Dialogia Iuridica Law Journal
Volume 15 Nomor 2, April 2024, pp. 053-077
ISSN: 2085-9945 | e-ISSN: 2579-3520

Pemberatan Sanksi Pidana pada Tindakan Peretasan Situs Milik Dewan Kehormatan Penyelanggara Pemilu Indonesia

Criminal Sanction Aggravation for Hacking of Sites Owned by Indonesian Election Organizer's Honor Board

Felicia Shadily[1], Go Lisanawati[2], Peter Jeremiah Setiawan[3]
[1 2 3]*Law Study Program, Faculty of Law, Universitas Surabaya, Jalan Raya Kalirungkut, Kali Rungkut, Kecamatan Rungkut, Kota Surabaya, Jawa Timur 60293*
[1]feliciashadily@yahoo.com, [2]go_lisanawati@staff.ubaya.ac.id, [3]peterjsetiawan@staff.ubaya.ac.id

Submitted: 2024-02-07 | Reviewed: 2024-03-18 | Revised: 2024-04-21 | Accepted: 2024-04-23

How to cite: Shadily, Felicia, et al. "Pemberatan Sanksi Pidana Pada Tindakan Peretasan Situs Milik Dewan Kehormatan Penyelanggara Pemilu Indonesia." *Dialogia Iuridica*, Vol. 15, No. 2, 2024, pp. 053-077.

DOI:
https://doi.org/10.28932/di.v15i2.8362

ABSTRAK

Artikel ini disusun berdasarkan persoalan pada kasus tentang seseorang bernisial H yang melakukan tindakan peretasan terhadap situs milik Dewan Kehormatan Penyelenggara Pemilu (DKPP). Atas tindakannya tersebut, pengadilan menjatuhkan vonis H bersalah melakukan tindak pidana, tanpa mempertimbangkan unsur pemberatan sebagaimana diatur dalam ketentuan pidana. Berdasarkan persoalan tersebut, studi kasus pada artikel ini bertujuan mengkaji penerapan pemberatan hukum pidana atas tindakannya melakukannya peretasan situs milik DKPP dalam ketentuan pidana Undang-Undang tentang Transaksi dan Informasi Elektronik. Berdasarkan metode yuridis normatif dan sesuai dengan pendekatan peraturan perundang-undangan serta pendekatan konseptual, maka H seharusnya dapat dibuktikan memenuhi unsur pemberatan dengan penambahan sepertiga dari ancaman pidana pokok. Hal tersebut dikarenakann H melakukan peretasan dengan sengaja dan tanpa hak mengubah, menambah, mengurangi, menyembunyikan informasi elektronik milik pemerintah, yakni

terhadap situs www.dkpp.go.id. Situs tersebut milik lembaga pemerintah yang memiliki tugas dan wewenang berkaitan dengan pelanggaran kode etik oleh penyelenggara pemilu. Situs tersebut juga dipergunakan untuk berbagai pelayanan publik yang berhubungan dengan pelanggaran kode etik oleh penyelenggara pemilu, termasuk di antaranya pengaduan hingga berbagai layanan informasi terkait dengan DKPP beserta tugas dan kewenangannya.

Keywords: Kejahatan Siber; Pemberatan Pidana; Peretasan

ABSTRACT

This article was prepared based on the case of a person with the initials H who hacked a website belonging to the Election Organizer Honorary Council (DKPP). Due to his actions, the court found H guilty of committing a criminal act, without considering the aggravating elements as regulated in the criminal provisions. Based on these issues, the case study in this article aims to examine the application of criminal law penalties for hacking DKPP sites in the criminal provisions of the Law on Electronic Transactions and Information. Based on the normative juridical method and in accordance with the statutory regulatory approach and conceptual approach, H should be proven to fulfill the aggravation element with the addition of one third of the main criminal threat. This was because H hacked intentionally and without the right to change, add, subtract, or hide electronic information belonging to the government, namely the site www.dkpp.go.id. The site belongs to a government agency that has duties and authority regarding violations of the code of ethics by election organizers. The site is also used for various public services related to violations of the code of ethics by election organizers, including

complaints and various information services related to DKPP and its duties and authorities.

Keywords: Criminal Aggravation; Cyber Crime; Hacking

I. INTRODUCTION

Perkembangan teknologi informasi dan modernisasi kehidupan sosial menjadikan internet sebagai kebutuhan dalam aktivitas kehidupan manusia sehari-hari. [1] Perkembangan yang dimaksud saat ini tidak hanya berhenti pada Era Industri 4.0, tetapi berkembang lebih lanjut pada *Era Society 5.0*. Pada era ini manusia dan menjadi sangat bergantung terhadap kecanggihan teknologi, yang merubah paradigma bahwa komunikasi dan interaksi manusia menjadi mudah serta efisien melalui media digital.[2] Perkembangan sebagaimana disebut juga memiliki problematika adanya peluang *evil behaviour* yang dalam masyarakat atau komunitas siber disebut sebagai kejahatan siber.[3] Persoalan perilaku jahat yang berujung pada kejahatan siber ini menjadi salah satu perbuatan pelanggaran-pelanggaran terhadap hak-hak ekonomi dan sosial yang saat ini paling umum dilakukan.[4]

Kejahatan siber baik dari segi pelaku maupun perbuatan merupakan fenomena yang harus diwaspadai karena memiliki karakteristik sangat berbeda dibandingkan dengan kejahatan konvensional-konvensional lainnya. Kejahatan ini dapat bermula dari keadaan privasi dan tersembunyi para pelaku hanya dengan bantuan komputer pribadi, *gadget,* telepon seluler dan yang kemudian menjangkau tempat-tempat terluar untuk menyerang dan membahayakan berbagai sistem lainnya, baik sistem komputer pribadi

[1] Alkaabi, Ali, et al. "Dealing with the Problem of Cybercrime', *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, Vol.* 53, 2011, pp 1–18, https://doi.org/10.1007/978-3-642-19513-6_1.
[2] Rahmawati, Melinda, et al. "The Era of Society 5.0 as the Unification of Humans and Technology: A Literature Review on Materialism and Existentialism." *Jurnal Sosiologi Dialektika*, Vol. 16. No. 2, 2021, pp. 151-162, https://doi.org/10.20473/jsd.v16i2.2021.151-162.
[3] Umanailo, M. Chairul Basrun, et al. "Cybercrime Case as Impact Development of Communication Technology That Troubling Society." *International Journal of Scientific and Technology Research*, Vol. 8, No. 9, 2019, pp. 1224–1228, http://repository.iainkediri.ac.id/id/eprint/630.
[4] Franjić, Siniša. "Cybercrime Is Very Dangerous Form of Criminal Behavior and Cybersecurity." *Emerging Science Journal*, Vol. 4, No. 18, 2020, pp. 18–26, https://doi.org/10.28991/esj-2020-SP1-02.

milik orang lain bahkan sistem komputer milik organisasi ekonomi sosial, lembaga publik hingga pemerintah.[5] Keadaan ini bahkan didefinisikan sebagai pintu masuk ancaman yang berisiko tinggi terhadap keamanan nasional.[6]

Kejahatan siber memiliki cakupan yang beragam dan berpokok pada penggunaan komputer, jaringannya dan/ atau internet untuk melakukan berbagai kegiatan ilegal. Prevalensi kejahatan ini dapat berupa serangan-serangan yang bertujuan untuk melakukan kecurangan dan *social engineering* seperti *phising* dan *ransomware*, hingga kejahatan terkait identitas dan peretasan (*hacking*).[7] Terkait serangan-serangan tersebut, Badan Siber dan Sandi Negara (BSSN) menjelaskan keadaan empirik di tahun 2022. BSSN menyebut lebih dari 700.000.000 serangan siber terjadi pada kurun waktu tersebut. Berdasarkan data BSSN, total 714.170.967 anomali trafik atau serangan siber yang terjadi di sepanjang 2022, dengan angka serangan paling tinggi terjadi pada Januari dengan angka serangan 272.962.734, lebih dari sepertiga total serangan selama semester pertama 2022. [8] Serangan siber termasuk peretasan juga tidak hanya dilakukan terhadap sistem elektronik milik perseorangan, atau lembaga swasta/ *private* tetapi bahkan juga dilakukan terhadap sistem elektronik milik pemerintah dan negara. Fakta serangan siber tersebut tidak hanya menimbulkan kerugian finansial semata melainkan kerugian lainnya, termasuk diantaranya bocornya informasi-informasi sensitif.[9]

