29 September 2021
Pemohon	Perseorangan (Rosiana Simon dan Kok An)
Pasal yang Diuji	Pasal 32 ayat (1), (2), dan (3); Pasal 48 ayat (1), (2), dan (3) UU ITE
Batu Uji	Pasal 28D Ayat (1); Pasal 28G Ayat (1) (pelindungan kehormatan diri pribadi)
Tentang	Kewajiban pekerja untuk merahasiakan informasi perusahaan
Pertimbangan Hukum	► Dapat diuji mengingat terdapat perbedaan dasar pengujian (Pasal 28G Ayat (1) UUD 1945) ► Tidak ada masalah konstitusionalitas tentang pelindungan data pribadi. ► MK memperluas penafsiran konstitusi dengan menyinggung Pasal 28D Ayat (2) UUD 1945 tentang perlakuan yang adil dan layak dalam hubungan kerja.
Amar Putusan	Menolak Permohonan.

Pertimbangan Majelis Hakim MK pada permohonan kedua memuat sejumlah pertimbangan penting, khususnya yang berkaitan dengan kerahasiaan data atau informasi perusahaan. Pertimbangan ini menjadi penting karena merefleksikan relevansi kasus-kasus yang didampingi di lapangan, yang tidak jauh dengan hubungan pekerja dengan perusahaan.

Dalam pertimbangannya, Majelis Hakim MK mengakui adanya kejanggalan[44] dalam perumusan Pasal 32 UU ITE yang terdiri dari delik formil dan delik materiil. Ayat (1) dan ayat (2) dari Pasal 32 merupakan delik formil yang melarang dilakukannya suatu perbuatan/tindakan, sementara ayat (3) merupakan delik materiil yang mengatur bahwa suatu perbuatan atau tindakan menjadi terlarang jika menimbulkan akibat tertentu. Dari unsur-unsur tersebut, Mahkamah berpendapat bahwa unsur delik yang berkaitan dengan akses atas hasil kinerja dalam suatu hubungan kerja adalah unsur delik "tanpa hak atau melawan hukum". Unsur delik "tanpa hak atau melawan hukum" inilah yang menurut Mahkamah berpotensi merugikan hak konstitusional

44 Mahkamah Konstitusi, "RINGKASAN PERMOHONAN PERKARA Nomor 17/PUU-XIX/2021: Pemindahan Informasi Elektronik Perusahaan Dapat Dipidana Menurut Undang-Undang Tentang Informasi dan Transaksi Elektronik," https://www.mkri.id/public/content/persidangan/resume/resume_perkara_2299_Perkara%20No.%2017.pdf, diakses pada November 2025.

para pemohon, khususnya ketika para pemohon dihadapkan pada kasus konkret, yaitu diperiksa sebagai saksi dalam dugaan pencurian data perusahaan.

Majelis berpendapat bahwa, dalam suatu skema hubungan kerja, pengaturan Pasal 32 UU ITE berada di tengah tarik-menarik antara kebutuhan pemberi kerja untuk merahasiakan hasil kerja, dengan kebutuhan pekerja untuk membuktikan kontribusinya atas suatu hasil kerja.[45] Kehendak pemberi kerja agar hasil kerja dirahasiakan, bahkan oleh pekerja yang ikut mengerjakan hal tersebut, dapat dimengerti dalam konteks kebutuhan pemberi kerja untuk, antara lain, merumuskan strategi maupun inovasi dalam menghadapi dan bertahan dalam persaingan bisnis. Pada sisi pekerja, ketatnya kerahasiaan hasil kerja dapat mengakibatkan kesulitan pekerja dalam membuktikan kinerjanya. Sebaliknya, tidak adanya kerahasiaan atas suatu hasil kerja akan memudahkan bagi pekerja untuk membuktikan kinerjanya. Namun dari sisi pemberi kerja, terutama jika pemberi kerja adalah badan usaha yang bekerja untuk mencari untung (*profit-oriented*), ketiadaan rahasia atas hasil kerja dapat mengakibatkan kegagalan strategi dan inovasi yang dapat menghilangkan daya kompetisinya.

Kondisi tarik-menarik antara kebutuhan pemberi kerja dengan pekerja semakin kompleks karena acapkali hasil kerja tersebut berada dalam penguasaan sepenuhnya pemberi kerja, dan kemudian sifat kerahasiaannya diperjanjikan secara hukum antara pemberi kerja dengan penerima kerja dalam sebuah kontrak kerja atau perjanjian yang sejenis.[46] Sehingga, jamak muncul pemahaman bahwa ketika pekerja mengakses hasil kerjanya, sementara di saat yang sama hasil kerja demikian merupakan rahasia perusahaan/pemberi kerja, lantas pekerja yang bersangkutan dianggap melanggar hak pemberi kerja dan karenanya pekerja yang bersangkutan dianggap melakukan perbuatan melawan hukum.

Masih berkaitan dengan konteks pertimbangan MK, berdasarkan FGD yang dilakukan oleh tim penulis, terdapat beberapa praktik kriminalisasi yang terjadi dalam kurun beberapa tahun belakangan, yang bersinggungan dengan isu ketenagakerjaan dan konten publikasi digital, sebagai berikut.

---

45 Putusan Mahkamah Konstitusi Nomor 17/PUU-XIX/2021, Poin [3.15.2], Paragraf 1, hal.34.

46 *Ibid.*, Paragraf 3.

Tabel 3.2: Daftar Kasus dengan Kriminalisasi Pasal 32 UU ITE

Nama Korban	Delik Pidana	Kronologi Singkat	Perkembangan Kasus
AS[47]	Pasal 32 ayat (1) UU ITE	AS dinilai menyebarkan materi mengandung konten yang bermasalah perihal ijazah palsu mantan presiden Indonesia, Joko Widodo. AS menjadi salah satu *host* dalam *podcast*-nya yang membahas perihal kasus tersebut.	Kasus *undue delay* karena pasca undangan klarifikasi, yang artinya kasus masih dalam proses penyelidikan di Bareskrim.
MY[48]	Pasal 32 ayat (1) UU ITE	Terjadi pada penangkapan pasca demonstrasi pada bulan Agustus 2025. MY ditangkap dengan menggunakan delik Pasal 32 ayat (1) UU ITE, akan tetapi dakwaan berubah menjadi Pasal 28 ayat (2) UU ITE. Adapun tindakan aktual yang dilakukan adalah "menempelkan poster" yang bertuliskan "*ALL COPS ARE BASTARD 1312*" dan "*THE WORST CHOICE IN LIFE IS TO BECOMING A FUCKING COPS*". Terdapat 2 (dua) orang teman MY yang kemudian melakukan dokumentasi dalam bentuk video atas tindakan penempelan tersebut, dan kemudian mempublikasikannya lewat media sosial tanpa seizin MY. Akan tetapi, kedua orang yang melakukan perekaman tersebut bahkan tidak dihadirkan sebagai saksi di dalam persidangan dan tidak dijadikan tersangka dengan UU ITE.	Nomor perkara 563/PID.SUS/2025/ PN CBI dengan tuntutan 1 (satu) tahun 3 (bulan) penjara dan Majelis Hakim memutus 6 (enam) bulan masa percobaan.

47 Disampaikan pada sesi FGD bersama pendamping hukum…, *Loc. Cit.*

48 *Ibid.*

Nama Korban	Delik Pidana	Kronologi Singkat	Perkembangan Kasus
I[49]	Pasal 32 ayat (1) UU ITE	I merupakan seorang konten kreator yang kerap menyampaikan kritik terhadap pejabat publik di media sosial yang dikemas sebagai guyonan. Masih dalam rangkaian protes pada akhir Agustus lalu, I mengunggah sebuah foto dari hasil *generative* AI yang menampilkan dirinya dan seorang pejabat publik. Atas unggahannya tersebut, I dilaporkan oleh pejabat publik yang bersangkutan di Unit Siber Polda Metro Jaya dengan tuduhan menggunakan Pasal 32 ayat (1) UU ITE.	I telah diperiksa dengan status sebagai saksi pada tahap penyidikan oleh pihak kepolisian pada awal September dan telah dilakukan upaya paksa berupa penyitaan terhadap telepon seluler, akun email, dan akun media sosial. Sampai dengan tulisan ini disusun, masih belum ada perkembangan maupun kejelasan lebih lanjut dari perkara yang menimpa I ini.
LF[50]	Pasal 32 ayat (1) UU ITE	LF Repost konten video dari akun kolektifa di *instastory* Instagram Terdakwa dengan caption *"most corrupt most useless most sickening disgusting stupid and morally bankrupt institution EVER. Fuck the police literally yall are just a bunch of dumbfucks and i hope every single one of you and your bloodline rots in the deepest hell. Ya allah i'm so mad."* Selain itu, Terdakwa juga me-*repost* unggahan dari akun @pandemictalks, berisi kalimat tentang almarhum Affan Kurniawan, "*Rajin, tulang*	Saat tulisan ini disusun, perkara sudah selesai pemeriksaan di pengadilan tingkat pertama dengan putusan Pengadilan Negeri Jakarta Selatan No.675/Pid. Sus/2025/PN JKT. SEL. Amar putusan kasus ini adalah menjatuhkan pidana 6 (enam) bulan penjara

49 *Ibid.*

50 *Ibid.*

Nama Korban	Delik Pidana	Kronologi Singkat	Perkembangan Kasus
		punggung keluarga yang tinggal di kontrakan 3x11 meter bersama 7 orang keluarga" dan menambahkan tulisan yang berisi "*Innalillahi wa innailaihi roji'un*" sebagai bentuk belasungkawa. Terdakwa juga mengunggah foto *story* Instagram yang dilakukan di gedung ASEAN *Inter Parliamentary Assembly* (AIPA) dengan gaya tangan menunjuk ke gedung Mabes Polri menggunakan *caption "when your office is right next to the national police headquarters. Please burn this building down and get them all yall i wish i could help throw some stones but my mom wants me home. Sending strength to all the protesters!!"*.	kepada LF berdasarkan Pasal 45A ayat (2) *jo.* Pasal 28 ayat (2) UU ITE, namun pidana penjara ini diganti dengan pidana pengawasan.

3.3 PENGGUNAAAN PASAL 32 UU ITE SEBAGAI ANCAMAN TERHADAP KEBEBASAN BEREKSPRESI DAN BERPENDAPAT

Berdasarkan informasi dan data yang diperoleh melalui kegiatan FGD pada 29 September 2025, tim penulis menemukan adanya indikasi penggunaan Pasal 32 UU ITE sebagai delik multitafsir yang berpotensi menjerat kebebasan berekspresi. Temuan ini didasarkan pada analisis teori kriminalisasi sebagaimana dirumuskan oleh Justin Miller (1934) dan Anugerah Rizki Akbari (2015). Dengan mempertimbangkan karakteristik hukum pidana yang bersifat memaksa serta keberadaan berbagai instrumen koersif yang dimilikinya, kriminalisasi kerap digunakan oleh pemerintah sebagai strategi yang efektif untuk mengontrol kehidupan sosial. Pola demikian tercermin dalam praktik penerapan dan implementasi Pasal 32 UU ITE oleh APH.

Lebih lanjut, Von Hirsch melalui teori *ordinal proportionality of punishment* menegaskan bahwa sanksi pidana harus dirumuskan secara sistematis dan mengikuti skala keseriusan tindak pidana. Dalam konteks Pasal 32 ayat (1) dan (2) UU ITE, tujuan pengaturan delik tersebut seharusnya dapat ditelusuri melalui

dokumen *Memorie van Toelichting* (MvT) pembentukan UU ITE. Namun demikian, hasil penelusuran tim penulis menunjukkan bahwa diskursus mengenai maksud dan rasionalitas pengaturan delik *a quo* tidak ditemukan secara eksplisit dalam dokumen MvT.

Apabila merujuk pada *Convention on Cybercrime* (ETS No. 185) sebagai landasan hukum internasional dalam perumusan pasal tersebut, delik *data interference* secara khusus dirancang untuk melindungi dan menjaga kerahasiaan, integritas, serta ketersediaan data dan sistem komputer. Konvensi ini juga secara tegas bertujuan melindungi tindakan-tindakan yang sah, termasuk aktivitas perancangan jaringan dan kegiatan lain yang berkaitan dengan pengoperasian sistem komputer. Namun, berdasarkan analisis terhadap praktik implementasi delik *data interference* dalam berbagai kasus yang telah diuraikan sebelumnya, ditemukan bahwa mayoritas pembuktian justru bertumpu pada Dokumen atau Informasi Elektronik berupa konten media sosial, bukan pada intervensi terhadap data yang berada di dalam sistem komputer, seperti situs web, aplikasi, atau infrastruktur digital lainnya. Padahal, tujuan utama pengaturan delik *data interference* adalah untuk menjaga integritas dan keutuhan data, sehingga data yang dimaksud seharusnya dipahami sebagai data asli (*original data*) yang tersimpan di dalam suatu sistem. Dengan demikian, konten media sosial, terlebih lagi konten yang merupakan hasil modifikasi, seperti penimpaan teks atau pengeditan menggunakan teknologi kecerdasan artifisial, tidak dapat serta-merta dikualifikasikan sebagai objek delik *data interference*. Selain itu, tindakan yang dilakukan oleh para korban dalam kasus-kasus tersebut juga tidak menimbulkan bahaya serius (*serious harm*) sebagaimana dipersyaratkan oleh Budapest Convention.

Kondisi ini menunjukkan adanya kesenjangan yang signifikan antara maksud pengaturan norma dan praktik penerapannya, di mana hukum yang seharusnya berfungsi sebagai instrumen perlindungan justru bertransformasi menjadi alat represi digital. Ketidakpahaman APH terhadap konteks, maksud, dan tujuan historis (*historical background*) pengaturan delik ini berkontribusi pada tingginya risiko kriminalisasi serta penyalahgunaan Pasal 32 UU ITE untuk membungkam ekspresi dan pendapat masyarakat.