Menanggulangi kejahatan siber tersebut, pemerintah telah mengatur berbagai perbuatan yang dilarang disertai ancaman sanksi pidana pada Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah beberapa kali terakhir dengan Undang-Undang No. 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (selanjutnya disebut UU ITE). Penerapan UU ITE tersebut dalam beberapa

[5] Ibid.
[6] Andini, Ni Komang Triana, et al. "Cybercrime and Threats to the Electoral System." *Journal of Digital Law and Policy, Vol.* 3, No. 1, 2023, pp. 26–37 https://doi.org/10.58982/jdlp.v3i1.508.
[7] Butarbutar, Russel. "Kejahatan Siber Terhadap Individu : Jenis , Analisis , Dan Perkembangannya." *Journal Technology and Economiacs Law*, Vol. 2, No. 2, 2023, pp. 297–316, https://scholarhub.ui.ac.id/telj/vol2/iss2/3/.
[8] CNN. "RI Dihantam 700 Juta Serangan Siber Di 2022, Modus Pemerasan Dominan." *CNN Indonesia*, 2022, https://www.cnnindonesia.com/teknologi/20220701164212-192-816150/ri-dihantam-700-juta-serangan-siber-di-2022-modus-pemerasan-dominan.
[9] Gulyas, Oliver, and Gabor Kiss. "Impact of Cyber-Attacks on the Financial Institutions." *Procedia Computer Science*, Vol. 219, 2023, No. 84–90, https://doi.org/10.1016/j.procs.2023.01.267.

perkara tindak pidana perlu mengacu pada berbagai hal, tidak hanya rumusan larangan perbuatan saja tetapi juga keadan-keadaan pemberatan. Salah satu kasus yang dapat dikaji terkait hal tersebut adalah perbuatan peretasan terhadap suatu situs di Indonesia yang memiliki spesifikasi khusus. Perkara atau kasus ini didasarkan pada Putusan Pengadilan Negeri Lahat Nomor: 76/Pid.Sus/2014/PN.LT. H alias CHMOD755 merupakan terpidana yang melakukan peretasan pada situs Dewan Kehormatan Penyelenggara Pemilu (selanjutnya DKPP) yakni *www.dkpp.go.id*) yang dilakukan pada bulan Desember 2013. H merubah tampilan interface situs *www.dkpp.go.id* dengan cara masuk melalui Mozilla Firefox, kemudian muncul situs Google lalu di kolom pencarian H mengetikkan kode *inurl=”php? id=”* kemudian enter dan muncullah situs-situs yang ada ID termasuk situs DKPP.

H mencoba masuk ke dalam situs-situs tersebut dengan memasukkan kode “url” namun hanya situs *www.dkpp.go.id* milik DKPP yang menjadi error. Setelah masuk kedalam situs dengan username dan password yang langsung muncul setelah kode perintah dimasukkan. H berhasil menerobos situs tersebut dan merubah tampilan *interface* situs, dengan cara H memblok tampilan semula yaitu mengganti file index halaman depan menggunakan *script html* lalu diganti dengan tampilan interface yang dibuat H. Tampilan interface situs *www.dkpp.go.id* yang semula berupa foto 7 (tujuh) orang pejabat DKPP dengan gambar Burung Garuda di pojok sebelah kiri serta ada tertulis pilihan berupa Putusan, Maklumat, Jadwal Sidang dan Form Pengaduan diubah menjadi berupa lambang berbentuk iblis dengan sayap putih dan inisial “MBT” yang merupakan singkatan dari “Manusia Biasa Team” dengan latar belakang (*wallpaper*) hitam dan tulisan “Tak ada yang perlu dibanggakan dari kami, hanya saja kami diciptakan sebagai orang paling tampan sedunia…” dengan inisial nickname *chmod755* feat Abraham Lincoln. Berdasarkan perbuatannya, H selanjutnya diperiksa dan Pengadilan Negeri Lahat menjatuhkan sanksi pidana berupa pidana penjara 10 (sepuluh) bulan dengan denda sebesar Rp 1.000.000,- (satu juta rupiah) sesuai ketentuan Pasal 46 ayat (3) UU ITE Jo. Pasal 30 ayat (3) UU ITE. Mengacu pada fakta-fakta sebagaimana dalam Putusan Pengadilan Negeri Lahat Nomor: 76 /Pid.Sus/2014/PN.LT, khususnya terkait perbuatan-perbuatan H terhadap objek berupa situs DKPP, maka dapat dikaji suatu

analisis persoalan hukum kontemporer.[10] Analisis tersebut berfokus pada perbuatan pidana peretasan beserta pemberatan sanksi pidana, khususnya sesuai norma sebagaimana diatur dalam UU ITE. Analisis persoalan hukum artikel ini didasarkan pada metode yuridis normatif dan sesuai dengan pendekatan peraturan perundang-undangan serta pendekatan konseptual. Pendekatan dimaksud beranjak pada peraturan perundang-undangan terkait serta doktrin-doktrin atau pandangan yang berkembang pada ilmu hukum.[11]

II. DISCUSSION

1. Pemberatan Pidana dalam Undang-Undang tentang Informasi dan Transaksi Elektronik

Pemberatan (*aggravation*) serta pengurangan (*mitigation*) merupakan persoalan penting dalam penentuan atau penjatuhan sanksi, termasuk sanksi pidana.[12] Pemberatan pidana adalah penjatuhan pidana yang dapat ditambahkan ancaman pidananya karena adanya kondisi tertentu yang terdapat dalam tindak pidana yang memenuhi rumusan undang-undang.[13] Pemberatan pidana dalam konteks kebijakan hukum pidana merupakan pedoman pembuatan atau penyusunan pidana bagi pembentuk undang-undang, yang dibedakan dengan pedoman pemidanaan bagi hakim dalam menjatuhkan pidana. Pemberatan pemidanaan pada dasarnya merupakan suatu gejala yang tersirat dari ancaman pidana yang terdapat dalam rumusan tindak pidana suatu ketentuan perundang-undangan. Berdasarkan hal tersebut, dapat diketahui kehendak pembentuk undang-undang berkenaan dengan jumlah dan jenis pidana yang dijatuhkan terhadap pelaku tindak pidana.[14] Pola pemberatan dalam ancaman pidana dalam KUHP sendiri dapat dibedakan dalam dua kategori. *Pertama*, yaitu pola pemberatan karena adanya perbarengan, baik karena konkursus idealis, konkursus realis, ataupun bentuk perbuatan

[10] Benuf, Kornelius, and Muhamad Azhar. "Metodologi Penelitian Hukum Sebagai Instrumen Mengurai Permasalahan Hukum Kontemporer." *Gema Keadilan*, No. 7, No. 1, 2020, pp. 20–33, https://doi.org/10.14710/gk.2020.7504.
[11] Marzuki, Peter Mahmud, *Penelitian Ilmu Hukum.* Jakarta, Kencana, 2011.
[12] Roberts, Julian V., *Mitigation and Aggravation at Sentencing.* Cambri, Cambridge University Press, 2011
[13] Anjari, Warih. "Penerapan Pemberatan Pidana Dalam Tindak Pidana Korupsi." *Jurnal Yudisial*, Vol. 15, No. 2, 2023, pp. 263, https://doi.org/10.29123/jy.v15i2.507.
[14] Arief, Barda Nawawi, *Bunga Rampai Kebijakan Hukum Pidana: Perkembangan Penyusunan Konsep KUHP Baru.* Jakarta, Kencana, 2011.

berlanjut/ *voortgezette handeling*. Berkaitan dengan ini, ancaman pidana yang ditentukan menjadi sepertiga lebih berat dari ancaman pidana yang terdapat dalam rumusan tindak pidana yang memuat ancaman pidana yang terberat.[15]