Sebagai upaya mencegah praktik kriminalisasi dalam penerapan Pasal 32 ayat (1) dan (2) UU ITE, dalam FGD pada 13 November 2025, Dr. Vidya Prahassacitta, S.H., M.H. selaku Dosen Hukum Pidana Universitas Bina Nusantara merekomendasikan

perlunya penyisipan rumusan pengecualian pidana berupa alasan pembenar, khususnya untuk kepentingan hukum yang lebih besar, seperti kepentingan umum maupun kepentingan negara. Rekomendasi ini sejalan dengan beberapa putusan pengadilan yang amarnya membebaskan terdakwa dari dakwaan *data interference* demi kepentingan hukum yang lebih luas. Contoh putusan tersebut adalah Putusan Pengadilan Negeri Jakarta Selatan No. 1068/Pid.Sus/2020/PN JKT.SEL, yang memuat kasus terdakwa mengirimkan dokumen internal perusahaan yang dianggap rahasia kepada pihak eksternal melalui surat elektronik untuk memberitahukan adanya pelanggaran perjanjian kerja sama antar perusahaan. Selain itu, terdapat Putusan Mahkamah Agung No. 31 K/Pid.Sus/2017 yang memuat kasus perekaman ulang suatu video rekaman CCTV menggunakan *handphone* yang memperlihatkan kejadian hilangnya *handphone* milik terdakwa. Rekaman pada handphone tersebut kemudian disalin untuk digunakan sebagai bukti dalam laporan polisi atas dugaan tindak pidana pencurian.

4

SITUASI PENERAPAN PASAL 32 UU ITE BERDASARKAN PUTUSAN PENGADILAN

4.1 JENIS PERBUATAN YANG DIDAKWA DENGAN PASAL 32 AYAT (1) UU ITE

Dari 112 putusan yang menggunakan Pasal 32 ayat (1) UU ITE, tim peneliti mengambil 12 contoh putusan untuk melihat tren penggunaan Pasal 32 ayat (1) UU ITE dalam putusan. Dari 12 putusan tersebut, terdapat 3 klasifikasi berdasarkan kesesuaian antara perbuatan dalam fakta hukum dengan pertimbangan hakim dalam putusan yakni: (A) perbuatan yang menurut hakim memenuhi unsur tindak pidana Pasal 32 ayat (1) UU ITE dan diputus bersalah; (B) perbuatan yang tujuan perbuatannya bukan *data interference* atau belum memenuhi unsur Pasal 32 ayat (1) UU ITE namun diputus bersalah; dan (C) perbuatan yang memang tidak memenuhi unsur perbuatan dari Pasal 32 ayat (1) UU ITE dan diputus bebas. Kategori B terdiri dari 4 putusan yang unsur perbuatannya sebetulnya menyangkut hak berekspresi dan merupakan perbuatan yang lebih cocok diuji dengan pasal lain misal, pencemaran nama baik atau ujaran kebencian. Keterangan lebih lanjut dari jenis perbuatan dan beberapa informasi terkait lainnya dapat dilihat pada tabel berikut:

Tabel 4.1: Rincian Putusan Pasal 32 ayat (1) UU ITE

No.	Nomor Putusan	Dakwaan	Jenis Perbuatan	Amar Putusan
A.	Perbuatan-perbuatan yang memenuhi unsur tindak pidana Pasal 32 ayat (1) UU ITE dan diputus bersalah			
1	155/Pid. Sus/2023/PN Lmj	Dakwaan alternatif Pasal 32 ayat (1) *juncto* Pasal 48 ayat (1) UU No. 11 Tahun 2008 tentang ITE *juncto* Pasal UU No. 19 Tahun 2016 tentang Perubahan UU No. 11 Tahun 2008 tentang ITE *atau* Pasal 32 ayat (2) *juncto* Pasal 48 ayat (2) UU No. 11 Tahun 2008 tentang ITE *juncto* Pasal UU No. 19 Tahun 2016 tentang Perubahan UU No. 11 Tahun 2008 tentang ITE	Terdakwa melakukan peretasan terhadap situs web orang lain untuk diperjualbelikan. Peretasan dilakukan dengan *brute force* untuk memeroleh nama pengguna (*username*) dan kata sandi (*password*) dari situs web tersebut. Setelah berhasil masuk ke situs web tersebut, Terdakwa mengunggah fitur *shell backdoor* agar calon pembeli bisa mengakses dan mengambil alih situs web tersebut.	Pidana penjara 2 tahun dan denda Rp20.000.000 (Dakwaan alternatif kedua)
2	42/PID/2018/ PT BTN 3026 K/Pid. Sus/2018	Pasal 32 ayat (1) juncto Pasal 48 ayat (1) UU No. 11 Tahun 2008 tentang ITE	Terdakwa meminta data mutasi rekening bank suatu koperasi kepegawaian kepada mantan pengurus koperasi dan kemudian data tersebut dikirimkan melalui *email* kepada Terdakwa padahal Terdakwa bukan pengurus yang sah dari koperasi tersebut dan permintaan data tersebut terjadi tanpa pengetahuan dan izin dari pengurus koperasi	Pidana penjara 1 tahun 6 bulan

No.	Nomor Putusan	Dakwaan	Jenis Perbuatan	Amar Putusan
3	210/Pid. Sus/2021/PN JKT.SEL	*Primer* Pasal 32 ayat (2) juncto pasal 48 ayat (2) UU No. 19 Tahun 2016 tentang Perubahan Atas UU No. 11 Tahun 2008 tentang ITE juncto Pasal 55 ayat (1) ke-1 KUHP; *Subsider* Pasal 32 ayat (1) juncto Pasal 48 ayat (1) UU No. 19 tahun 2016 tentang Perubahan Atas UU No. 11 Tahun 2008 tentang ITE juncto Pasal 55 ayat (1) ke-1 KUHP	Terdakwa memberikan layanan pengecekan data informasi debitur (IDEB) melalui aplikasi SLIK OJK kepada pemesan. Akses terhadap aplikasi SLIK OJK dilakukan dengan perbantuan teman Terdakwa yang bekerja di bank dan memiliki otoritas mengakses aplikasi tersebut. Atas permintaan Terdakwa dari pemesanan pengecekan IDEB, teman Terdakwa mengakses SLIK OJK dan mengunduh IDEB. Hasil unduhan dibuat dalam bentuk tipe file PDF dan dikirim kepada Terdakwa melalui email, dengan mengedit dan menghapus nama user SLIK OJK teman Terdakwa. Terdakwa memasang tarif berupa uang tanda jadi dalam bentuk pulsa dari operator tertentu dan uang pelunasan dalam bentuk yang sama. Bayaran berupa pulsa ini kemudian dikonversi menjadi uang yang ditransfer ke rekening Terdakwa.	Pidana penjara 7 bulan dan denda Rp5.000.000 (Dakwaan subsider)
4	Tk. Pertama 284/ Pid.B/2012/ PN.DPK Tk. Banding 42/Pid/2018/ PT BTN	Pasal 363 ayat (1) ke-4 KUHP; Atau Pasal 50 juncto Pasal 22 huruf a, b UU No. 36 Tahun 1999 tentang Telekomunikasi; Atau	Terdakwa bersama dengan rekannya mengakses server suatu perusahaan telekomunikasi secara ilegal untuk kemudian membuat suatu aplikasi *logging* sehingga Terdakwa dapat mengisipulsa secara ilegal dan mendapatkan akses internet gratis ke nomor-	Pidana penjara 2 tahun dan denda Rp 50.000.000

No.	Nomor Putusan	Dakwaan	Jenis Perbuatan	Amar Putusan
		Pasal 46 ayat (3) juncto Pasal 30 ayat (3) UU No. 11 Tahun 2008 tentang ITE juncto Pasal 55 ayat (1) ke-1 KUHP; Atau Pasal 48 ayat (1) juncto Pasal 32 ayat (1) UU No. 11 Tahun 2008 tentang ITE juncto Pasal 55 ayat (1) ke-1 KUHP; Atau Pasal 51 ayat (2) juncto Pasal 36 juncto Pasal 34 ayat (1) huruf b UU No. 11 Tahun 2008 juncto Pasal 55 ayat (1) ke-1 KUHP	nomor seluler yang dimiliki Terdakwa sehingga menimbulkan kerugian bagi perusahaan tersebut	
5	41/Pid. Sus/2020/PN Mar	Dakwaan Subsidaritas *Primer* Pasal 32 ayat (1) *juncto* Pasal 48 ayat (1) UU No. 11 Tahun 2008 tentang ITE *Subsider* Pasal 30 ayat (1) *juncto* Pasal 46 ayat (1) UU No. 11 Tahun 2008 tentang ITE	Terdakwa mengakses situs web *e-dikbang* Polri dengan cara memasukkan nomor NRP Polri secara acak. Setelah berhasil masuk, Ramdan mengunggah file pengganti di situs web tersebut yang mengubah tampilan situs web dengan kalimat yang kurang lebih menyatakan bahwa, "Kasus Novel Baswedan Hanya Pengalihan Isu dari Kasus Mega Korupsi Jiwasraya". Terdakwa memberikan keterangan bahwa tujuan dari perbuatannya adalah untuk memberitahukan	Pidana penjara 1 tahun dan denda Rp50.000.000 (Dakwaan primer)

No.	Nomor Putusan	Dakwaan	Jenis Perbuatan	Amar Putusan
			polisi bahwa terdapat kelemahan dalam situs web kepolisian.	
6	Tk. Pertama 148/ Pid.B/2011/ PN.PLW Tk. Banding 3/Pid. Sus/2012/PTR	Dakwaan tunggal Pasal 32 ayat (1) UU No. 11 Tahun 2008 tentang ITE	Terdakwa merupakan *technical manager* perusahaan, yang masa kerjanya akan segera berakhir. Sebelum masa kerjanya berakhir, pihak perusahaan memeriksa laptop kantor yang biasanya digunakan Terdakwa saat bekerja. Dari pemeriksaan tersebut, pihak perusahaan mendapatkan bahwa laptop kantor Terdakwa pernah dihubungkan kepada beberapa perangkat elektronik, seperti external hardisk dan USB flashdisk milik Terdakwa. Terdakwa tanpa izin perusahaan memindahkan data perusahaan tersebut ke perangkat eksternal hardisk dan USB flashdisk milik dirinya dengan mengirim email dari email perusahaan ke email pribadi Terdakwa. Setelah diperiksa oleh pihak perusahaan, dalam perangkat external hardisk dan USB flashdisk Terdakwa terdapat data dan dokumen elektronik milik perusahaan. Data dan dokumen elektronik tersebut memuat informasi hasil riset pengembangan perusahaan.	Tk. pertama: Pidana penjara 3 tahun dan denda Rp100.000.000 Tk. banding:Pidana penjara 6 bulan dan denda Rp25.000.000
B	Perbuatan yang tujuannya bukanlah *data interference* namun diputus bersalah dengan Pasal 32 ayat (1) UU ITE			

No.	Nomor Putusan	Dakwaan	Jenis Perbuatan	Amar Putusan
1	390/Pid. Sus/2024/PN Dps	Dakwaan tunggal Pasal 48 ayat (1) *juncto* Pasal 32 ayat (1) UU No. 11 Tahun 2008 tentang ITE *juncto* Pasal 55 ayat (1) ke-1 KUHP	Terdakwa memiliki akun media sosial Instagram untuk membantu masyarakat melaporkan/ mempublikasikan kasus yang merugikan masyarakat yang bersangkutan. Media sosial ini terbuka untuk publik. Pada perkara di putusan, Terdakwa mengunggah kasus perselingkuhan pasangan dari seorang pelapor di media sosial tersebut. Unggahan tersebut terdiri dari foto beserta teks dan informasi pribadi seseorang yang menjadi selingkuhan pasangan pelapor. Foto dan informasi pribadi selingkuhan tersebut Terdakwa dapatkan dari pertukaran informasi dengan pelapor melalui DM Instagram dan WhatsApp.	Pidana penjara 5 tahun dan denda Rp5.000.000
2.	61/Pid. Sus/2020/ PN.Lbo	Dakwaan kumulatif *Kesatu* Pasal 48 ayat (1) *juncto* Pasal 32 ayat (1) UU No. 19 Tahun 2016 tentang Perubahan Atas UU No. 11 Tahun 2008 tentang ITE dan *Kedua* Pasal 45A ayat (2) *juncto* Pasal 28 ayat (2) UU	Lewat ponsel pribadi Terdakwa, Terdakwa mengakses akun media sosial Facebook seseorang tanpa izin, hanya karena Terdakwa yang membantu membuatkan akun tersebut. Melalui akun media sosial Facebook tersebut, Terdakwa mengambil foto seseorangyang sudah teredit dengan tato di kedua pipi foto orang tersebut, lalu mengunggah foto orang tersebut	Pidana penjara 7 bulan

No.	Nomor Putusan	Dakwaan	Jenis Perbuatan	Amar Putusan
		No. 19 Tahun 2016 tentang Perubahan Atas UU No. 11 Tahun 2008 tentang ITE	ke portal publik dengan keterangan teks yang pada intinya mengatakan bahwa seseorang dalam foto tersebut merupakan "tukang pukul", bahkan babinsa dan polisi menjadi korban.	
3	Tk. Pertama 959/Pid. Sus/2019/ PN.Jkt.Brt Tk. Banding 167/Pid. Sus/2020/ PT.DKI Tk. Kasasi 3518 K/Pid. Sus/2020	Dakwaan alternatif *Kesatu* Pasal 32 ayat (1) *juncto* Pasal 48 ayat (1) UU No. 19 Tahun 2016 tentang Perubahan Atas UU No. 11 Tahun 2008 tentang ITE atau *Kedua* Pasal 25 ayat (2) huruf a *juncto* Pasal 118 UU No. 28 Tahun 2014 tentang Hak Cipta	Terdapat dua terdakwa yang merupakan direktur utama dari masing-masing perusahaan penyiaran. Kedua perusahaan penyiaran di bawah koordinasi kedua terdakwa tersebut tanpa izin menayangkan siaran atau saluran RCTI, Global TV, MNC TV, dan iNews.	Tk. pertama, banding, dan kasasi: pidana penjara 2 tahun dan denda 500 juta rupiah (dakwaan kesatu)
4	869/ Pid.B/2017/ PN.JKT.SEL	Dakwaan alternatif Kesatu Pasal 363 ayat (1) ke-5 KUHP jo. Pasal 64 ayat (1) KUHPatau Kedua Pasal 48 ayat (1) jo. Pasal 32 ayat (1) UU ITE	Terdakwa selaku supervisor di perusahaan yang menyediakan jasa perawatan menteri SST (Self Service Terminal) bagi Bank CIMB Niaga memanfaatkan posisinya untuk mengakses data (nomor pin dan kartu ATM) nasabah Bank CIMB Niaga. Terdakwa menggandakan kartu	Pidana penjara 2 tahun dan 6 bulan serta denda 100 juta rupiah

No.	Nomor Putusan	Dakwaan	Jenis Perbuatan	Amar Putusan
			ATM yang berisikan data para nasabah dan menggunakannya untuk melakukan sejumlah transaksi.	
C	Perbuatan yang memang tidak memenuhi unsur perbuatan dari Pasal 32 ayat (1) UU ITE dan diputus bebas			
1	1068/Pid. Sus/2020/ PN JKT.SEL	Pasal 32 ayat (3) *juncto* Pasal 48 ayat (3) UU No. 11 Tahun 2008 tentang ITE; Subsidair Pasal 32 ayat (2) *juncto* Pasal 48 ayat (2) UU No.11 Tahun 2008 tentang ITE; Lebih subsidair Pasal 32 ayat (1) *juncto* Pasal 48 ayat (1) UU No. 11 Tahun 2008 tentang ITE;	Terdakwa mengirim kepada pihak eksternal suatu dokumen internal perusahaan yang dianggap rahasia melalui surat elektronik untuk memberitahukan adanya pelanggaran perjanjian kerjasama antar-perusahaan	Bebas
2	Tk. Pertama 175/Pid. Sus/2016/ PN.Jkt.Pst. Tk. Kasasi 31 K/Pid. Sus/2017	Dakwaan alternatif Kesatu Pasal 32 Ayat (1) *juncto* Pasal 48 Ayat (1) UU No. 11 Tahun 2008 tentang ITE;	Terdakwa melakukan perekaman dengan menggunakan *handphone* terhadap suatu video rekaman CCTV yang memperlihatkan kejadian hilangnya *handphone* milik Terdakwa di suatu ruangan. Kemudian, Terdakwa membuat salinan atas rekaman di *handphone* tersebut	Bebas

No.	Nomor Putusan	Dakwaan	Jenis Perbuatan	Amar Putusan
		atau Kedua Pasal 30 Ayat (1) *juncto* Pasal 46 Ayat (1) UU No. 11 Tahun 2008 tentang ITE	dan salinan tersebut digunakan sebagai bukti untuk membuat laporan polisi terkait dugaan pencurian	

Berdasarkan putusan-putusan tersebut, tim peneliti menjabarkan fakta hukum dari 8 putusan sebagai contoh dari keempat klasifikasi tersebut untuk memudahkan dalam memahami konteks perbuatan dan pertimbangan hakim dalam putusan. Penjabaran tersebut dibagi ke dalam 3 klasifikasi sebagaimana telah disebutkan sebelumnya:

A. Perbuatan yang menurut hakim memenuhi unsur tindak pidana Pasal 32 ayat (1) UU ITE dan diputus bersalah

1. Putusan Nomor 155/Pid.Sus/2023/PN Lmj

Pada perkara ini, Terdakwa AR melakukan peretasan website-website orang lain dengan cara melakukan *brute force* untuk memperoleh *username* dan *password* dari website-website tersebut. Setelah berhasil melakukan log in ke website-website tersebut, AR mengunggah *shell backdoor* agar calon pembeli bisa mengakses dan mengambil alih website-website tersebut. Website-website tersebut dijual oleh AR dengan rentang harga Rp25.000,- hingga Rp40.000,-. Setelah ada laporan peretasan dan penyalahgunaan data milik orang lain, AR ditangkap dan didakwa dengan dakwaan alternatif menggunakan Pasal 32 ayat (1) jo. Pasal 48 ayat (1) UU ITE **atau** Pasal 32 ayat (2) jo. Pasal 48 ayat (2) UU ITE.

Berdasarkan fakta-fakta hukum tersebut, majelis hakim menguraikan cara AR melakukan *illegal access* dan memodifikasi website-website yang diaksesnya dalam pertimbangan putusan. Oleh karena terbukti tanpa hak dan dengan sengaja melakukan *illegal access*, mengubah website, dan menjual website tersebut kepada pihak lain, AR dipidana penjara selama 2 tahun dan denda 20 juta rupiah berdasarkan Pasal 32 ayat (1) UU ITE.

2. Putusan Nomor 41/Pid.Sus/2020/PN Mar

Pada Desember 2019, Terdakwa RY mengakses website e-dikbang Polri dengan

cara memasukkan nomor NRP Polri secara acak. Setelah berhasil masuk, RY mengunggah file pengganti di website tersebut yang mengubah tampilan website dengan kalimat yang kurang lebih menyatakan bahwa, "Kasus Novel Baswedan Hanya Pengalihan Isu dari Kasus Mega Korupsi Jiwasraya". RY memberikan keterangan bahwa tujuan dari perbuatannya adalah untuk memberitahukan polisi bahwa terdapat kelemahan dalam website kepolisian. Setelah IP *address* RY dilacak, pihak kepolisian pun melaporkan RY. RY didakwa dengan dakwaan subsidair yakni, *primair*: Pasal 32 ayat (1) jo. Pasal 48 ayat (1) UU ITE dan *subsidair*: Pasal 30 ayat (1) jo. Pasal 46 ayat (1) UU ITE.

Dalam pertimbangannya, majelis hakim menyatakan bahwa sub unsur perbuatan dari Pasal 32 ayat (1) UU ITE bersifat alternatif sehingga ketika salah satunya terpenuhi maka sub unsur lain tak perlu dibuktikan. Kemudian, majelis hakim menggunakan penafsiran bahasa untuk mengurai definisi sub-sub unsur perbuatan dalam pasal tersebut. Berdasarkan definisi tersebut, majelis hakim menganalisis perbuatan RY yang mana RY dinyatakan telah mengakses dan mengubah tampilan website e-dikbang Polri dengan cara-cara yang sudah dijabarkan sebelumnya. Selain itu, majelis hakim pun menyatakan bahwa RY telah melakukan perbuatannya dengan sengaja dan ini terlihat dari langkah persiapan dan alat-alat yang digunakan oleh Terdakwa untuk melakukan perbuatannya. Dengan ini, RY diputus bersalah atas dakwaan primair dan dijatuhi pidana penjara 1 tahun dan denda lima puluh juta rupiah.

3. Putusan Nomor 03/Pid.Sus/2012/PTR

Berdasarkan surat dakwaan, Terdakwa RL yang menjabat sebagai Technical Manager di PT. RAPP mengirimkan data dari *email* perusahaan ke *email* pribadi. Saat diminta menyerahkan laptop dan *external hard disk*, ditemukan sejumlah data milik PT. RAPP dalam kedua alat tersebut. Dalam pembelaannya, RL menyatakan bahwa ia hanya berniat melakukan pencadangan atas data-data tersebut dan tidak memiliki niat untuk merugikan perusahaan. RL kemudian didakwa dengan dakwaan tunggal menggunakan Pasal 32 ayat (1) UU ITE.

Dalam pertimbangannya, majelis hakim tingkat banding menilai bahwa *judex factie* sudah dipertimbangkan dengan benar. Selain itu, pengadilan banding menambahkan bahwa RL tidak mematuhi aturan internal PT. RAPP, di antaranya terkait larangan *back up* data dan perlunya izin untuk melakukan *back up* data. Hakim tingkat banding memandang perbuatan RL telah memenuhi unsur meskipun

tidak terdapat kerugian bagi PT. RAPP karena, menurut hakim, **tindak pidana dalam Pasal 32 UU ITE adalah tindak pidana formil sehingga ada tidaknya akibat tidak menjadi syarat untuk terjadinya tindak pidana.**

4. Putusan Nomor 42/PID/2018/PT BTN

Pada Juni 2015, AA, selaku mantan Ketua Pengurus Koperasi Awak Pesawat Garuda (KOAPGI), meminta mantan manager keuangan KOAPGI untuk mengirimkan data mutasi bank rekening milik KOAPGI ke alamat email AA. Permintaan tersebut diteruskan kepada staf IT KOAPGI dan data tersebut dikirimkan kepada AA tanpa sepengetahuan pengurus KOAPGI. Menurut pembelaan AA, terjadi dualisme kepengurusan karena adanya cacat hukum dalam penentuan Ketua KOAPGI yang baru dan hakim tingkat pertama mengesampingkan pendapat para ahli dan saksi di persidangan. Namun, pengadilan tingkat banding menguatkan putusan tingkat pertama dan AA dipidana dengan penjara selama 1 tahun dan 6 bulan. Penuntut Umum maupun AA kemudian mengajukan kasasi namun permohonan kasasi tersebut ditolak oleh pengadilan tingkat kasasi. Baik pengadilan tingkat banding maupun kasasi menilai bahwa *judex factie* telah tepat dalam memutus perkara ini karena AA, bersama-sama dengan dua orang lainnya, dinilai telah menyalahi ketentuan AD/ART KOAPGI dan tidak memiliki hak untuk mentransmisikan data KOAPGI.

5. Putusan Nomor 869/Pid.B/2017/PN.JKT.SEL

Dalam perkara ini, Terdakwa EH adalah supervisor PT. Andalan Terampil Multisis (ATM) yang memberikan jasa perawatan mesin Self Service Terminal (SST) bagi Bank CIMB Niaga. EH menggunakan jabatannya untuk menganalisis data transaksi dari beberapa lokasi SST CIMB Niaga dan berhasil membobol data nomor PIN dan nomor kartu ATM beberapa nasabah CIMB Niaga. Setelahnya, EH menggandakan data kartu ATM tersebut dan menggunakannya untuk bertransaksi di sejumlah mesin ATM CIMB Niaga. Sejumlah 306 juta rupiah diambil oleh EH dari beberapa rekening CIMB Niaga untuk melunasi cicilan rumah dan kartu kreditnya. Berdasarkan fakta hukum ini, EH didakwa dengan dakwaan alternatif menggunakan *pertama,* Pasal 363 ayat (1) ke-5 KUHP jo. Pasal 64 ayat (1) KUHP; **atau** *kedua,* Pasal 48 ayat (1) jo. Pasal 32 ayat (1) UU ITE.

Pada pertimbangannya, majelis hakim memeriksa cara yang digunakan oleh EH selaku supervisor SST untuk mendapatkan data terkait nasabah CIMB Niaga dan bagaimana EH menggandakan kartu ATM yang berisikan data masing-masing

nasabah. Hakim juga menyesuaikan keterangan tersebut dengan bukti CCTV dan keterangan Kepala Bagian Debit Card CIMB Niaga mengenai ketidaksesuaian antara saldo dengan catatan transaksi para nasabahnya. Berdasarkan kesesuaian fakta hukum dan bukti tersebut dengan unsur perbuatan Pasal 32 ayat (1) UU ITE, EH dipidana dengan pidana penjara 2 tahun dan 6 bulan serta denda 100 juta rupiah. Putusan ini kemudian dikuatkan oleh pengadilan tingkat banding.

B. Perbuatan yang tujuannya bukanlah data interference namun diputus bersalah dengan Pasal 32 ayat (1) UU ITE

1. Putusan Nomor 61/Pid.Sus/2020/PN Lbo

Berdasarkan fakta-fakta hukum, MS membuatkan akun Facebook untuk saksi N di telepon genggam milik Terdakwa. Pada Januari 2020, MS mengakses akun Facebook saksi N dan mencari akun Facebook milik U. Dari akun Facebook U, MS mengambil sebuah foto U yang sudah diedit dengan adanya dua tato di pipi U. MS lalu mengunggah foto tersebut di laman Facebook Portal Gorontalo dengan menambahkan keterangan bahwa Utun adalah tukang pukul yang tidak takut pada polisi atau tentara. Dalam putusan disebutkan bahwa keterangan tersebut **menimbulkan rasa kebencian atau permusuhan terhadap Babinsa/Tentara dan Polisi karena Mahmud dianggap sengaja menuliskan keterangan tersebut agar U dicari oleh Polisi dan Babinsa/Tentara.** Oleh karena perbuatan ini, MS didakwa dengan dakwaan kumulatif menggunakan Pasal 48 ayat (1) jo. Pasal 32 ayat (1) UU ITE **dan** Pasal 45A ayat (2) jo. Pasal 28 ayat (2) UU ITE.

Pada pertimbangan hukumnya, majelis hakim hanya menguraikan definisi beberapa unsur seperti "kesengajaan", "tanpa hak", serta beberapa unsur yang terdapat dalam penjelasan UU ITE. Selebihnya, hanya terdapat uraian fakta hukum sebagaimana dijabarkan sebelumnya. Majelis hakim kemudian langsung menyimpulkan bahwa perbuatan Terdakwa telah melanggar ketentuan Pasal 48 ayat (1) jo. Pasal 32 ayat (1) UU ITE.

Kemudian, dalam mempertimbangkan dakwaan kedua, majelis hakim sempat menjelaskan bahwa yang dimaksud dengan aktivitas penyebaran informasi yang berisikan ujaran provokatif yang mendorong kebencian atau permusuhan yang ditujukan untuk melukai, melecehkan, mengintimidasi, merendahkan, menurunkan, dan mengorbankan kelompok sasaran. Majelis hakim juga menjelaskan bahwa golongan, berdasarkan Pasal 156 KUHP, adalah **tiap bagian dari rakyat Indonesia yang berbeda dengan suatu atau beberapa bagian lainnya karena ras, negeri**

asal, agama, tempat asal, keturunan, kebangsaan, atau kedudukan menurut hukum tata negara. Namun, tanpa penjelasan mengenai bagaimana Babinsa/Tentara maupun Polisi merupakan bagian dari golongan yang dilindungi dalam pasal ini ataupun bagaimana perbuatan MS menimbulkan kebencian terhadap Babinsa/Tentara dan Polisi, majelis hakim langsung menyimpulkan bahwa unsur-unsur pasal 28 ayat (2) UU ITE terpenuhi. Oleh karena seluruh dakwaan dianggap terbukti oleh majelis hakim, MS dipidana dengan penjara selama 7 bulan.