Kedua pemberatan khusus sebagaimana diatur dalam rumusan tindak pidana (delik) pada Buku II dan Buku III KUHP. Pemberatan khusus pada delik ini bisa dibedakan 2 kelompok. Kelompok kesatu merupakan pemberatan dalam kategori khusus seragam didasarkan pada subjek atau objek menurut tindak pidana (delik). Pemberatan berdasarkan subjek atau pelaku delik di antaranya pelaku pengulangan tindak pidana (residivis). Pidana pada kelompok ini ditambah sepertiga dari ancaman pidana maksimalnya. Ketentuan pengulangan sendiri juga diatur khusus dalam Buku II KUHP tentang Kejahatan Pasal 486, 487, dan 488 KUHP. Seseorang dapat dikatakan sebagai pelaku pengulangan apabila sudah memenuhi syarat-syarat pengulangan. Ancaman hukuman juga diperberat karena terdapat karakteristik khusus pelaku delik, contohnya jika pelaku adalah seorang pegawai negeri. Sedangkan, pemberatan berdasarkan kualifikasi khusus pada objek delik, dapat berupa perkara tindak pidana penganiayaan terhadap orang tua, pasangan, atau anak dari pelaku, yang mengakibatkan hukuman tambahan sepertiga dari hukuman maksimum yang berlaku khususnya. [16]

Kelompok kedua dari pemberatan khusus merupakan kategori pemberatan yang tidak seragam, di mana peningkatan bisa terjadi baik secara kualitatif maupun kuantitatif terhadap ancaman hukuman. Pemberatan pidana dalam hal ini terjadi karena terjadi perubahan jenis pidana, seperti perubahan dari hukuman penjara menjadi hukuman mati dalam delik pembunuhan berencana. Pemberatan juga dapat terjadi dengan menambahkan jumlah maksimum khusus hukuman. Hal ini dilakukan ketika terdapat unsur khusus (baik dari perilaku maupun akibat) dalam suatu tindak pidana yang menjadi dasar pemberatan hukuman khusus tersebut. Prinsip pemberatan hukuman khusus ini dirumuskan dan berlaku hanya untuk tindak pidana tertentu saja, tidak berlaku secara universal untuk semua tindak pidana.[17]

[15] *Ibid.*
[16] *Ibid.*
[17] *Ibid.*

Pembagian pemberatan dalam KUHP secara ringkas, juga dapat dibagi dalam pemberatan pidana umum dan pemberatan pidana khusus. Pemberatan pidana umum berlaku untuk seluruh tindak pidana dan diatur dalam Buku I KUHP. Pemberatan pidana khusus, berlaku untuk tindak pidana tertentu dan diatur dalam Buku II dan Buku III KUHP serta peraturan yang ada diluar KUHP atau tindak pidana khusus.[18] Pemberatan yang diatur dalam Buku I KUHP dan merupakan pemberatan umum meliputi: (1) Pemberatan pidana karena jabatan berdasarkan Pasal 52 KUHP; (2) Pemberatan pidana karena menggunakan sarana prasarana bendera kebangsaan berdasarkan Pasal 52A KUHP; dan (3) Pemberatan pidana karena gabungan tindak pidana berdasarkan Pasal 65 KUHP.

Terkait dasar pemberatan pidana khusus dalam KUHP, meliputi: (1) Pengulangan tindak pidana yang diatur dalam Buku II dan Buku III KUHP; (2) Delik yang dikualifisir (misalnya Pasal 356 KUHP); (3) Delik yang dilakukan oleh orang tertentu dan dalam keadaaan tertentu (misalnya Pasal 374 KUHP); serta (3) Pemberatan dalam tindak pidana khusus. Chazawi juga membagi pemberatan pidana meliputi: a) dasar pemberat pidana karena jabatan; b) dasar pemberat pidana dengan menggunakan sarana bendera kebangsaan; dan c) dasar pemberat pidana karena pengulangan.[19]

Salah satu pemberatan umum diatur dalam Pasal 52 KUHP yang menentukan: "Bilamana seseorang pejabat karena melakukan perbuatan pidana melanggar suatu kewajiban khusus dari jabatanya, atau pada waktu melakukan perbuatan pidana memakai kekuasaan, kesempatan atau sarana yang diberikan kepadanya karena jabatanya, pidananya dapat ditambah sepertiga." Jonkers sebagaimana dikutip oleh Adami Chazawi menjelaskan Pasal 52 KUHP tersebut adalah dasar pemberatan pidana (*strafvergogingsgronden*) karena kedudukan pelakunya sebagai pegawai negeri, dimana letak pemberatan pidana tersebut yaitu pelaku adalah seorang pegawai negeri.[20] Dalam hal ini yang menjadi fokus adalah status atau kedudukan yang melekat pada pelaku yaitu sebagai seorang pegawai negeri sipil. Terdapat maksud bahwa agar seorang pegawai negeri dapat diperberat hukumannya, maka harus memenuhi unsur-unsur sebagai

[18] Anjar, *Op.Cit.*
[19] Chazawi, Adami, *Pelajaran Hukum Pidana (Bagian 1) : Stelsel Pidana, Tindak Pidana, Teori-Teori Pemidanaan & Batas Berlakunya Hukum Pidana.* Jakarta, Rajawali Pers, 2013.
[20] Hamzah, Andi, *Asas-Asas Hukum Pidana Di Indonesia Dan Perkembangannya.* Jakarta, Sofmedia, 2018.

berikut: (1) Ia melanggar kewajiban khusus dari jabatannya. (2) Pada waktu melakukan tindak pidana, ia memakai kekuasaan, kesempatan atau sarana yang ada padanya karena jabatannya.

Pemberatan dalam tindak pidana sendiri juga diterapkan dalam UU ITE yang diterapkan dalam kejahatan peretasan dimana pemberatan tersebut dibedakan sesuai dengan subjek dan objeknya. Pemberatan dalam tindak pidana yang tercantum di dalam UU ITE yang dimuat dalam Pasal 52 UU ITE yaitu pemberatan sebesar 1/3 (sepertiga) dan 2/3 (dua pertiga) dari maksimum ancaman pidananya. Pemberatan 1/3 dari pidana pokok yang diterapkan dalam hal tindak pidana pada Pasal 27 ayat (1) menyangkut kesusilaan atau eksploitasi seksual terhadap anak (Pasal 52 ayat (1)) dan Pasal 30 sampai dengan Pasal 37 ditujukan terhadap Komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik Pemerintah dan/atau yang digunakan untuk layanan publik (Pasal 52 ayat (2)). Di sisi lain, pemberatan 2/3 diterapkan dalam Pasal 30 sampai dengan Pasal 37 UU ITE ditujukan terhadap Komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik Pemerintah dan/atau badan strategis termasuk dan tidak terbatas pada lembaga pertahanan, bank sentral, perbankan, keuangan, lembaga internasional, otoritas penerbangan (Pasal 52 ayat (3)) dan Pasal 27 sampai dengan Pasal 37 dilakukan oleh korporasi (Pasal 54 ayat (4)).

Pemberatan berdasarkan objek dari delik diwujudkan dalam Pasal 52 ayat (2) yaitu: “Dalam hal perbuatan sebagaimana dimaksud dalam Pasal 30 sampai dengan Pasal 37 ditujukan terhadap Komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik Pemerintah dan/atau yang digunakan untuk layanan publik dipidana dengan pidana pokok ditambah sepertiga.”

Berdasarkan pasal tersebut memuat unsur-unsur bahwa apabila terdapat tindak pidana sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 37 dilakukan terhadap komputer dan/atau sistem elektronik serta informasi elektronik dan/atau dokumen elektronik milik pemerintah dan/atau digunakan untuk layanan publik atau kepentingan masyarakat sanksi pidananya ditambah sepertiga dari pidana yang semestinya. Pasal 52 ayat (3) juga menerapkan alasan yang sama yaitu dengan menerapkan pemberatan pada objek delik tetapi terdapat perbedaan yaitu objek delik

yang dimaksud pada Pasal 52 ayat (3) adalah terhadap Komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik Pemerintah dan/atau badan strategis termasuk dan tidak terbatas pada lembaga pertahanan, bank sentral, perbankan, keuangan, lembaga internasional, otoritas penerbangan yang dimana ancamannya adalah pidana maksimal ancaman pidana pokok masing-masing Pasal ditambah dua pertiga.

Pemberatan pada Pasal 52 ayat (2) dan (3) UU ITE ini berpaku pada objek dari peretasan itu sendiri yaitu Komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik Pemerintah dan/atau yang digunakan untuk layanan publik dan/ atau badan strategis termasuk dan tidak terbatas pada lembaga pertahanan, bank sentral, perbankan, keuangan, lembaga internasional, otoritas penerbangan dimana apabila timbul permasalahan dalam objek-objek tersebut yang menimbulkan terhambatnya layanan publik dan tidak dapat diaksesnya kebutuhan masyarakat sehingga dapat menimbulkan permasalahan di masyarakat. Dampak dari tindak pidana yang ditujukan terhadap milik pemerintah dapat berdampak besar bagi pemerintah maupun masyarakat sendiri yang dimana kerugian yang dialami bukan bersifat privat melainkan publik sehingga diperlukan adanya pemberatan sebagai langkah preventif dan juga langkah represif bagi yang telah melakukan tindak pidana tersebut. Pemberatan berdasarkan subjeknya diwujudkan dalam Pasal 52 ayat (4) UU ITE yang menyebutkan

> "Dalam hal tindak pidana sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 37 dilakukan oleh korporasi dipidana dengan pidana pokok ditambah dua pertiga."

Jika terdapat tindak pidana sebagaimana dimaksud dalam Pasal 27 sampai dengan 37 UU ITE dilakukan oleh korporasi dengan dasar untuk menghukum setiap perbuatan melawan hukum yang memenuhi unsur sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 37 yang dilakukan oleh korporasi atau (*corporate crime*) yang memiliki kapasitas untuk mewakili korporasi, mengambil keputusan dalam korporasi, melakukan pengawasan dan pengendalian dalam korporasi, dan melakukan kegiatan demi keuntungan korporasi (Penjelasan atas Pasal 52 ayat (4) UU ITE). Hal ini didasari oleh UU ITE yang telah mengatur terkait pertanggungjawaban pidana bagi korporasi adalah

mengenai pihak-pihak yang dapat dimintai pertanggungjawaban pidana dalam hal terjadi 3 kejahatan korporasi (*corporate crime*). Dalam hal ini UU ITE menganut ajaran pertanggungjawaban korporasi dalam kebijakan hukum pidana yaitu *doctrine of identification* yang dengan menerapkan pertanggungjawaban pidana korporasi dalam hal pelaku tindak pidana adalah korporasi itu sendiri. Hal ini menyatakan dengan jelas bahwa beban pertanggungjawaban pidana yang dilakukan oleh korporasi dibebankan pada korporasinya dan juga kepada pengurusnya yang mempunyai kedudukan fungsional.[21]

Perbedaan pemberatan yang dimuat di dalam UU ITE tidak memberikan penjelasan lebih rinci mengenai alasan pembeda pemberatan dan pertimbangan atas pembedaan pemberatan tersebut. Pemberatan terkait persoalan eksploitasi anak ataupun kesusilaan terhadap anak, menjadi materi yang sama berharga dan pentingnya dengan apabila tindak pidana ITE ditujukan pada Informasi Elektronik dan/ atau Dokumen Elektronik milik Pemerintah yang menduduki peran strategis, seperti lembaga pertahanan, bank sentral, perbankan, dan lain sebagainya.[22] Selanjutnya dijelaskan bahwa peran dan kedudukan dari lembaga-lembaga pemerintahan sebagaimana dimaksudkan antara Pasal 52 ayat (2) dan ayat (3) UU ITE juga tidak memiliki signifikansi untuk dibedakan, mengingat bahwa setiap lembaga memiliki kepentingan yang sama atas informasi elektronik dan/atau dokumen elektronik tersebut.[23] Pada pokoknya pemberatan pidana baik pada KUHP dan UU ITE merupakan pedoman atau petunjuk dalam menjatuhkan pidana. Pedoman atau petunjuk juga merupakan fungsi kontrol bagi pengadilan agar putusan pemidanaan berdaya guna sesuai tujuan pemidanaan bagi pelaku tindak pidana.[24]

[21] Mulasari, Laila. "Ajaran Pertanggungjawaban Pidana Korporasi dalam Kebijakan Hukum Pidana di Bidang Mayantara." *Hukum dan Dinamika Masyarakat*, *Vol.* 9, No. 2, 2012, pp. 113–120, http://dx.doi.org/10.56444/hdm.v9i2.301.
[22] Lisanawati, Go. "Menyoal Pemberatan Pidana Sepertiga Dan Duapertiga Pada UU ITE Dan Harmonisasinya Atas RUU KUHP." in *Problematika Pembaharuan Hukum Nasional*, 2013, pp. 107–115, http://repository.ubaya.ac.id/id/eprint/9554.
[23] Ibid.
[24] Irmawanti, et al. "Urgensi Tujuan Dan Pedoman Pemidanaan Dalam Rangka Pembaharuan Sistem Pemidanaan Hukum Pidana." *Jurnal Pembangunan Hukum Indonesia*, Vol. 3, No. 2, 2021, pp. 217–27, https://doi.org/10.14710/jphi.v3i2.217-227.

2. Pemberatan Sanksi Pidana Peretasan Situs Milik Dewan Kehormatan Penyelenggara Pemilu Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah beberapa kali terakhir dengan Undang-Undang No. 1 Tahun 2024

Berdasarkan Pasal 1 angka (1) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah beberapa kali terakhir dengan Undang-Undang No. 1 Tahun 2024 (UU ITE) Informasi elektronik memiliki banyak rupa yakni satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *electronic data interchange (EDI)*, surat elektronik (*electronic mail*), telegram, teleks, *telecopy* atau sejenisnya, huruf, tanda, angka, kode akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya. Informasi elektronik yang dimaksud adalah informasi yang dapat dimengerti dan diakses oleh orang-orang yang dimana sebelum adanya perkembangan globalisasi dan teknologi, informasi-informasi tersebut hanya dapat diakses secara konvensional. Salah satu contohnya adalah seperti situs pemerintah yang dimana terdapat banyak sekumpulan informasi yang dapat diakses oleh masyarakat dengan menggunakan internet, apabila dibandingkan dengan sebelum adanya internet maka masyarakat hanya dapat mengakses informasi melalui koran, televisi, dan media konvensional lainnya. Kehadiran Informasi Elektronik berdampak baik bagi masyarakat maupun pemerintah untuk dapat mempermudah akses informasi. Sebelum adanya perkembangan dan inovasi teknologi, akses informasi hanya dapat dilakukan secara konvensional melalui media seperti koran, televisi, dan lainnya. Salah satu contohnya adalah situs pemerintah yang memberikan akses lebih mudah bagi masyarakat melalui internet dibandingkan dengan cara konvensional. Kehadiran informasi elektronik memberikan dampak positif dengan mempermudah akses informasi dan layanan dari pemerintah kepada masyarakat.