2. Putusan Nomor 390/Pid.Sus/2024/PN Dps

Dalam perkara ini, HS merupakan pendamping korban kasus perselingkuhan rumah tangga sekaligus KDRT. Adapun korban menghubungi HS setelah mendapatkan kontak HS dari akun Instagram @ayoberanilaporkan5. Setelah korban menghubungi HS, HS menyarankan dan mendampingi korban untuk melaporkan kasusnya ke POMDAM Denpasar. Selain itu, HS dan korban pun bersepakat untuk mengunggah foto-foto BA yang diduga berselingkuh dengan suami korban ke Instagram. Pada 18 Januari 2024, Hari berusaha menghubungi BA namun tidak mendapat tanggapan sehingga keesokan harinya, Hari mengunggah foto BA dan keluarganya yang disertai penambahan beberapa teks. Perbuatan ini dilakukan dengan alasan agar kasus korban mendapatkan perhatian publik dan POMDAM Denpasar dapat segera menangani laporan korban. BA kemudian melaporkan HS dan HS didakwa dengan dakwaan tunggal Pasal 48 ayat (1) jo. Pasal 32 ayat (1) UU ITE jo. Pasal 55 ayat (1) ke-1 KUHP.

Pada bagian pertimbangan, majelis hakim mendefinisikan unsur tanpa hak sebagai perbuatan yang melanggar hak subyektif orang lain, norma-norma dalam kepatutan masyarakat atau setiap perbuatan yang dianggap tercela oleh masyarakat, atau tanpa mengindahkan cara yang ditentukan dalam aturan umum atau melawan hukum. Majelis hakim juga mengutip penjelasan MvT terkait kesengajaan. Selebihnya, majelis hakim hanya menuliskan definisi yang terdapat dalam undang-undang khususnya UU ITE dan mengurai ulang temuan fakta hukum. Tidak terdapat analisis khusus yang menjelaskan keterkaitan antara definisi yang diuraikan maupun teori kesengajaan dan tanpa hak dengan fakta hukum yang didapatkan. Oleh Pengadilan Negeri Denpasar, HS diputus bersalah dan dipidana dengan pidana penjara selama 5 tahun serta denda sebesar 5 juta rupiah. Atas putusan ini, Penuntut Umum kemudian mengajukan banding namun Pengadilan Tinggi Denpasar menguatkan putusan tingkat pertama. Selanjutnya, HS pun

mengajukan kasasi namun permohonan kasasi tersebut ditolak dengan alasan bahwa meskipun Terdakwa memiliki keterangan yang berbeda tentang apa yang sebetulnya terjadi, pemeriksaan *judex facti* sudah dilakukan di tingkat pertama dan banding. Dengan demikian, pengadilan kasasi tidak bisa lagi memeriksa *judex facti* maupun mempertimbangkan berat ringannya pemidanaan.

3. Putusan Nomor 3518 K/Pid.Sus/2020

Dalam putusan kasasi, majelis hakim kasasi menilai bahwa permohonan kasasi dari Penuntut Umum maupun kedua Terdakwa tidak dapat dibenarkan. Hal ini karena, berdasarkan pemeriksaan atas fakta dan bukti di persidangan telah terungkap bahwa kedua Terdakwa merupakan Direktur dari perusahaan masing-masing yang terbukti telah mengubah, menambah, mengurangi, melakukan transmisi informasi dan dokumen elektronik milik PT. GVC, MMC, dan RCTI. Pengadilan tingkat kasasi juga menyatakan bahwa permohonan kasasi tidak dapat dibenarkan oleh karena menyangkut pemeriksaan fakta-fakta hukum. Dengan demikian, kedua Terdakwa tetap dinyatakan bersalah melanggar Pasal 32 ayat (1) jo. Pasal 48 ayat (1) UU ITE.

C. Perbuatan yang memang tidak memenuhi unsur perbuatan dari Pasal 32 ayat (1) UU ITE dan diputus bebas

1. Putusan Nomor 175/Pid.Sus/2016/PN.Jkt.Pst.

Berdasarkan fakta-fakta hukum di persidangan, IS kehilangan telepon genggamnya setelah mendatangi kantor SA. Oleh karena itu, IS bersama AD kembali datang ke kantor SA dan bertemu dengan AG, karyawan kantor tersebut, untuk meminta AG memperlihatkan rekaman CCTV. Pada rekaman tersebut, terlihat bahwa SA mengambil dompet berisi 2 telepon genggam milik IS dari tas IS. Ketika rekaman tersebut diputar, AD merekam layar monitor yang memperlihatkan rekaman CCTV tersebut. Oleh karena upaya berdialog dengan SA tidak berhasil, IS melaporkan pencurian tersebut ke Polsek Tanah Abang, Jakarta. Namun, SA kemudian melaporkan balik IS. Pada perkara ini, IS didakwa dengan dakwaan alternatif menggunakan: *pertama,* Pasal 32 ayat (1) jo. Pasal 48 ayat (1) UU ITE; **atau** *kedua,* Pasal 30 ayat (1) jo. Pasal 46 ayat (1) UU ITE.

Dalam mempertimbangkan esensi dari unsur perbuatan pada Pasal 32 ayat (1) UU ITE dan mengaitkannya dengan fakta hukum yang ada, majelis hakim menyatakan bahwa IS hanya melihat gambar dari layar monitor CCTV dan IS tidak pernah menyentuh peralatan CCTV maupun menghubungkan telepon genggam (yang

digunakan Aditya untuk merekam) ke sistem peralatan CCTV. Konten video yang orisinil tetap terdapat dalam sistem komputer CCTV. Dengan demikian, esensi unsur perbuatan pada Pasal 32 UU ITE dalam perkara ini tidak terpenuhi. Selain itu, majelis hakim juga menyatakan bahwa IS memiliki kepentingan hukum yang mendasari kebutuhannya melihat rekaman CCTV. Kepentingan hukum tersebut adalah untuk **membuktikan suatu perbuatan yang berkaitan dengan kepentingan haknya** sehingga perbuatan IS tidak didasarkan pada niat jahat. Dengan ini, perbuatan IS tidak bisa disebut sebagai perbuatan melawan hukum. Berdasarkan argumentasi hukum ini, IS diputus bebas dari seluruh dakwaan. Putusan ini kemudian diajukan ke tingkat kasasi namun IS tetap dibebaskan oleh pengadilan tingkat kasasi.

4.2 JENIS PERBUATAN YANG DIDAKWA DENGAN PASAL 32 AYAT (2) UU ITE

Dari website Direktori Putusan Mahkamah Agung, tim peneliti mengumpulkan 39 putusan perkara yang menggunakan Pasal 32 ayat (2) UU ITE dalam dakwaannya. Dari 39 putusan perkara tersebut, tim peneliti menguraikan lebih lanjut 19 putusan sebagai contoh dari jenis perbuatan yang didakwa menggunakan Pasal 32 ayat (2) UU ITE. Terdapat setidaknya 2 klasifikasi putusan berdasarkan hubungan antara jenis perbuatan dalam fakta hukum dan pertimbangan hakim pada putusan. Adapun 2 klasifikasi tersebut adalah: A) Perbuatan yang terbukti memenuhi seluruh unsur Pasal 32 ayat (2) UU ITE dan dinyatakan bersalah; dan B) Unsur perbuatan terpenuhi namun unsur tanpa hak dari perbuatan tersebut tidak terpenuhi. Uraian beberapa putusan tersebut dapat dilihat dalam tabel berikut:

Tabel 4.2: Rincian Putusan Pasal 32 ayat (2) UU ITE

No	Nomor Putusan	Dakwaan	Jenis Perbuatan	Putusan
A.	**Perbuatan yang terbukti memenuhi seluruh unsur Pasal 32 ayat (2) UU ITE dan dinyatakan bersalah**			
1	1704/Pid. Sus/2022/ PN Sby	Pertama: Pasal 48 ayat (2) jo. Pasal 32 ayat (2) UU ITE jo. Pasal 55 (1) ke-1 jo. Pasal 65 ayat (1) KUHP; atau Kedua, Pasal 50 jo. Pasal 34 ayat (1) UU ITE jo. Pasal 55 (1) ke-1 jo. Pasal 65 ayat (1) KUHP.	Menggunakan alat berupa kamera dan microphone tersembunyi untuk pemindahan data jawaban ujian UTBK SBM PTN dari tim joki ke peserta ujian.	Pidana penjara 8 bulan dan denda 10 juta rupiah

No	Nomor Putusan	Dakwaan	Jenis Perbuatan	Putusan
2	799/Pid. Sus/2025/ PN Pbr.	Pertama: Pasal 32 ayat (2) jo. Pasal 48 ayat (2) UU ITE; atau Kedua: Pasal 32 ayat (1) jo. Pasal 48 ayat (1) UU ITE	Menyalurkan siaran milik perusahaan lain ke televisi lokal tanpa izin.	Pidana penjara 4 tahun dan denda 100 juta rupiah
3	1239/Pid. Sus/2025/ PT.Mdn	Kesatu: Pasal 32 ayat (2) jo. Pasal 48 ayat (2) UU ITE; atau Kedua: Pasal 362 KUHP.	Mengirimkan data perusahaan (data supplier dan relasi perusahaan) kepada orang lain.	Pidana penjara 1 tahun dan denda 50 juta rupiah
4	764/ Pid.B/2016/ PN.Jkt.Sel	Pertama Primair: Pasal 48 ayat (2) jo. Pasal 32 ayat (2) UU ITE jo. Pasal 64 ayat (1) KUHP; Subsidair: Pasal 48 ayat (1) jo. Pasal 32 ayat (1) UU ITE jo. Pasal 64 ayat (1) KUHP; Atau Kedua Primair: Pasal 363 ayat (1) ke-5 jo. Pasal 64 ayat (1) KUHP; Subsidair: Pasal 362 jo. Pasal 64 ayat (1) KUHP; Atau Ketiga: Pasal 50 jo. Pasal 22 huruf b UU Telekomunikasi jo. Pasal 64 ayat (1) KUHP	Meretas dan mengambil pulsa dari Telkomsel tanpa membayar lalu menjualnya pada agen pulsa.	Pidana penjara 1 tahun dan 6 bulan serta denda 50 juta rupiah
5	655/Pid. Sus/2022/ PN Ptk. 654/Pid. Sus/2022/ PN Ptk.	Pertama: Pasal 48 ayat (2) jo. Pasal 32 ayat (2) UU ITE jo. Pasal 55 ayat (1) ke-1 KUHP; atau Kedua: Pasal 45B jo. Pasal 29 UU ITE jo. Pasal 55 ayat (1) ke-1 KUHP	Memberikan akses akun nasabah kepada *desk collection* yang digunakan untuk menagih utang pinjaman online nasabah dengan	Penjara 1 tahun dan 8 bulan serta denda satu milyar seratus dua puluh lima juta rupiah

No	Nomor Putusan	Dakwaan	Jenis Perbuatan	Putusan
			cara mengirimkan pesan berisikan peringatan/ancaman pada nasabah dan menyebarkan data pribadi nasabah pada beberapa kontak dalam *phonebook* nasabah.	
6	527/Pid. Sus/2020/Pn Smn	Primair: Pasal 32 ayat (2) jo. Pasal 48 ayat (2) jo. Pasal 52 ayat (2) UU ITE jo. Pasal 65 ayat (1) KUHP; Subsidair: Pasal 30 ayat (1) jo. Pasal 46 ayat (1) jo. Pasal 52 ayat (2) UU ITE jo. Pasal 65 ayat (1) KUHP	Melakukan peretasan ke beberapa website Mahkamah Agung, pemerintah daerah, lembaga pemasyarakatan, dan kampus untuk melakukan *defacing* dan/atau membuat website terkait tidak dapat diakses.	Penjara 3 tahun dan 6 bulan serta denda 300 juta rupiah
7	511/Pid. Sus/2023/ PN JKT.SEL	Kesatu Kesatu: Pasal 46 ayat (1) jo. Pasal 30 ayat (1) UU ITE jo. Pasal 56 KUHP; atau Kedua: Pasal 46 ayat (2) jo. Pasal 30 ayat (2) UU ITE jo. Pasal 56 KUHP; atau Ketiga: Pasal 46 ayat (3) jo. Pasal 30 ayat (3) UU ITE jo. Pasal 56 KUHP; atau Keempat: Pasal 48 ayat (1) jo. Pasal 32 ayat (1) UU ITE jo. Pasal 56 KUHP; atau Kelima: Pasal 51 ayat (2) jo. Pasal 36 UU ITE jo. Pasal 56 KUHP; dan Kedua: Pasal 3 UU TPPU	Mengirimkan email yang berisikan link website *phishing* untuk mendapatkan username dan password akun Coinbase.	Pidana penjara 6 tahun dan denda 2 miliar rupiah (Pasal 32 ayat (2) UU ITE dan TPPU)

No	Nomor Putusan	Dakwaan	Jenis Perbuatan	Putusan
8	458/Pid. Sus/2020/ PT.DKI	Kesatu: Pasal 32 ayat (2) jo. Pasal 48 ayat (2) UU ITE jo. Pasal 55 ayat (1) ke-1 KUHP; Atau Kedua: Pasal 30 ayat (2) jo. Pasal 46 ayat (2) UU ITE jo. Pasal 55 ayat (1) ke-1 KUHP; Atau Ketiga: Pasal 363 ayat (1) ke-4 KUHP	Menggandakan data nasabah Bank Mandiri dan membuat duplikat kartu ATM yang berisikan data tersebut.	Penjara 4 tahun dan denda 100 juta rupiah
9	441/Pid. Sus/2024/ PN.Pbr	Primair: Pasal 48 ayat (2) jo. Pasal 32 ayat (2) UU ITE; Subsidair: Pasal 48 ayat (1) jo. Pasal 32 ayat (1) jo. UU ITE; Lebih subsidair: Pasal 46 ayat (2) jo. Pasal 30 ayat (2) UU ITE	Membuat dan menyebarkan web tiruan atau aplikasi mata uang *crypto* palsu untuk mencuri data ID dan password akun *crypto* korban.	Penjara 1 tahun dan denda 200 juta rupiah
10	424/Pid. Sus/2023/ PN Byw	Kesatu: Pasal 48 ayat (1) jo. Pasal 32 ayat (1) UU ITE jo. Pasal 55 ayat (1) KUHP jo. Pasal 65 ayat (1) KUHP; Atau Kedua: Pasal 48 ayat (2) jo. Pasal 32 ayat (2) UU ITE jo. Pasal 55 ayat (1) KUHP jis. Pasal 65 ayat (1) KUHP; Atau Ketiga: Pasal 363 ayat (1) ke-4 KUHP jo. Pasal 65 ayat (1) KUHP	Memberikan akses bagi orang yang tidak berhak berupa user ID dan password milik teller dan Kepala Unit BRI Sukonatar untuk memindahkan saldo dari sejumlah rekening nasabah Bank BRI ke rekening orang lain.	Penjara 1 tahun
11	423/Pid. Sus/2023/ PN Byw	Kesatu: Pasal 48 ayat (1) jo. Pasal 32 ayat (1) UU ITE jo.	Mengiming-imingi dan menyuruh orang untuk memberikan	Penjara 1 tahun dan 8 bulan