UU ITE sebagai bentuk dari hukum siber ditetapkan untuk mengatur pemanfaatan informasi dan transaksi elektronik agar memberikan rasa aman, keadilan, dan kepastian hukum bagi pengguna dan penyelenggara teknologi informasi, termasuk perlindungan terhadap situs-situs milik pemerintah dan memberikan pelayanan terhadap publik atau masyarakat. Salah bentuk dari implementasi tujuan perlindungan tersebut adalah adanya

pengaturan tindak pidana dalam UU ITE.[25] Tindak pidana dalam UU ITE merupakan salah bentuk pengaturan kejahatan siber di Indonesia. Kejahatan ini didefinisikan sebagai aktivitas atau perbuatan pidana apapun yang dilakukan dengan melibatkan komputer, perangkat jaringan, termasuk jaringannya. Kejahatan ini terbagi dalam *cyber-dependent crimes* dan *cyber-enabled crime*s.[26] *Cyber-enabled crimes* meliputi kejahatan tradisional yang mengadopsi teknologi informasi sebagai sumber daya, seperti penipuan, perundungan hingga pencemaran nama baik yang dilakukan di *cyberspace*, sedangkan *cyber-dependent crimes* adalah kejahatan yang menyerang komputer, perangkat dan jaringan, seperti peretasan.[27]

Josua Sitompul menjelaskan tindak-tindak pidana yang diatur dalam UU ITE di dalam Bab VII tentang perbuatan yang dilarang mengelompokkan perbuatan-perbuatan tersebut menjadi beberapa kategori, salah satu tindak pidana dalam UU ITE adalah tindak pidana yang berhubungan dengan gangguan (interferensi), yaitu gangguan terhadap informasi atau dokumen elektronik (*data interference*) (Pasal 32 UU ITE).[28] Kejahatan tersebut termasuk *cyber-dependent crimes,* yang berhubungan erat dengan penggunaan teknologi yang berbasis komputer dan jaringan telekomunikasi adalah tindak pidana yang berhubungan dengan gangguan terhadap data dan sistem (*data interference & system interference*). Josua Sitompul menerangkan bahwa tujuan pengaturan *data interference* adalah untuk menjaga kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan *(availability*) informasi atau dokumen elektronik. Pada dasarnya pihak yang memiliki hak atau kewenangan yang dapat mengambil tindakan yang mempengaruhi kerahasiaan, keutuhan, dan ketersediaan informasi atau dokumen elektronik.[29] Persoalan *data interference & system interference* yang menyerang

[25] Safiranita, Tasya, et al. "The Indonesian Electronic Information and Transactions Within Indonesia's Broader Legal Regime: Urgency for Amendment?." *Jurnal HAM*, Vol. 12, No. 3, 2021, pp. 533, https://doi.org/10.30641/ham.2021.12.533-552.
[26] Robalo, Teresa Lancry A.S., and Razwana Begum Bt Abdul Rahim. "Cyber Victimisation, Restorative Justice and Victim-Offender Panels." *Asian Journal of Criminology*, Vol. 18., No.1, 2023, pp. 61–74, https://doi.org/10.1007/s11417-023-09396-9.
[27] Robalo and Abdul Rahim.
[28] Sitompul, Josua, *Cyberspace, Cybercrime, Cyberlaw, Tinjauan Aspek Hukum Pidana.* Jakarta, Tatanusa, 2012.
[29] Ibid.

kerahasiaan, keutuhan, dan ketersediaan informasi elektronik tidak bisa dilepaskan kaitannya dengan risiko serangan siber dan keamanan siber.[30]

Perkara yang hendak dikaji adalah perbuatan peretasan yang dilakukan oleh H terhadap situs Dewan Kehormatan Penyelenggara Pemilu (DKPP). Berdasarkan Putusan Pengadilan Negeri Lahat Nomor 76/Pid.Sus/2014/PN/LT H telah dinyatakan sah bersalah melakukan tindak pidana sesuai Pasal 30 ayat (3) jo. Pasal 46 ayat (3) UU ITE. Perbuatan yang dilakukan oleh H berdasarkan perkara tersebut dapat dikaji dengan pasal tindak pidana yang berbeda berdasarkan Pasal 32 ayat (1) jo. Pasal 48 ayat (1) UU ITE yang menentukan:

> "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apapun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik."

Berdasarkan ketentuan Pasal 32 ayat (1) UU ITE tersebut, maka terdapat unsur-unsur larangan sebagai berikut: (1) Unsur pertama adalah setiap orang; (2) Unsur kedua adalah dengan sengaja dan tanpa hak atau melawan hukum; (3) Unsur ketiga adalah dengan cara apapun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu informasi elektronik dan/atau dokumen elektronik; (4) Unsur keempat adalah milik orang lain atau publik.

Berdasarkan fakta kasus yang akan dikaji, maka dikaitkan dengan perbuatan H unsur- unsur Pasal Pasal 32 ayat (1) UU ITE dapat dijelaskan sebagai berikut:

Unsur pertama Pasal 32 ayat (1) UU ITE yaitu "setiap orang" yang terdapat pada Pasal 1 angka 21 UU ITE yang menentukan bahwa: "Orang adalah orang perseorangan, baik warga negara Indonesia, warga negara asing, maupun badan hukum." Merujuk pada fakta hukum, unsur setiap orang ini telah terpenuhi pada diri H. Ia merupakan warga negara Indonesia yang telah melewati pemeriksaan di tingkat penyidikan maupun pra penuntutan yang telah ditetapkan sebagai pelaku.

[30] Cremer, Frank, et al. "Cyber Risk and Cybersecurity: A Systematic Review of Data Availability." *Geneva Papers on Risk and Insurance: Issues and Practice*, Vol. 47, No. 3, 2022, pp. 698–736, https://doi.org/10.1057/s41288-022-00266-6.

Unsur kedua Pasal 32 ayat (1) UU ITE yaitu “dengan sengaja” dan “tanpa hak atau melawan hukum”. istilah “dengan sengaja” maksudnya adalah tahu dan menghendaki dilakukannya perbuatan yang dilarang, atau tahu dan menghendaki timbulnya akibat yang dilarang. Unsur “tanpa hak” adalah tidak memiliki hak berdasarkan undang-undang, perjanjian, atau alas hukum lain yang sah. Yang dimaksud alas hukum lain yang sah misalnya berdasarkan peraturan perusahaan. Unsur “tanpa hak atau melawan hukum” adalah delik pokoknya bahwa pada dasarnya tindakan tersebut tanpa persetujuan pihak yang berhak adalah perbuatan yang dilarang. Pasal tersebut memberikan perlindungan terhadap properti dan privasi seseorang. Berdasarkan fakta hukum, H, yang tidak memiliki hak atas tindakannya, tanpa alasan hak, menggunakan aplikasi "*Cyberghost.Exe*" dan VPN untuk merubah IP Address, sehingga situs www.dkpp.go.id tidak dapat diidentifikasi. Tindakan ini menyebabkan Dian dan Saksi Idham tidak dapat mengakses situs tersebut. H berupaya menutup jejak dengan menggunakan aplikasi CyberGhost.exe, menunjukkan kesadaran bahwa tindakannya melanggar hukum. H, dengan nickname "setan dari surga," membagikan perbuatannya di akun Facebook dan meninggalkan situs tanpa mengembalikan tampilan semula. Tindakan berbagi dilakukan dengan tujuan mendapatkan pujian dari sesama hacker dalam MBT (Manusia Biasa Team).

Unsur ketiga Pasal 32 ayat (1) UU ITE yaitu dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu informasi elektronik dan/atau dokumen elektronik. Joshua Sitompul memberikan pengertian unsur “mengubah” (*alteration*) adalah melakukan modifikasi informasi atau dokumen elektronik asli atau originalnya. Pada hakikatnya unsur “mengubah” terkandung makna “penambahan” atau “pengurangan”, ketiga unsur ini untuk menegaskan tindakan-tindakan yang dimaksud. Unsur-unsur mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan merupakan unsur-unsur yang tersusun secara alternatif. H dapat melakukan salah satu dari unsur-unsur tersebut, melakukan beberapa unsur, atau melakukan seluruh unsur. Pembuktiannya dapat dilakukan terhadap satu unsur saja, terhadap beberapa unsur maupun terhadap seluruh unsur.

Berdasarkan fakta yang ada, H menanam *backdoor* sebagai alat untuk merubah file-file yang ada di server dengan cara mengupload *file backdoor* dengan ekstensi php pada sebuah postingan dengan cara menambah artikel berita dengan mengupload backdoor yang telah H simpan di harddisk dari CPU yang terdapat didalam folder Desktop>sh3ll yang diberi nama hnshell.pp. Setelah H memposting dengan menggunakan backdoor tersebut maka terdapat perubahan pada situs *www.dkpp.go.id* dari tampilan semula yaitu 7 (tujuh) orang pejabat DKPP dengan gambar dengan gambar burung garuda di pojok sebelah kiri serta ada tertulis pilihan berupa Putusan, Maklumat, Jadwal Sidang dan Form Pengaduan menjadi tampilan interface yang diubah oleh H berupa lambang berbentuk iblis dengan sayap putih dan inisial "MBT" yang merupakan singkatan dari "Manusia Biasa Team" dengan latar belakang (wallpaper) hitam dan tulisan "Tak ada yang perlu dibanggakan dari kami, hanya saja kami diciptakan sebagai orang paling tampan sedunia…" dengan inisial nickname chmod755 feat Abraham Lincoln.

Unsur keempat Pasal 32 ayat (1) UU ITE yaitu milik orang lain atau publik. Pada Pasal 1 angka 12 UU ITE memberikan pengertian unsur milik orang lain adalah orang perorangan, baik warga negara Indonesia, warga negara asing, maupun badan hukum yang menjadi korban langsung dari perbuatan yang dimaksud dalam Pasal 27 sampai Pasal 34 UU ITE. Istilah orang lain adalah kekuasaan yang didukung secara baik sosial maupun hukum untuk memegang kontrol terhadap sesuatu yang dimiliki secara eksklusif dan menggunakannya untuk pribadi. Unsur publik adalah sekelompok individu yang mempunyai kepentingan dan minat yang sama pada hal yang sama, publik tersebar dimana-mana, tidak saling mengenal, bisa besar hingga kecil tetapi dalam hal ini, situs yang diretas oleh H adalah situs pemerintah. Berdasarkan uraian penjelasan Pasal 32 ayat (1) jo. Pasal 48 ayat (1) UU ITE tersebut, maka perbuatan H telah memenuhi semua unsur dari Pasal 32 ayat (1) jo. Pasal 48 ayat (1) UU ITE.

Ketentuan pidana dalam UU ITE juga mengatur adanya pemberatan penjatuhan sanksi pidana pokok jika perbuatan-perbuatan yang dilakukan memiliki sifat-sifat yang memberatkan. Terkait dengan kasus tersebut, maka pemberatan yang dapat diterapkan adalah pemberatan berdasarkan objek tindak pidana yaitu Pasal 52 ayat (2) UU ITE yang menentukan bahwa:

> ”Dalam hal perbuatan sebagaimana dimaksud dalam Pasal 30 sampai Pasal 37 ditujukan terhadap Komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik Pemerintah dan/atau digunakan untuk layanan publik dipidana dengan pidana pokok ditambah sepertiga”.

Berdasarkan fakta kasus yang akan dikaji, maka apabila dikaitkan dengan perbuatan H, unsur-unsur dalam Pasal 52 ayat (2) UU ITE dapat dijelaskan sebagai berikut: *Unsur pertama* Pasal 52 ayat (2) UU ITE yaitu, “dalam hal perbuatan sebagaimana dimaksud dalam Pasal 30 sampai 37”. Berdasarkan fakta dalam kasus ini, tindakan H telah memenuhi salah satu pasal dalam Pasal 30 sampai Pasal 37 UU ITE yaitu Pasal 32 ayat (1) UU ITE dengan cara H mengubah suatu Informasi Elektronik dan/atau Dokumen Elektronik milik publik. Perbuatan H telah memenuhi unsur tersebut sebagaimana yang telah dijelaskan, sehingga unsur “dalam hal perbuatan sebagaimana dimaksud dalam Pasal 30 sampai 37” pada Pasal 52 ayat (3) UU ITE telah terpenuhi.

Unsur kedua Pasal 52 ayat (2) UU ITE yaitu, “ditujukan terhadap Komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik Pemerintah dan/atau digunakan untuk layanan publik.” Objek dari tindakan H yang telah memenuhi unsur pada Pasal 32 ayat (1) UU ITE adalah situs www.dkpp.go.id yang dimana situs tersebut adalah situs milik pemerintah sehingga objek perbuatan pidana dari H adalah Sistem Elektronik milik pemerintah yang pengertiannya berdasarkan Pasal 1 angka (5) UU ITE yaitu,

> “Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan Informasi Elektronik.”

Pasal 52 ayat (3) UU ITE juga menerapkan alasan yang sama yaitu dengan menerapkan pemberatan pada objek delik tetapi terdapat perbedaan yaitu objek delik yang dimaksud pada Pasal 52 ayat (3) UU ITE adalah terhadap Komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik Pemerintah dan/atau badan strategis termasuk dan tidak terbatas pada lembaga pertahanan, bank sentral, perbankan, keuangan, lembaga internasional, otoritas penerbangan yang dimana ancamannya adalah pidana maksimal ancaman pidana pokok masing-masing pasal ditambah dua pertiga.

Pemberatan pada Pasal 52 ayat (2) dan (3) UU ITE ini berpaku pada objek dari peretasan itu sendiri yaitu Komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik Pemerintah dan/atau yang digunakan untuk layanan publik dan/ atau badan strategis termasuk dan tidak terbatas pada lembaga pertahanan, bank sentral, perbankan, keuangan, lembaga internasional, otoritas penerbangan dimana apabila timbul permasalahan dalam objek-objek tersebut yang menimbulkan terhambatnya layanan publik dan tidak dapat diaksesnya kebutuhan masyarakat sehingga dapat menimbulkan permasalahan di masyarakat. Dampak dari tindak pidana yang ditujukan terhadap milik pemerintah dapat berdampak besar bagi pemerintah maupun masyarakat sendiri yang dimana kerugian yang dialami bukan bersifat privat melainkan publik sehingga diperlukan adanya pemberatan sebagai langkah preventif dan juga langkah represif bagi yang telah melakukan tindak pidana tersebut.

Berdasarkan pasal tersebut maka dapat diketahui bahwa pemberatan pidana yang dilakukan oleh H dapat ditambah sepertiga dari pidana pokok apabila objek dari tindak pidananya berupa Komputer dan/ atau Sistem Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik Pemerintah dan/atau digunakan untuk layanan publik. Pada kasus tersebut, objek dari tindak pidana yang dilakukan oleh H adalah situs *www.dkpp.go.id* sebagai situs milik pemerintah. Pemberatan ini didasarkan pada dampak kerugian yang ditimbulkan oleh *cyber crime* yang dimana *cybercrime* yang dimaksud adalah kejahatan terhadap sistem atau jaringan komputer. Sistem elektronik yang menjadi objek perbuatan pidana dari H adalah Informasi Elektronik dan/ atau Sistem Elektronik milik pemerintah yang pengertiannya diatur dalam UU ITE. Menurut Pasal 1 UU ITE "Informasi Elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *electronic data interchange (EDI)*, surat elektronik (*electronic mail*), telegram, teleks, telecopy atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya" sedangkan, "Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan Informasi Elektronik." Situs *www.dkpp.go.id* adalah informasi elektronik milik DKPP.

Berdasarkan Undang-Undang No. 7 Tahun 2017, DKPP adalah lembaga yang bertugas menangani pelanggaran kode etik Penyelenggara Pemilu dan merupakan satu kesatuan fungsi penyelenggaraan Pemilu. DKPP merupakan lembaga negara yang dibentuk untuk memeriksa dan memutuskan pengaduan dan/atau laporan adanya dugaan pelanggaran kode etik yang dilakukan oleh KPU, Bawaslu beserta jajarannya di antaranya anggota KPU, anggota KPU Provinsi, anggota KPU Kabupaten/Kota, anggota PPK, anggota PPS, anggota PPLN, anggota KPPS, anggota KPPSLN, anggota Bawaslu, anggota Bawaslu Provinsi dan anggota Panwaslu Kabupaten/Kota, anggota Panwaslu Kecamatan, anggota Pengawas Pemilu Lapangan dan anggota Pengawas Pemilu Luar Negeri. [31] Lembaga DKPP bermula pada tahun 2008 dengan dibentuknya Dewan Kehormatan Komisi Pemilihan Umum (DK KPU). Lembaga ini adalah institusi etik bersifat *ad-hoc*. yang dibentuk berdasarkan amanat Undang-Undang Nomor 22 Tahun 2007, namun belum mempunyai kewenangan yang kuat, lembaga ini hanya memiliki kewenangan memanggil, memeriksa, dan menyidangkan hingga memberikan rekomendasi kepada KPU. Guna mendorong misi untuk meningkatkan kapasitas wewenang dan memastikan institusi ini jadi tetap dan tidak hanya menangani Kode Etik pada KPU tapi juga Bawaslu di tiap tingkatan maka dibentuklah DKPP secara resmi lahir pada tanggal 12 Juni 2012.[32]