No	Nomor Putusan	Dakwaan	Jenis Perbuatan	Putusan
		Pasal 55 ayat (1) KUHP jo. Pasal 65 ayat (1) KUHP; Atau Kedua: Pasal 48 ayat (2) jo. Pasal 32 ayat (2) UU ITE jo. Pasal 55 ayat (1) KUHP jis. Pasal 65 ayat (1) KUHP; Atau Ketiga: Pasal 363 ayat (1) ke-4 KUHP jo. Pasal 65 ayat (1) KUHP	data berupa *user ID* dan *password* milik *teller* dan Kepala Unit BRI Sukonatar untuk memindahkan saldo dari sejumlah rekening nasabah Bank BRI ke rekening orang lain.	
12	412/ Pid.B/2019/ PNCkr	Kesatu: Pasal 363 ayat (1) ke-4, ke-5 jo. Pasal 53 ke-1 KUHP; dan Kedua: Pasal 32 ayat (2) jo. Pasal 48 ayat (2) UU ITE jo. Pasal 55 ayat (1) ke-1 KUHP	Membuat dan menggunakan kartu ATM palsu/duplikat untuk mengambil uang dari beberapa rekening nasabah BNI.	Penjara 1 tahun dan denda 25 juta rupiah (Pasal 32 ayat (2) dan pencurian)
13	370/Pid. Sus/2024/ PN Mtr 369/Pid. Sus/2024/ PN Mtr	Pertama: Pasal 32 ayat (2) jo. Pasal 36 jo. Pasal 51 ayat (2) UU ITE jo. Pasal 55 ayat (1) ke-1 KUHP jo. Pasal 64 ayat (1) KUHP; atau Kedua: Pasal 30 ayat (2) jo. Pasal 36 jo. Pasal 51 ayat (2) UU ITE jo. Pasal 55 ayat (1) ke-1 KUHP jo. Pasal 64 ayat (1) KUHP	Menggunakan data berupa *username*, *password*, serta pin *internet banking* BNI milik perusahaan, mengirimkannya pada orang lain, dan mengakses akun *internet banking* tersebut.	Penjara 7 bulan dan denda 1 juta rupiah
14	355/Pid. Sus/2021/ PN Dps	Pertama: Kesatu: Pasal 30 ayat (1) jo. Pasal 46 ayat (1) UU ITE; Atau	Mengakses data pribadi nasabah berupa nomor rekening, nomor hp, email, pin *mobile banking*, serta kode OTP dan menggunakannya untuk bertransaksi.	Penjara 5 tahun dan denda 2 milyar rupiah

No	Nomor Putusan	Dakwaan	Jenis Perbuatan	Putusan
		Kedua: Pasal 32 ayat (2) jo. Pasal 48 ayat (2) UU ITE; Dan Kedua: Pasal 3 UU TPPU		
15	142/Pid. Sus/2020/ PT.DKI	Pasal 32 ayat (2) jo. Pasal 48 ayat (2) UU ITE	Mengirimkan data-data yang dianggap sebagai data "strategi keuangan BCA" kepada pihak-pihak lain yang dianggap tidak berhak atas dokumen-dokumen perpajakan tersebut.	Penjara 2 tahun dan denda 500 juta rupiah
16	69/Pid. Sus/2024/ PN Plg	Pertama: Pasal 46 ayat (1) jo. Pasal 30 ayat (1) UU ITE; atau Kedua: Pasal 48 ayat (2) jo. Pasal 32 ayat (2) UU ITE	Melakukan peretasan ke *handphone* untuk mendapatkan informasi kode OTP yang digunakan untuk mengganti kata sandi akun BRImo.	Penjara 7 tahun dan denda satu miliar seratus dua puluh lima juta rupiah
17	32/Pid. Sus/2020/ PN. Gsk	Kesatu: Pasal 48 ayat (2) jo. Pasal 32 ayat (2) UU ITE jo. Pasal 55 ayat (1) ke-1 KUHP; Atau Kedua: Pasal 48 ayat (1) jo. Pasal 32 ayat (1) UU ITE jo. Pasal 55 ayat (1) ke-1 KUHP; Atau Ketiga: 46 ayat (2) jo. Pasal 30 ayat (2) UU ITE jo. Pasal 55 ayat (1) ke-1 KUHP	Membeli data kartu kredit milik WNA untuk membeli tiket pesawat dan reservasi hotel.	Penjara 1 tahun dan 10 bulan serta denda 10 juta rupiah

No	Nomor Putusan	Dakwaan	Jenis Perbuatan	Putusan
18	39/Pid. Sus/2021/ PN Rkb	Primair: Pasal 48 ayat (2) jo. Pasal 32 ayat (2) UU ITE jo. Pasal 65 ayat (1) KUHP; Subsidair: Pasal 48 ayat (1) jo. Pasal 32 UU ITE jo. Pasal 65 ayat (1) KUHP; Lebih Subsidair: Pasal 46 ayat (1) jo. Pasal 40 ayat (1) UU ITE jo. Pasal 65 ayat (1) KUHP.	Meretas wifi Indomaret untuk mendapatkan *password* dan mengakses server PT. Indomarco Prismatama yang digunakan untuk melakukan transaksi pembelian pulsa di Lazada, BliBli, dan Tokopedia.	Penjara 1 tahun dan 4 bulan dan denda 500 juta rupiah
B.	**Unsur perbuatan terpenuhi namun unsur tanpa hak dari perbuatan tersebut tidak terpenuhi**			
1	694/Pid. Sus/2018/ PN.Jkt.Utr 2200/K.Pid. Sus/2019	*Kesatu* Pasal 32 ayat (2) UU ITE Atau *Kedua* Pasal 30 ayat (2) UU ITE Atau *Ketiga* Pasal 30 ayat (1) UU ITE	Terdakwa mengirimkan data pelanggan PT. DCP melalui *email* kepada kepala perwakilan Houghton Singapura yang memberikan hak distribusi produk Houghton kepada PT. DCP. Terdakwa lalu digugat secara perdata dan dilaporkan secara pidana dengan tuduhan membongkar rahasia atau memberitahukan kepada pihak lain mengenai dokumen perusahaan yang seharusnya dirahasiakan.	Bebas

Terhadap jenis-jenis perbuatan yang dirumuskan dalam tabel, para hakim memiliki pertimbangan yang berbeda-beda terkait dakwaan. Dari 3 contoh putusan yang dijabarkan di bawah ini, terdapat setidaknya 2 klasifikasi putusan berdasarkan

hubungan antara jenis perbuatan dan pertimbangan hakim. Adapun 2 klasifikasi tersebut adalah: 1) Perbuatan yang dianggap oleh hakim sebagai mentransfer atau memindahkan data elektronik dan unsur dengan sengaja serta tanpa haknya terpenuhi; dan 2) Perbuatan memindahkannya terpenuhi namun unsur tanpa haknya tidak terpenuhi. Beberapa di antaranya adalah sebagai berikut:

A. Contoh Putusan dengan Perbuatan yang Terbukti Memenuhi Seluruh Unsur Pasal 32 Ayat (2) UU ITE dan Dinyatakan Bersalah

1. Putusan Nomor 1704/Pid.Sus/2022/PN Sby

Berdasarkan fakta hukum, ketiga Terdakwa direkrut oleh seseorang pada 2020 untuk mencari peserta ujian yang ingin menggunakan jasa joki ujian UTBK SBM PTN. Setelah mendapatkan para peserta ujian, ketiga Terdakwa mengenalkan alat (kamera, modem, dan alat komunikasi) dan memasangkannya pada tubuh para peserta ujian agar para peserta tersambung dengan tim operator dan tim master yang akan memberikan jawaban ujian. Ketiga Terdakwa didakwa dengan dakwaan alternatif yakni: *pertama*, Pasal 48 ayat (2) jo. Pasal 32 ayat (2) UU ITE jo. Pasal 55 (1) ke-1 jo. Pasal 65 ayat (1) KUHP; atau *kedua,* Pasal 50 jo. Pasal 34 ayat (1) UU ITE jo. Pasal 55 (1) ke-1 jo. Pasal 65 ayat (1) KUHP.

Pada pertimbangannya, majelis hakim menilai unsur perbuatan Pasal 32 ayat (2) UU ITE telah terpenuhi dengan berdasarkan pada fakta hukum yang ditemukan dan keterangan para Terdakwa. Ketiga Terdakwa dihukum dengan sanksi pidana yang sama yakni penjara selama 8 bulan dan denda sebesar 10 juta rupiah.

2. Putusan Nomor 799/Pid.Sus/2025/PN Pbr.

Dalam perkara ini, Terdakwa merupakan Direktur PT. Ginta Vision (GV) yang bekerja sama dengan PT. Mediatama Televisi (Nex Parabola) pada Januari 2020. Berdasarkan kerja sama tersebut, PT. GV berhak mendistribusikan siaran milik Nex Parabola ke televisi lokal di Rokan Hulu. Kemudian, pada 2021, PT. GV dan Nex Parabola tidak lagi bekerja sama dan sejak Agustus 2020, Niko belum membayar siaran-siaran dari Nex Parabola yang sudah disalurkan ke para pelanggannya. Hingga 2024, PT. GV masih menyalurkan siaran milik Nex Parabola tanpa ada izin dari Nex Parabola sehingga Nex Parabola mengalami kerugian sebesar 20 juta rupiah per bulan sejak Januari 2021 hingga Agustus 2024. Berdasarkan fakta hukum ini, Niko didakwa dengan dakwaan alternatif yaitu: *pertama*, Pasal 32 ayat (2) jo. Pasal 48 ayat (2) UU

ITE **atau** *kedua*, Pasal 32 ayat (1) jo. Pasal 48 ayat (1) UU ITE.

Pada pertimbangannya, majelis hakim mengurai peralatan dan cara yang digunakan oleh Terdakwa untuk menyalurkan siaran milik Nex Parabola ke para pelanggan yang membayar biaya pemasangan alat dan biaya langganan pada Terdakwa. Hakim juga menyebutkan kerugian yang diderita oleh PT. Mediatama Televisi dan dengan demikian menyatakan unsur perbuatan Pasal 32 ayat (2) UU ITE terpenuhi. Dengan demikian, Terdakwa diputus bersalah dan dijatuhi sanksi pidana penjara 4 tahun dan denda sebesar 100 juta rupiah.

B. Contoh Putusan yang Unsur Perbuatannya Terpenuhi namun Unsur tanpa Hak dari Perbuatan Tersebut Tidak Terpenuhi

1. Putusan Nomor 694/Pid.Sus/2018/PN.Jkt.Utr.

Dalam perkara ini, G selaku Segment Business Manager di PT Dwi Centro Perkasa (DCP) yang merupakan distributor oli Houghton Singapura di Indonesia. Pada September 2016, Houghton Singapura memutus hubungan kerja sama dengan PT DCP. Lalu, dalam rangka menjalankan tugasnya, G mengirimkan data pelanggan melalui *email* kepada kepala perwakilan Houghton Singapura. Data ini dikirimkan pada Houghton Singapura karena Houghton, melalui perjanjian kerja sama, memberikan hak distribusi produknya pada PT. DCP. G lalu digugat secara perdata dan dilaporkan secara pidana dengan tuduhan membongkar rahasia atau memberitahukan kepada pihak lain mengenai dokumen perusahaan yang seharusnya dirahasiakan.

G didakwa dengan dakwaan alternatif menggunakan *pertama,* Pasal 32 ayat (2) UU ITE; atau *kedua,* Pasal 30 ayat (2) UU ITE; atau *ketiga,* Pasal 30 ayat (1) UU ITE. Dalam pertimbangannya, majelis hakim menilai bahwa informasi yang dikirimkan oleh G bukanlah informasi yang harus dirahasiakan dari Houghton Singapura mengingat PT. DCP adalah distributor tunggal dari oli Houghton. Selain itu, majelis hakim juga merujuk pada putusan perdata kasus ini yang sudah putus lebih dulu. Dalam putusan perdata yang memenangkan G, hakim menilai bahwa tindakan G bukanlah perbuatan melawan hukum karena masih dalam hubungannya dengan tugas dan tanggung jawab G selaku Segment Business Manager Houghton. Berdasarkan pertimbangan ini, G dibebaskan dari semua dakwaan. Penuntut Umum kemudian mengajukan kasasi dan pada tingkat kasasi, pengadilan kasasi menolak permohonan kasasi tersebut.

4.3 ANALISIS PERTIMBANGAN HAKIM DALAM PEMENUHAN KRITERIA INDIKASI KRIMINALISASI DALAM PENGGUNAAN PASAL 32 UU ITE

Berdasarkan putusan-putusan yang dianalisis tersebut, terdapat beberapa permasalahan dalam implementasi Pasal 32 ayat (1) dan ayat (2) UU ITE dalam putusan pengadilan. Permasalahan ini muncul terutama saat Pasal 32 ayat (1) dan ayat (2) UU ITE disandingkan dengan instrumen hukum internasional berkaitan dengan *cybercrime*, yaitu Convention on Cybercrime (2001), atau sering disebut sebagai Budapest Convention.

- **Memisahkan illegal access dari data interference**

Sebagaimana telah dijelaskan dalam bab 2 terkait perbedaan *illegal access* dan *data interference,* penting untuk ditegaskan bahwa ketentuan larangan *data interference* seperti yang terdapat dalam Pasal 32 UU ITE tidak selalu harus didahului dengan *illegal access*. Dalam Budapest Convention, *illegal access* diatur sebagai satu jenis larangan yang terpisah dari *data interference* maupun *system interference*. *Illegal access* dipandang sebagai perbuatan yang perlu diatur sebagai tindak pidana ketika perbuatan mengakses keseluruhan atau sebagian komputer tersebut dilakukan dengan sengaja dan tanpa hak. Pemidanaan *illegal access* sebaiknya diterapkan apabila aksesnya dilakukan dengan merusak keamanan komputer dan dengan tujuan untuk memperoleh data komputer, untuk tujuan buruk lainnya, atau berkaitan dengan sistem komputer yang terhubung dengan sistem komputer lainnya.[51] Dengan demikian, pengertian dari *illegal access* adalah memasuki sistem komputer, baik keseluruhan maupun sebagian, dan ini tidak termasuk sekadar mengirimkan surat elektronik atau dokumen tertentu. Penekanan dari "tanpa hak" dalam ketentuan *illegal access* menjadi penting karena seseorang yang diberikan izin oleh orang yang memiliki otoritas untuk mengakses suatu perangkat atau perangkat yang aksesnya terbuka untuk publik tidak dapat dipidana dengan ketentuan *illegal access*.

Berdasarkan Budapest Convention dan penjelasannya, *illegal access* merupakan pelanggaran dasar yang mengancam dan menyerang keamanan sistem dan data komputer.[52] *Illegal access* dapat memiliki tujuan yang luas, namun titik berat dari larangan ini adalah memasuki suatu perangkat yang tidak seharusnya diakses

51 *Explanatory Report to the Convention on Cybercrime Budapest…, Op.Cit,* Pasal/Art. 2.

52 *Ibid,* Pasal/Art. 44.

oleh publik/secara bebas tanpa izin. Oleh karena tujuan dari perbuatan ini luas (sepanjang buruk atau ilegal), ada kemungkinan *illegal access* tersebut juga diikuti dengan bentuk perbuatan lain yang dilarang seperti *data interference* atau *system interference*. Dalam kasus seperti ini, terjadi dua atau lebih perbuatan pidana yang berhubungan, sehingga yang terjadi adalah perbuatan berlanjut. Namun, penting untuk dipahami bahwa perbuatan *data interference* tidak harus selalu diawali dengan *illegal access*. *Data interference* dapat terjadi tanpa *illegal access*, misalnya dalam kasus-kasus pelaku mendapatkan izin dari pihak yang memiliki otoritas untuk mengakses perangkat, lalu menyalahgunakan izin tersebut untuk merusak integritas atau fungsi data.

Gambar 4.1: Ilustrasi Kasus Perbedaan *Illegal Access*, *Data Interference*, dan *System Interference*

Sayangnya, dalam beberapa putusan yang ditemukan, terdapat kasus-kasus yang menunjukkan inkonsistensi penggunaan Pasal 30 dan Pasal 32 UU ITE dalam dakwaan. Dalam beberapa putusan, misalnya Putusan No. 284/Pid.B/2012/PN.DPK, 41/Pid.Sus/2020/PN Mar, dan 355/Pid.Sus/2021/PN Dps, didakwa secara alternatif dengan Pasal 30 dan Pasal 32 UU ITE, dengan fakta hukumnya yang menunjukkan terjadi *illegal access* terhadap komputer maupun sistem komputer atau jaringan telekomunikasi. Namun, dalam kasus pada Putusan No. 175/Pid.Sus/2016/PN.Jkt.Pst., salah satu dakwaannya menggunakan Pasal 30 UU ITE, padahal tidak terjadi *illegal access*, mengingat pihak yang mengakses komputer adalah orang yang berotoritas dan perbuatan mengaksesnya dilakukan tanpa niat dan tujuan buruk. Dalam kasus-kasus lain yakni pada Putusan No. 869/Pid.B/2017/PN.JKT.SEL, 764/Pid.B/2016/PN.Jkt.Sel, dan 39/Pid.Sus/2021/PN Rkb ditemukan fakta bahwa perbuatan didahului dengan *illegal access* namun Penuntut Umum tidak mendakwakan Pasal 30 UU ITE sebagai perbuatan berlanjut dengan Pasal 32 UU ITE.

Selain itu, dalam contoh putusan yang menggunakan Pasal 32, seperti Putusan No. 869/Pid.B/2017/PN.JKT.SEL, terdakwa diketahui membobol atau melakukan *cracking* data SST sehingga bisa mendapatkan nomor pin dan kartu ATM nasabah bank. Contoh lain adalah Putusan No. 764/Pid.B/2016/PN.Jkt.Sel dan 39/Pid.Sus/2021/PN Rkb yang menunjukkan fakta bahwa terdakwa melakukan peretasan ke sistem milik orang lain untuk melakukan tindak pidana. Ketiga putusan ini, sebagaimana tiga contoh putusan Pasal 32 UU ITE yang didahului dengan *illegal access*, memiliki kemiripan dalam cara terdakwa mengakses data yakni tanpa hak dan melalui cara seperti *cracking*. Dalam perkara semacam ini, APH seharusnya lebih jeli dalam membedakan perbuatan yang dilakukan agar tidak keliru dalam mengklasifikasikan perbuatan sesuai pasal yang seharusnya dikenakan.

- **Permasalahan unsur "memindahkan" dalam Pasal 32 UU ITE dan potensi tumpang tindih perbuatan Pasal 32 ayat (1) dengan Pasal 32 ayat (2) UU ITE**

Pasal 32 ayat (2) UU ITE secara khusus mengatur larangan memindahkan atau mentransfer informasi dan/atau data elektronik kepada sistem elektronik orang lain secara tanpa hak. Ketiadaan satu definisi atas "transfer" dan "memindahkan" dalam UU ITE ini menimbulkan perbedaan dalam implementasinya. Hal ini terlihat dalam 3 contoh putusan Pasal 32 ayat (2) UU ITE yang sudah dijabarkan pada bagian

sebelumnya. Dalam putusan terkait distribusi siaran televisi, perbuatan yang terjadi dalam perkara tersebut sebetulnya adalah meneruskan atau mendistribusikan siaran televisi. Tidak terjadi pemindahan atau transfer yang mengakibatkan berpindahnya dokumen dan/atau informasi elektronik dari satu tempat ke tempat lain. Perusahaan yang memiliki siaran televisi tersebut tetap memiliki siaran tersebut sebagai aset sementara perusahaan yang mendistribusikan tetap dapat menyiarkan siaran yang sama. Hal ini tentu berbeda dengan perbuatan memindahkan data dari satu perangkat ke perangkat lain dan menghapus data otentik di perangkat asal data tersebut.

Sebagai perbandingan, ketentuan *data interference* dalam Budapest Convention tidak memasukkan unsur "memindahkan", "transmisi", maupun "transfer" data di dalamnya. Istilah seperti "transfer" dan "transmisi" dalam Budapest Convention terdapat dalam ketentuan terkait "*illegal interception*" dan "*computer related fraud*". Perbuatan intersepsi ilegal yang dimaksud dalam Budapest Convention merupakan bentuk pelanggaran hak privasi dari komunikasi data dan sebetulnya serupa dengan intersepsi komunikasi dalam artian tradisional.[53] Oleh karena itu, konsep "transfer" dalam ketentuan ini tidak terlepas dari transfer data elektronik untuk mengintersepsi komunikasi antara beberapa pihak dan tentunya berbeda dengan "transfer" yang dimaksud dalam Pasal 32 UU ITE. Aturan intersepsi sendiri telah diatur di dalam UU ITE, namun terdapat pada pasal yang berbeda, yakni Pasal 31. Ketentuan Pasal 31 UU ITE ini pun telah mencakup intersepsi yang berpotensi menyebabkan perubahan informasi dan/atau dokumen elektronik.

Dengan demikian, memang tidak terdapat padanan istilah "memindahkan" pada Pasal 32 UU ITE dengan ketentuan dalam Budapest Convention. Sebagaimana disinggung sebelumnya, istilah memindahkan muncul baik dalam Pasal 32 ayat (1) maupun pada ayat (2) UU ITE. Tidak begitu jelas perbedaan antara perbuatan memindahkan dalam Pasal 32 ayat (1) dengan ayat (2) tersebut selain perbuatan pada ayat (2) yang dipidana apabila informasi dan/atau dokumen elektronik tersebut dipindahkan ke sistem elektronik milik orang lain. Pertanyaan yang muncul adalah, apakah memindahkan yang dimaksud dalam Pasal 32 ayat (1) UU ITE adalah memindahkan dalam satu sistem elektronik yang sama? Bagaimana contohnya? Dan, apa dampaknya terhadap integritas maupun fungsi data?

53 *Ibid,* Pasal/Art. 51-52.

Dalam contoh putusan yang ditemukan, terdapat putusan yang didakwa dengan Pasal 32 ayat (1) dan (2) UU ITE namun diputus bersalah menggunakan Pasal 32 ayat (1) UU ITE meskipun terjadi pemindahan data. Sebagai perbandingan, dapat dilihat pada tabel di bawah ini, terdapat satu contoh putusan yang diputus dengan Pasal 32 ayat (1) UU ITE meskipun terdapat perbuatan memindahkan data dan satu contoh putusan lain yang dipidana dengan Pasal 32 ayat (2) UU ITE:

Tabel 4.3: Perbandingan Perbuatan yang Diputus dengan Pasal 32 ayat (1) dan ayat (2) UU ITE

Putusan No. 210/Pid.Sus/2021/PN JKT.SEL (Terbukti bersalah Pasal 32 ayat (1) UU ITE)	**Putusan No. 1239/Pid.Sus/2025/ PT.Mdn (Terbukti bersalah Pasal 32 ayat (2) UU ITE)**
Terdakwa memberikan layanan pengecekan data informasi debitur (IDEB) melalui aplikasi SLIK OJK kepada pemesan. Akses terhadap aplikasi SLIK OJK dilakukan dengan perbantuan teman Terdakwa yang bekerja di bank dan memiliki otoritas mengakses aplikasi tersebut. Atas permintaan Terdakwa dari pemesanan pengecekan IDEB, teman **Terdakwa mengakses SLIK OJK dan mengunduh IDEB. Hasil unduhan dibuat dalam bentuk tipe file PDF dan dikirim kepada Terdakwa melalui email,** dengan mengedit dan menghapus nama user SLIK OJK teman Terdakwa. Terdakwa memasang tarif berupa uang tanda jadi dalam bentuk pulsa dari operator tertentu dan uang pelunasan dalam bentuk yang sama. Bayaran berupa pulsa ini kemudian dikonversi menjadi uang yang ditransfer ke rekening Terdakwa.	Terdakwa merupakan karyawan di suatu perusahaan yang memiliki akses terhadap data supplier, data rekan, maupun daftar harga produk. Suatu hari, terdakwa **menduplikasi data-data tersebut dan mengirimkan data tersebut pada orang di luar perusahaan tanpa seizin perusahaan.**

Pada Putusan No. 210/Pid.Sus/2021/PN JKT.SEL, Terdakwa memang mendapatkan data terlebih dulu dari temannya. Namun, Terdakwa kemudian memperdagangkan

data tersebut dan dalam prosesnya melakukan transfer atau transmisi data ke orang lain. Hal yang serupa pun terjadi dalam Putusan No. 1239/Pid.Sus/2025/PT.Mdn yang mana Terdakwa selaku karyawan di satu perusahaan, melakukan transfer data kepada orang lain di luar perusahaan tanpa hak. Dalam kedua kasus ini, karakteristik perbuatan yang dilakukan oleh kedua terdakwa dapat dikatakan mirip namun keduanya dikenakan pasal yang berbeda. Dalam kasus-kasus serupa, batasan antara perbuatan "memindahkan" dan "transfer" yang terdapat dalam Pasal 32 ayat (1) dengan Pasal 32 ayat (2) UU ITE menjadi kabur. Selain membingungkan, hal ini juga berkaitan dengan keadilan dan kepastian hukum mengingat ancaman pidana yang diatur dalam Pasal 32 ayat (2) UU ITE lebih berat ketimbang Pasal 32 **ayat (1) UU ITE.**

- **Penghukuman terhadap perbuatan yang tidak termasuk data interference dan potensi ancaman terhadap kebebasan berekspresi**

Berdasarkan contoh putusan-putusan di atas, Pasal 32 UU ITE membawa potensi penghukuman terhadap perbuatan-perbuatan yang seharusnya tidak dipidana berdasarkan pasal tersebut. Praktik ini berpotensi menimbulkan *chilling effect* dan menghalangi pemenuhan hak atas kebebasan berekspresi di ranah digital. Beberapa kasus sebenarnya merupakan bentuk penyampaian ekspresi atau pembelaan diri atas haknya sehingga seharusnya tidak perlu dilanjutkan hingga ke proses persidangan dan putusan. Dalam beberapa kasus lain, perbuatan yang didakwakan dapat saja dipidana, tetapi bukan melalui penerapan Pasal 32 UU ITE. Adanya putusan-putusan yang keliru mengimplementasikan ketentuan Pasal 32 UU ITE ini akan menimbulkan contoh yang buruk dan mengakibatkan kebingungan antara perbuatan mana yang termasuk dalam kategori Pasal 32 UU ITE dengan perbuatan mana yang sebetulnya merupakan penghinaan individu, berita bohong, dan sebagainya. Adanya penggunaan Pasal 32 UU ITE untuk melaporkan individu yang menggunakan hak berekspresinya juga menunjukkan fenomena berulang pasca pasal pidana semacam pencemaran nama baik dan ujaran kebencian diperketat rumusannya melalui revisi UU ITE.