DKPP sebagai lembaga negara tidak bisa dipisahkan dengan pengertian sebagai lembaga pemerintahan. Lembaga negara dalam konsep hukum tata negara dapat dibagi kedalam lembaga negara yang langsung (*unmittelbare* organ) dan lembaga pemerintahan sebagai lembaga negara yang tidak langsung (*mittenbare organ*). Jimly Asshiddiqie sebagaimana dikutip oleh Saldi Isra[33] menyebut bahwa lembaga Negara terkadang disebut dengan lembaga lembaga pemerintahan, pemerintahan non departemen dan lembaga negara saja.[34] DKPP secara kelembagaan memiliki tugas dan wewenang berkaitan dengan pemeriksaan, pemberian sanksi dan memutus adanya pelanggaran kode

[31] Rosnawati, Rosnawati. "Dinamika Penegakan Kode Etik Penyelenggara Pemilu Di Indonesia." *Jurnal Bawaslu Provinsi Kepulauan Riau*, Vol. 4, No.1, 2022, pp. 45–54, https://doi.org/10.55108/jbk.v4i1.104
[32] Chakim, M. Lutfi. "Desain Institusional Dewan Kehormatan Penyelenggara Pemilu (DKPP) Sebagai Peradilan Etik." *Jurnal Konstitusi*, Vol. 11, No. 2, 2016, pp. 393, https://doi.org/10.31078/jk11210.
[33] Isra, Saldi, *Lembaga Negara: Konsep, Sejarah, Wewenang Dan Dinamika Konstitusional/* Depok, Rajawali Pers, 2020.
[34] Rayhan, Ahmad, and Qotrun Nida. "Hierarkie Lembaga Negara Di Indonesia." *Sultan Jurisprudence: Jurnal Riset Ilmu Hukum*, Vol.1, No. 1, 2021, pp. 67–78, https://doi.org/10.51825/sjp.v1i1.11373.

etik oleh penyelenggara pemilu. DKPP sendiri dapat membentuk peraturan DKPP dan menetapkan keputusan DKPP.[35]

Situs *www.dkpp.go.id* sendiri memiliki beberapa fitur di antaranya (1) Pengaduan, berikut panduan, formulir dan hasil verifikasi pengaduan; (2) Jadwal Sidang, mulai dari sidang pemeriksaan hingga putusan; (3) Risalah Sidang Pemeriksaan; dan (4) Hasil Putusan DKPP; (5) Call Centre DKPP termasuk email dan berbagai media sosial DKPP. Fitur-fitur tersebut juga secara khusus digunakan sebagai bentuk pelayanan terhadap pemeriksaan pelanggaran etik dalam penyelenggaran pemilu. Disamping itu, publik juga bisa mengakses informasi berupa (1) Profil DKPP, (2) Publikasi baik dalam bentuk aktivitas, rilis pers dan bahan Pustaka (3) Peraturan, (2) DKPP Video (3) PPID/ Pejabat Pengelola Informasi dan Dokumentasi. (4) JDIH/ Jaringan Dokumentasi Informasi Hukum dan (5) CSIRT/ *Computer Security Incident Response Team.* Lembaga DKPP juga melaporkan kinerjanya pada masyarakat sesuai prinsip-prinsip umum pemerintahan yang baik dan sebagai bagian dari kewajiban pelaksanaan asas-asa keterbukaan dan tanggung jawab. Pelaksanaan kinerja dan kewajiban tersebut merupakan amanat dari Undang Undang No. 14 Tahun 2008 Tentang Keterbukaan Informasi Publik.

Berdasarkan penjelasan tersebut, maka Pasal 52 ayat (2) UU ITE dalam hal ini dapat diterapkan dalam perbuatan yang dilakukan oleh H. Objek dari perbuatan peretasan H adalah situs milik DKPP sebagai lembaga negara atau lembaga milik pemerintah yang memiliki tugas dan wewenang berkaitan dengan pemeriksaan, pemberian sanksi dan memutus adanya pelanggaran kode etik oleh penyelenggara pemilu. Situs tersebut juga dipergunakan untuk berbagai pelayanan publik yang berhubungan dengan pelanggaran kode etik oleh penyelenggara pemilu, termasuk di antaranya pengaduan hingga berbagai layanan informasi terkait dengan DKPP beserta tugas dan kewenangannya. Tindakan peretasan oleh H membuat akses dan penggunaan situs tersebut terganggu. Hal ini juga sejalan dengan pernyataan saksi Purnomo HS selaku pekerja di Subdit IT dan *Cyber Crime* Direktorat Tindak Pidana Ekonomi Khusus Bareskrim Polri sebagai penyidik yang tuga sehari-harinya adalah melakukan kegiatan penyelidikan dan penyidikan yang

[35] Syaefudin, Muhammad, and Kadi Sukarna. "Kewenangan Dewan Kehormatan Penyelenggara Pemilu (DKPP) Dalam Menegakan Kode Etik Pelanggaran Pemilihan Umum." *Jurnal USM Law Review*, Vol. 1, No. 2, 2018, pp. 104–20, http://dx.doi.org/10.26623/julr.v2i1.2261.

berhubungan dengan tindak pidana siber. Saksi Purnomo HS menyatakan bahwa berdasarkan hasil Analisa log file situs *www.dkpp.go.id* yang telah di *hack deface* yang dilakukan terhadap situs DKPP mengakibatkan situs tersebut tidak bisa dibuka dan digunakan secara normal sebagaimana mestinya.

H sebagai pelaku bertanggung jawab atas perbuatannya dengan sengaja melakukan tindakan retas situs *www.dkpp.go.id*. Motivasi H adalah kepuasan diri dan keinginan untuk mendapatkan pujian dari sesama *hacker* dalam MBT (Manusia Biasa Team). H mengetahui bahwa DKPP adalah lembaga pemerintah dan telah meretas sekitar 50 situs pribadi. H memiliki kemampuan untuk membedakan perbuatan yang sesuai dan melawan hukum, dan mengetahui bahwa tindakannya salah. Setelah berhasil mengubah tampilan situs, H membagikan perbuatannya di akun Facebook dengan nama "setan dari surga" dan alamat email chmodrwxrwx@yahoo.co.id untuk memenuhi motifnya, lalu meninggalkan situs tanpa mengembalikan tampilan semula maka perbuatan H juga dianggap memenuhi unsur kesalahan.

III. CONCLUSION

H terbukti yang melakukan peretasan dengan mengubah tampilan atau *interface* situs *www.dkpp.go.id* sebagai situs milik Dewan Kehormatan Penyelenggara Pemilu (DKPP). Peretasan yang dilakukan H terhadap situs milik Dewan Kehormatan Penyelenggara Pemilu (DKPP) tersebut merupakan tindak pidana melakukan peretasan dengan mengubah, menambah suatu sistem elektronik milik publik sesuai Pasal 32 ayat (1) jo. Pasal 48 ayat (1) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah beberapa kali terakhir dengan Undang-Undang No. 1 Tahun 2024. Perbuatan H yang melakukan peretasan terhadap situs milik Dewan Kehormatan Penyelenggara Pemilu (DKPP) juga memenuhi unsur pemberatan tindak pidana sesuai Pasal 52 ayat (2) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah beberapa kali terakhir dengan Undang-Undang No. 1 Tahun 2024, karena situs *www.dkpp.go.id* merupakan situs milik pemerintah dan/ atau dipergunakan untuk layanan publik. Situs tersebut milik DKPP sebagai lembaga pemerintah yang memiliki tugas dan wewenang berkaitan dengan pemeriksaan, pemberian sanksi dan memutus adanya pelanggaran kode etik oleh

penyelenggara pemilu. Situs tersebut juga dipergunakan untuk berbagai pelayanan publik yang berhubungan dengan pelanggaran kode etik oleh penyelenggara pemilu, termasuk di antaranya pengaduan hingga berbagai layanan informasi terkait dengan DKPP beserta tugas dan kewenangannya. Oleh karena itu, H dapat dikenakan penambahan sanksi pidana satu per tiga atau sepertiga dari pidana pokok dalam Pasal 32 ayat (1) jo. Pasal 48 ayat (1) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah beberapa kali terakhir dengan Undang-Undang No. 1 Tahun 2024.