Hal yang seharusnya menjadi fokus analisis dari perkara Pasal 32 UU ITE adalah apakah perbuatan yang didakwakan telah menimbulkan gangguan terhadap integritas suatu dokumen atau informasi elektronik. Dalam konteks ini, perlu dipahami pembedaan antara: 1) dokumen atau informasi elektronik milik pihak lain yang tersimpan dalam suatu perangkat atau sistem elektronik yang terhadapnya

kemudian seseorang melakukan gangguan atau *interference*; dan 2) dokumen atau informasi elektronik milik suatu pihak yang terhadapnya orang lain membuat salinan atau membuat tangkapan layar atau melakukan perekaman atau perbuatan lainnya tanpa sama sekali menimbulkan gangguan terhadap keutuhan/integritas dari dokumen atau informasi elektronik yang dimiliki suatu pihak tersebut. Perbuatan yang seharusnya dipidana oleh Pasal 32 UU ITE seharusnya adalah perbuatan dengan karakteristik yang pertama.

Beberapa contoh pemidanaan melalui Pasal 32 UU ITE yang tidak tepat dapat dilihat pada putusan Pengadilan Negeri Limboto nomor 61/Pid.Sus/2020/PN Lbo dan putusan Pengadilan Negeri Denpasar nomor 390/Pid.Sus/2024/PN Dps. Dalam putusan Pengadilan Negeri Limboto nomor 61/Pid.Sus/2020/PN Lbo, pengadilan tidak menggambarkan dengan jelas bagaimana perbuatan terdakwa telah mengganggu keutuhan/integritas dari foto yang ada di akun Facebook salah satu saksi dalam perkara ini. Dalam pertimbangannnya, pengadilan hanya mengulang uraian dakwaan bahwa terdakwa, dengan menggunakan akun Facebook yang aksesnya ia miliki sendiri, "mengambil foto" saksi yang sudah teredit dengan gambar tato dan kemudian "memposting foto tersebut ke PORTAL GORONTALO" dengan menambahkan *caption* tertentu yang dianggap mendorong kebencian terhadap suatu kelompok. Dari gambaran ini, dapat dipahami bahwa terdakwa tidak melakukan *editing* terhadap foto dan hanya "memposting" foto tersebut di media lain. Pengadilan tidak menjelaskan lebih detail bagaimana perbuatan "mengambil foto" dan "memposting foto" tersebut mengganggu integritas foto yang ada di akun Facebook saksi, misalnya dengan mengubah atau menghapus foto yang ada di akun Facebook saksi. Dalam situasi seperti ini, pengadilan seharusnya memeriksa lebih lanjut bagaimana pengaruh perbuatan terdakwa terhadap *file* asli yang ada di akun Facebook saksi. Pertimbangan majelis hakim juga tidak secara rinci membahas terpenuhi tidaknya unsur kesengajaan, tanpa hak, maupun melawan hukum dari perbuatan terdakwa.

Sementara itu, dalam putusan Pengadilan Negeri Denpasar nomor 390/Pid.Sus/2024/PN Dps terdakwa diputus bersalah karena pada akun media sosialnya telah membuat unggahan foto-foto seorang perempuan yang dituduh berselingkuh dengan seorang laki-laki yang sudah beristri dengan tambahan *caption* yang dianggap mencederai kehormatan/nama baik perempuan tersebut. Dari uraian dalam putusan, diketahui bahwa foto-foto yang menjadi permasalahan tersebut pada dasarnya didapatkan terdakwa dari istri sah sang laki-laki yang berselingkuh

tersebut. Istri tersebut mengirimkan foto-foto perempuan yang menjadi selingkuhan suaminya kepada terdakwa melalui aplikasi percakapan daring. Dalam hal ini, terdapat dua situasi yang perlu diperhatikan dari fakta hukum yang ditemukan pengadilan. Pertama, foto-foto yang diterima terdakwa adalah *file* foto yang hanya berupa salinan yang dikirimkan lewat aplikasi percakapan daring, sehingga dalam konteks ini *file* foto yang terdakwa punya dan unggah ke media sosialnya bukan *file* asli milik orang lain. Kedua, *file* foto yang dipunyai oleh terdakwa tersebut diperoleh dari orang lain yang memberikan persetujuan untuk mengubah atau melakukan modifikasi terhadap *file* foto tersebut. Maka, pada dasarnya perbuatan tersebut bukan perbuatan *data interference* karena tidak ada gangguan terhadap integritas *file* foto asli dan tidak terpenuhinya unsur "tanpa hak" yang termasuk unsur perbuatan yang dilarang dalam UU ITE. Namun, pengadilan pada akhirnya memutus terdakwa bersalah berdasarkan Pasal 32 ayat (1) UU ITE.

Dalam kedua contoh putusan tersebut, sebenarnya ketentuan pidana dalam Pasal 32 UU ITE tidak tepat untuk diterapkan pada perbuatan-perbuatan tersebut. Hal ini menegaskan adanya permasalahan rumusan unsur-unsur Pasal 32 UU ITE yang tidak jelas dan ketat serta kemungkinan bahwa APH juga tidak memiliki pemahaman yang cukup mengenai konteks penggunaan Pasal 32 UU ITE yang selaras dengan prinsip-prinsip HAM. Salah satu hal lain yang tidak ditemukan dalam beberapa kasus yang menggunakan dakwaan Pasal 32 UU ITE, termasuk kedua kasus yang disebutkan di atas, adalah tidak adanya pemeriksaan yang seksama terhadap elemen niat jahat dari perbuatan *data interference* yang dituduhkan. Dengan ketiadaan analisis yang mendalam terhadap niat jahat para terdakwa, maka Pasal 32 UU ITE dapat dengan mudah digunakan untuk menghukum perbuatan yang pada hakikatnya bukan *data interference*. Hal ini tidak berarti bahwa perbuatan-perbuatan yang menjadi contoh di atas tidak dapat dipidana. Namun, sangat mungkin terdapat pasal pidana lain yang lebih tepat untuk digunakan daripada Pasal 32 UU ITE.

Terlepas dari adanya praktik-praktik keliru dari implementasi Pasal 32 UU ITE ini, terdapat contoh putusan lain yang cukup bisa menggambarkan bagaimana seharusnya Pasal 32 UU ITE diterapkan sebagai larangan *data interference*. Dalam putusan Pengadilan Negeri Jakarta Pusat nomor 175/Pid.Sus/2016/PN.Jkt.Pst. diketahui bahwa terdakwa, dengan menggunakan telepon genggam, melakukan perekaman terhadap suatu hasil rekaman CCTV yang memperlihatkan kejadian hilangnya telepon genggam milik terdakwa di suatu ruangan. Dalam perkara ini pengadilan dengan seksama menilai bahwa terdakwa tidak melakukan perubahan

atau gangguan apapun terhadap *file* rekaman CCTV yang asli yang terdapat dalam perangkat CCTV sehingga tidak terdapat perbuatan *data interference* yang dimaksud dalam Pasal 32 ayat (1) UU ITE dan terdakwa diputus tidak bersalah. Pengadilan juga secara tepat menilai konteks niat terdakwa yang hanya berupaya membela haknya atas telepon genggamnya yang hilang sehingga tidak terdapat niat jahat dari perbuatan terdakwa. Dari contoh putusan ini, kita dapat melihat bagaimana seharusnya pengadilan memeriksa dan menghubungkan perbuatan terdakwa dengan konteks Pasal 32 UU ITE sebagai larangan terhadap *data interference*.

5

PENUTUP

Berdasarkan permasalahan yang digarisbawahi dalam tulisan ini dan paparan dalam bab-bab sebelumnya, bab ini memuat kesimpulan dan rekomendasi yang dapat menjadi perhatian dan ditindaklanjuti oleh pemangku kebijakan terkait.

5.1 KESIMPULAN

1. Pasal 32 ayat (1) dan ayat (2) UU ITE telah ditafsirkan secara tumpang tindih dan tidak konsisten oleh jaksa dan hakim.
2. Perumusan norma Pasal 32 ayat (2) UU ITE mengulang perumusan norma Pasal 32 ayat (1) UU ITE dengan hukuman pidana yang lebih berat.
3. *Illegal access* pada Pasal 30 UU ITE dan *data interference* pada Pasal 32 UU ITE memiliki basis perbuatan yang berbeda.
4. Pasal 32 UU ITE dalam penerapannya kerap digunakan sebagai alat kriminalisasi yang menjerat kebebasan berekspresi dan berpendapat masyarakat.

5.2 REKOMENDASI

1. Perlu adanya penafsiran ulang Pasal 32 ayat (1) UU ITE dengan mengacu pada asas-asas hukum pidana dan Budapest Convention

Penafsiran atas Pasal 32 ayat (1) UU ITE seharusnya merujuk pada asas-asas hukum pidana dan juga definisi serta contoh yang terdapat dalam Budapest Convention beserta dokumen penjelasannya.

- **Unsur "dengan sengaja"**

Undang-Undang ITE tidak menjelaskan apa yang dimaksud maupun jenis dari

kesengajaan dalam unsur "dengan sengaja" yang terdapat pada pasal ini Namun, dalam KUHP (baik yang lama dan baru), suatu perbuatan dapat dipidana apabila dilakukan dengan sengaja atau lalai meskipun kelalaian hanya dapat dipidana apabila ditegaskan dalam rumusan pasal. Lebih lanjut, dalam *Asas-Asas Hukum Pidana di Indonesia,* Wirjono Prodjodikoro menjelaskan tiga jenis kesengajaan yakni, 1) Kesengajaan yang bersifat tujuan yakni kesengajaan yang terpenuhi apabila pelaku menghendaki tercapainya akibat dari suatu perbuatan pidana. Kesengajaan bersifat tujuan ini terbagi lagi menjadi dua teori, yakni teori kehendak dan teori bayangan. Teori kehendak menganggap kesengajaan terpenuhi apabila pelaku menghendaki terjadinya perbuatan dan akibat dari perbuatannya. Sedangkan, teori bayangan menganggap kesengajaan terpenuhi apabila pelaku membayangkan dan mengusahakan akibat dari perbuatannya akan tercapai; 2) Kesengajaan secara keinsafan kepastian yakni saat melakukan perbuatannya, pelaku tidak bermaksud mencapai akibat yang diatur dalam pasal tetapi ia mengetahui betul bahwa akibat tersebut pasti akan tercapai saat ia melakukan perbuatannya; 3) Kesengajaan secara keinsafan kemungkinan yakni pelaku hanya membayangkan bahwa ada kemungkinan suatu akibat terjadi oleh karena perbuatannya namun ia tidak mengetahui pasti bahwa akibat tersebut akan terjadi.[54]

Ketiga jenis kesengajaan tersebut pada intinya terpenuhi karena adanya maksud dari pelaku untuk melakukan perbuatannya terlepas dari akibat dari perbuatan tersebut betul-betul diniatkan terjadi atau setidaknya dapat dibayangkan oleh pelaku. Dengan demikian, kesengajaan berbeda dengan kelalaian atau *culpa* yang disebabkan oleh kecerobohan atau tidak berhati-hatinya seseorang sehingga suatu perbuatan atau akibat terjadi. Van Hamel menjelaskan bahwa kelalaian dapat terjadi akibat seseorang kurang melihat ke depan atau memprediksikan sesuatu dan kurang berhati-hati.[55]

Dalam memaknai "dengan sengaja" dalam konteks Pasal 32 UU ITE, sebaiknya kesengajaan dimaknai sebagai **kesengajaan yang bersifat tujuan**. Sehingga, harus dibuktikan bahwa seseorang betul-betul menghendaki perbuatan "mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, atau menyembunyikan" yang berakibat pada berubah, berkurang,

---

54 Wirjono Prodjodikoro, *Asas-asas Hukum Pidana di Indonesia*, (Bandung: Refika Aditama, 2003), hal. 67-70.

55 Andi Hamzah, *Asas-Asas Hukum Pidana*, (Jakarta: Rineka Cipta, 2008), hlm. 112.

atau rusaknya integritas dan fungsi data berupa informasi dan/atau dokumen elektronik.

- **Unsur "tanpa hak"**

Tidak terdapat penjelasan juga terkait unsur "tanpa hak" di dalam UU ITE maupun peraturan perundangan lainnya. Namun, dalam Penjelasan Budapest Convention, terdapat beberapa narasi terkait unsur "tanpa hak". Pada dasarnya, "tanpa hak" menjadi salah satu unsur yang harus terpenuhi dalam beberapa kejahatan yang diatur dalam Budapest Convention seperti *illegal access*, *system interference*, dan *data interference.* Meskipun unsur ini harus terpenuhi, tidak berarti bahwa serta merta suatu perbuatan dapat dipidana apabila dilakukan tanpa hak karena unsur ini berkaitan dengan konteks perbuatan dan ada tidaknya alasan pembenar atau prinsip dan kepentingan lainnya yang dapat membenarkan suatu perbuatan yang dilarang tersebut[56].

Lebih lanjut, dokumen ini juga menjelaskan bahwa tindakan yang umum dalam mengoperasikan sistem, praktik komersil, dan proses merancang sistem jaringan tidak termasuk dalam kategori perbuatan yang dilakukan tanpa hak. Sepanjang perbuatan tersebut dilakukan dengan maksud dan tujuan baik seperti memfasilitasi komunikasi atau modifikasi data untuk keamanan komunikasi, seharusnya dianggap sejalan dengan prinsip pelindungan privasi yang sah dan oleh karenanya dilakukan dengan hak.[57] Sekiranya penafsiran yang sama atas unsur ini dapat diterapkan dalam menafsirkan unsur "tanpa hak" dalam Pasal 32 UU ITE.