BIBLIOGRAPHY

Books

Arief, Barda Nawawi, *Bunga Rampai Kebijakan Hukum Pidana: Perkembangan Penyusunan Konsep KUHP Baru.* Jakarta, Kencana, 2011.

Chazawi, Adami, *Pelajaran Hukum Pidana (Bagian 1) : Stelsel Pidana, Tindak Pidana, Teori-Teori Pemidanaan & Batas Berlakunya Hukum Pidana.* Jakarta, Rajawali Pers, 2013.

Hamzah, Andi, *Asas-Asas Hukum Pidana Di Indonesia Dan Perkembangannya.* Jakarta, Sofmedia, 2018.

Isra, Saldi, *Lembaga Negara: Konsep, Sejarah, Wewenang Dan Dinamika Konstitusional/* Depok, Rajawali Pers, 2020.

Marzuki, Peter Mahmud, *Penelitian Ilmu Hukum.* Jakarta, Kencana, 2011.

Roberts, Julian V., *Mitigation and Aggravation at Sentencing.* Cambri, Cambridge University Press, 2011

Sitompul, Josua, *Cyberspace, Cybercrime, Cyberlaw, Tinjauan Aspek Hukum Pidana.* Jakarta, Tatanusa, 2012.

Journals

Alkaabi, Ali, et al. "Dealing with the Problem of Cybercrime', *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications*

Engineering, *Vol.* 53, 2011, pp 1–18, https://doi.org/10.1007/978-3-642-19513-6_1.

Andini, Ni Komang Triana, et al. "Cybercrime and Threats to the Electoral System." *Journal of Digital Law and Policy, Vol.* 3, No. 1, 2023, pp. 26–37 https://doi.org/10.58982/jdlp.v3i1.508.

Anjari, Warih. "Penerapan Pemberatan Pidana Dalam Tindak Pidana Korupsi." *Jurnal Yudisial*, Vol. 15, No. 2, 2023, pp. 263, https://doi.org/10.29123/jy.v15i2.507.

Benuf, Kornelius, and Muhamad Azhar. "Metodologi Penelitian Hukum Sebagai Instrumen Mengurai Permasalahan Hukum Kontemporer." *Gema Keadilan*, No. 7, No. 1, 2020, pp. 20–33, https://doi.org/10.14710/gk.2020.7504.

Butarbutar, Russel. "Kejahatan Siber Terhadap Individu : Jenis , Analisis , Dan Perkembangannya." *Journal Technology and Economiacs Law*, Vol. 2, No. 2, 2023, pp. 297–316, https://scholarhub.ui.ac.id/telj/vol2/iss2/3/.

Chakim, M. Lutfi. "Desain Institusional Dewan Kehormatan Penyelenggara Pemilu (DKPP) Sebagai Peradilan Etik." *Jurnal Konstitusi*, Vol. 11, No. 2, 2016, pp. 393, https://doi.org/10.31078/jk11210.

Cremer, Frank, et al. "Cyber Risk and Cybersecurity: A Systematic Review of Data Availability." *Geneva Papers on Risk and Insurance: Issues and Practice*, Vol. 47, No. 3, 2022, pp. 698–736, https://doi.org/10.1057/s41288-022-00266-6.

Franjić, Siniša. "Cybercrime Is Very Dangerous Form of Criminal Behavior and Cybersecurity." *Emerging Science Journal*, Vol. 4, No. 18, 2020, pp. 18–26, https://doi.org/10.28991/esj-2020-SP1-02.

Gulyas, Oliver, and Gabor Kiss. "Impact of Cyber-Attacks on the Financial Institutions." *Procedia Computer Science*, Vol. 219, 2023, No. 84–90, https://doi.org/10.1016/j.procs.2023.01.267.

Irmawanti, et al. "Urgensi Tujuan Dan Pedoman Pemidanaan Dalam Rangka Pembaharuan Sistem Pemidanaan Hukum Pidana." *Jurnal Pembangunan Hukum Indonesia*, Vol. 3, No. 2, 2021, pp. 217–27, https://doi.org/10.14710/jphi.v3i2.217-227.

Lisanawati, Go. "Menyoal Pemberatan Pidana Sepertiga Dan Duapertiga Pada UU ITE Dan Harmonisasinya Atas RUU KUHP." in *Problematika Pembaharuan Hukum Nasional*, 2013, pp. 107–115, http://repository.ubaya.ac.id/id/eprint/9554.

Mulasari, Laila. "Ajaran Pertanggungjawaban Pidana Korporasi dalam Kebijakan Hukum Pidana di Bidang Mayantara." *Hukum dan Dinamika Masyarakat, Vol.* 9, No. 2, 2012, pp. 113–120, http://dx.doi.org/10.56444/hdm.v9i2.301.

Rahmawati, Melinda, et al. "The Era of Society 5.0 as the Unification of Humans and Technology: A Literature Review on Materialism and Existentialism." *Jurnal Sosiologi Dialektika*, Vol. 16. No. 2, 2021, pp. 151-162, https://doi.org/10.20473/jsd.v16i2.2021.151-162.

Rayhan, Ahmad, and Qotrun Nida. "Hierarkie Lembaga Negara Di Indonesia." *Sultan Jurisprudence: Jurnal Riset Ilmu Hukum*, Vol.1, No. 1, 2021, pp. 67–78, https://doi.org/10.51825/sjp.v1i1.11373.

Robalo, Teresa Lancry A.S., and Razwana Begum Bt Abdul Rahim. "Cyber Victimisation, Restorative Justice and Victim-Offender Panels." *Asian Journal of Criminology*, Vol. 18., No.1, 2023, pp. 61–74, https://doi.org/10.1007/s11417-023-09396-9.

Rosnawati, Rosnawati. "Dinamika Penegakan Kode Etik Penyelenggara Pemilu Di Indonesia." *Jurnal Bawaslu Provinsi Kepulauan Riau*, Vol. 4, No.1, 2022, pp. 45–54, https://doi.org/10.55108/jbk.v4i1.104

Safiranita, Tasya, et al. "The Indonesian Electronic Information and Transactions Within Indonesia's Broader Legal Regime: Urgency for Amendment?." *Jurnal HAM*, Vol. 12, No. 3, 2021, pp. 533, https://doi.org/10.30641/ham.2021.12.533-552.

Syaefudin, Muhammad, and Kadi Sukarna. "Kewenangan Dewan Kehormatan Penyelenggara Pemilu (DKPP) Dalam Menegakan Kode Etik Pelanggaran Pemilihan Umum." *Jurnal USM Law Review*, Vol. 1, No. 2, 2018, pp. 104–20, http://dx.doi.org/10.26623/julr.v2i1.2261.

Umanailo, M. Chairul Basrun, et al. "Cybercrime Case as Impact Development of Communication Technology That Troubling Society." *International Journal of Scientific and Technology Research*, Vol. 8, No. 9, 2019, pp. 1224–1228, http://repository.iainkediri.ac.id/id/eprint/630.

Law and Regulations

Law No. 1 of 2024 on the Second Amendment to Law No. 11 of 2008 on Information and Electronic Transactions

Law No. 7 of 2017 on General Elections

Law No. 14 of 2008 on Openness of Public Information

Court Verdicts

Lahat District Court Decision No. 76/Pid.Sus/2014/PN.LT

Online Resources

CNN. "RI Dihantam 700 Juta Serangan Siber Di 2022, Modus Pemerasan Dominan." *CNN Indonesia*, 2022, https://www.cnnindonesia.com/teknologi/20220701164212-192-816150/ri-dihantam-700-juta-serangan-siber-di-2022-modus-pemerasan-dominan.