- **Unsur "melawan hukum"**

Para ahli pidana terdahulu berusaha menafsirkan mengenai apa yang dimaksud dengan melawan hukum. Misalnya, Pompe menyatakan bahwa melawan hukum lebih luas definisinya dari sekadar bertentangan dengan undang-undang. Sedangkan, Van Bemmelen menjelaskan bahwa pada dasarnya unsur "melawan hukum" dalam hukum pidana tidak berbeda dengan hukum perdata. Van Bemmelen merujuk pada putusan *Hoge Raad* dalam perkara Lindenbaum vs. Cohen yang mendefinisikan perbuatan melawan hukum sebagai berbuat atau tidak berbuat yang bertentangan dengan atau melanggar: a) hak subjektif orang lain; b) kewajiban hukum pelaku; c)

56 Council of Europe, *Convention on Cybercrime* (ETS. No. 185), Par. 38.

57 *Ibid*, par. 62.

kaidah kesusilaan; atau d) kepatutan dalam masyarakat.[58] Kemudian, terdapat ahli seperti Jan Remmelink dan Van Veen yang menawarkan solusi dari definisi melawan hukum agar disesuaikan dengan ketentuan setiap delik berdasarkan tujuan dari delik atau peraturan tersebut, sejarah pembentukannya, dan sebagainya.[59]

UU ITE tidak menjelaskan secara eksplisit mengenai apa yang dimaksud dengan unsur melawan hukum dalam Pasal 32 UU ITE namun istilah ini muncul beberapa kali dalam UU ITE. Salah satunya dalam bagian umum dari Penjelasan Pasal 1 UU ITE yang menyebutkan bahwa pertumbuhan teknologi merupakan pedang bermata dua yang dapat membawa dampak positif seperti peningkatan kesejahteraan namun di sisi lain dapat membawa dampak negatif yakni sebagai sarana efektif untuk perbuatan melawan hukum. Melihat konteks tersebut, pada dasarnya melawan hukum dalam UU ITE dapat diartikan secara sederhana sebagai perbuatan tindak pidana yang diatur dalam UU ITE tersebut. Namun, tentu saja penjelasan Van Bemmelen juga masih berkaitan karena seharusnya perbuatan pidana dalam UU ITE, termasuk Pasal 32 UU ITE, tidak hanya melanggar peraturan perundangan tetapi juga berpotensi melanggar hak subjektif orang lain, kewajiban hukum pelaku, kaidah kesusilaan, maupun kepatutan dalam masyarakat. Hal ini terlihat dari berbagai putusan yang sudah dijelaskan sebelumnya yakni adanya perbuatan-perbuatan yang melanggar ketentuan Pasal 32 UU ITE dan merugikan hak orang lain maupun korporasi.

- **Unsur perbuatan: "mengubah, menambah, mengurangi, melakukan transmisi, merusak menghilangkan, memindahkan, atau menyembunyikan"**

Undang-Undang ITE tidak mendefinisikan unsur perbuatan yang terdapat dalam Pasal 32 UU ITE. Namun, sebagian dari unsur perbuatan tersebut memiliki padanannya dengan ketentuan dalam Budapest Convention. Dokumen penjelasan dari Budapest Convention juga menyertakan penjelasan dari perbuatan-perbuatan yang dilarang terkait *data interference*:

58 Shinta Agustina, dkk, *Penafsiran Unsur Melawan Hukum dalam Pasal 2 Undang-Undang Pemberantasan Tindak Pidana Korupsi,* Jakarta: Lembaga Kajian dan Advokasi Independensi Peradilan, 2016, hal. 53-54.

59 *Ibid.*

Tabel 5.1: Perbandingan Unsur Perbuatan dari Ketentuan *Data Interference*

UU ITE	Budapest Convention	Penjelasan Budapest Convention
Mengubah	Alteration	Modifikasi data yang tersedia. Memasukkan kode yang berbahaya, seperti virus dan Trojan merupakan bentuk dari modifikasi data.
Menambah	-	-
Mengurangi	Damaging and deteriorating	Mengubah integritas atau isi informasi dari suatu data dan program yang berdampak negatif.
Melakukan transmisi	-	-
Merusak	Damaging and deteriorating	Tindakan ini dianggap sebagai tindakan yang tumpang tindih dengan tindakan mengurangi.
Menghilangkan	Deletion	Dianggap setara dengan menghancurkan benda fisik. Menghilangkan didefinisikan sebagai menghancurkan data dan membuat data tersebut tidak dapat dikenali.
Memindahkan	-	-
Menyembunyikan	-	-
-	Suppressing	Semua tindakan yang menghalangi atau menghentikan ketersediaan data bagi orang yang memiliki akses terhadap komputer atau tempat data tersebut disimpan.

Tidak semua unsur perbuatan dalam Pasal 32 ayat (1) UU ITE memiliki padanan dengan Budapest Convention. Namun, perbuatan menambah, mentransfer, atau menyembunyikan data dapat dipahami sebagai bentuk perbuatan yang berpotensi mengganggu integritas maupun ketersediaan data. Hal yang menjadi permasalahan adalah perbuatan mentransmisikan data yang, sebagaimana telah dijelaskan pada pembahasan sebelumnya, tumpang tindih dengan Pasal 32 ayat (2) UU ITE. Hal ini bermasalah dalam tataran implementasi. Terlebih ketika perbedaan antara Pasal 32 ayat (2) dengan ayat (1) UU ITE sulit untuk dijelaskan. Terlepas dari lebih banyaknya unsur perbuatan yang diatur dalam UU ITE, seharusnya titik berat dari pasal ini adalah pada kesengajaan dan tanpa hak. Kembali lagi pada penjelasan dua unsur ini di atas, apabila tidak dilakukan dengan kesengajaan tanpa maksud maupun secara melawan hukum dan tanpa hak maka jenis perbuatan apapun itu dalam Pasal 32 ayat (1) UU ITE ini seharusnya tidak dapat dipidana.

- **Unsur "informasi dan/atau dokumen elektronik"**

Budapest Convention tidak menggunakan istilah informasi elektronik maupun dokumen elektronik dalam ketentuan *data interference*. Istilah yang digunakan adalah data komputer dan program komputer. Penjelasan Pasal 1 (b) dari Budapest Convention menjelaskan bahwa data komputer didefinisikan berdasarkan pada definisi data ISO. Ini berarti, data yang dimaksud dalam Konvensi ini adalah data yang "cocok untuk diproses" atau data dalam bentuk elektronik atau bentuk lain yang dapat diproses secara langsung. Data komputer ini diartikan sebagai data dalam sistem komputer yang dioperasikan dengan menjalankan program komputer. Sedangkan, Penjelasan Pasal 1 (a) dari Budapest Convention menjelaskan bahwa program komputer adalah serangkaian instruksi yang dapat dieksekusi oleh komputer untuk mencapai hasil yang diinginkan.

Definisi dalam penjelasan Budapest Convention ini sebetulnya cukup umum dan mengingat Konvensi ini disusun pada tahun 2001, tentu terdapat berbagai istilah dan perkembangan teknologi yang berbeda. Dengan demikian, sebetulnya tidak ada salahnya ketika definisi dari data komputer/elektronik tersebut diserahkan pada regulasi tiap negara. Secara lebih khusus, ketentuan paragraf 62 Explanatory Report Budapest Convention[60] merujuk segala bentuk tindakan yakni menghancurkan, merusak, merubah, atau menyembunyikan data komputer. Selain itu tindakan yang

60 *Explanatory Report to the Convention on Cybercrime Budapest…, Op.Cit,* Pasal/Art. 62.

biasa dilakukan dalam perancangan jaringan, atau pengoperasian pada suatu sistem operasi komputer pada piranti perangkat lunak. Definisi dalam penjelasan Budapest Convention ini sebetulnya cukup umum dan mengingat Konvensi ini disusun pada tahun 2001, tentu terdapat berbagai istilah dan perkembangan teknologi yang berbeda.

2. Menghapus Pasal 32 ayat (2) UU ITE yang ada saat ini

Pada dasarnya, keberadaan Pasal 32 ayat (1) UU ITE masih dibutuhkan untuk melindungi pengguna data dan program elektronik dari kerusakan integritas maupun fungsi data dan program. Namun, penafsirannya harus dilakukan secara ketat dan tidak boleh disalahgunakan untuk menjerat orang yang menggunakan haknya untuk berekspresi. Ketentuan yang sebetulnya menimbulkan masalah dengan keberadaannya adalah Pasal 32 ayat (2) UU ITE.

Disimpulkan dari paparan pada bab-bab sebelumnya, terdapat tiga alasan perlunya menghapus Pasal 32 ayat (2). *Pertama*, penerapan Pasal 32 ayat (2) untuk unsur "memindahkan atau mentransfer" dalam putusan pengadilan tidak konsisten dan membingungkan. Hal ini kerap ditunjukkan pada ketidaksinambungan antara dakwaan, bukti di persidangan, dan putusan hakim. Keberulangan penyebutan unsur "memindahkan" dalam Pasal 32 ayat (1) dan ayat (2) kerap digunakan bersamaan dalam satu kasus, sehingga membuat batas antara perbuatan "memindahkan" dalam Pasal 32 ayat (1) dan ayat (2) dan "transfer" dalam Pasal 32 ayat (2) menjadi kabur.

Kedua, rumusan Pasal 32 ayat (2) pada dasarnya sama dengan rumusan Pasal 32 ayat (1), sekalipun terdapat unsur "kepada sistem elektronik orang lain yang tidak berhak". Unsur ini menekankan bahwa kewenangan mengakses informasi data atau program komputer tidak sama dengan hak untuk menerima informasi data atau program komputer yang dimaksud, terlebih ketika pengirim dan penerima sama-sama tidak memiliki hak untuk mengakses, mengirim, dan menerima informasi data atau program komputer yang dimaksud. Logika unsur ini menjadi tumpang tindih dengan logika unsur Pasal 32 ayat (1), khususnya unsur "melakukan transmisi" dan "memindahkan". Unsur "melakukan transmisi" dan "memindahkan" pada dasarnya sama dengan menujukan informasi data atau program komputer ke sistem elektronik orang lain, terlebih ketika transmisi dan pemindahan ini dilakukan tanpa hak.

Terakhir, tidak ada padanan unsur "memindahkan atau mentransfer" dalam Budapest Convention. Dalam kaitannya dengan konsep data interference yang

melekat pada pengaturan Pasal 32, sebagaimana relevan dengan ketentuan di Budapest Convention, unsur "memindahkan atau mentransfer" tidak berkaitan dengan perlindungan integritas dan fungsi data dan program komputer. Dengan demikian, menghapus Pasal 32 ayat (2) dapat menjamin kepastian hukum, mengingat ancaman pidana yang diatur dalam Pasal 32 ayat (2) UU ITE lebih berat dibanding Pasal 32 ayat (1) UU ITE.

3. Menambahkan penjelasan norma Pasal 32 ayat (1) UU ITE dalam Ketentuan Penjelasan

Rumusan delik siber pada Pasal 32 ayat (1) dan ayat (2) UU ITE yang ada saat ini tidak memuat penjelasan yang memadai tentang definisi maupun batasan unsur delik. Ketentuan Penjelasan Pasal 32 ayat (1) dan ayat (2) yang ada saat ini hanya memuat frasa "cukup jelas" dan tidak membantu dalam menjelaskan definisi dan batasan unsur delik pasal tersebut. Ketidakcukupan rujukan dalam mendefinisikan dan membatasi unsur delik pasal ini memengaruhi kualitas penafsiran unsur delik oleh polisi, jaksa, dan hakim dalam menangani perkara konkret yang berkaitan dengan *illegal access* dan *data interference*. Di tengah keterbatasan pemahaman dan ketersediaan rujukan interpretasi bagi polisi, jaksa, dan hakim terhadap Pasal 32, akibatnya bagi masyarakat adalah penerapan unsur pasal oleh polisi, jaksa, dan hakim yang salah sasaran sehingga membatasi kebebasan berekspresi dan berpendapat masyarakat di ruang digital. Penerapan unsur pasal yang keliru ini akhirnya menimbulkan *chilling effect*, yang menyebabkan masyarakat untuk membatasi atau menahan ekspresi diri di ruang digital karena kekhawatiran akan kriminalisasi.

Dalam upaya menambahkan penjelasan unsur delik Pasal 32 ini, perlu adanya rujukan terhadap penjelasan *illegal access* dan *data interference* dalam Budapest Convention. Dalam Budapest Convention, *illegal access* merujuk pada tindakan memasuki suatu perangkat atau sistem elektronik yang tidak diperuntukkan bagi publik atau tidak dapat diakses secara bebas, tanpa izin atau otorisasi yang sah. Sementara itu, *data interference* menitikberatkan pada perbuatan yang mengganggu, merusak, atau menghilangkan integritas dan fungsi data maupun program komputer. Berdasarkan perbedaan tersebut, *illegal access* dan *data interference* tidak serta-merta berkaitan secara otomatis. Dalam kondisi tertentu, kedua tindak pidana ini memang dapat terjadi secara bersamaan sebagai suatu perbuatan berlanjut, namun hal tersebut tidak selalu demikian.

Selain itu, Ketentuan Penjelasan Pasal 32 UU ITE berperan penting bagi polisi, jaksa, dan hakim dalam melakukan penilaian secara terpisah unsur "tanpa hak" atas cara seseorang mengakses sistem atau data, serta akibatnya terhadap integritas data atau informasi komputer, sebagaimana rekomendasi poin 1 tulisan ini. Ketersediaan rujukan penjelasan unsur delik dalam Ketentuan Penjelasan Pasal 32 UU ITE dan penilaian yang cermat oleh polisi, jaksa, dan hakim atas unsur "tanpa hak" menjadi krusial untuk membedakan antara *illegal access* dan akses yang dilakukan berdasarkan otorisasi atau pada sistem yang terbuka untuk publik, meskipun kemudian terjadi gangguan terhadap data atau program komputer. Akhirnya, ketersediaan rujukan penjelasan unsur delik ini dapat menjamin kebebasan masyarakat dalam berekspresi dan berpendapat di ruang digital.

4. Menambahkan rumusan pengecualian pidana berupa alasan pembenar dalam rumusan Pasal 32 UU ITE menjadi Pasal 32 ayat (2) yang baru

Sebagaimana telah disebutkan dalam bab sebelumnya, bahwa penambahan rumusan pengecualian pidana berupa alasan pembenar ini berkaitan dengan kemungkinan kondisi terjadinya *data interference* dalam rangka melindungi kepentingan hukum yang lebih besar, seperti kepentingan umum maupun kepentingan negara. Alasan pembenar ini dapat berupa upaya mengungkap suatu tindak penipuan yang tidak bisa dilakukan tanpa *data interference*. Selain itu, alasan pembenar dapat berupa *data interference* yang dilakukan untuk memenuhi kepentingan hukum subjek hukum, misalnya dalam pengumpulan bukti laporan kepolisian.