ISSN 2541-6502
E-ISSN 2776-9844

AKTUAL JUSTICE
JURNAL ILMIAH MAGISTER HUKUM
PASCASARJANA UNIVERSITAS NGURAH RAI

KEJAHATAN DUNIA MAYA: ILLEGAL AKSES DIKAJI DARI PUTUSAN NOMOR 41/PID.SUS/2020/PN MAR

Agnes Rolanda[1], Aksel Stefan Wenur[2], Cindy Destiani[3], Raden Ayu Rani Mutiara Dewi[4], Slamet Riyadi[5],Rizky Karo Karo[6]

[1]Fakultas Hukum Universitas Pelita Harapan, Email: agnesrolanda18@gmail.com
[2]Fakultas Hukum Universitas Pelita Harapan, Email: wenuraksel@gmail.com
[3]Fakultas Hukum Universitas Pelita Harapan, Email: cindy.destiani23@gmail.com
[4]Fakultas Hukum Universitas Pelita Harapan, Email: ranimutiara056@gmail.com
[5]Fakultas Hukum Universitas Pelita Harapan, Email: riyadislamat14@gmail.com
[6]Program Doktor Hukum Universitas Pelita Harapan, Email: rizky.karokaro@uph.edu

Abstract

Cybercrime has garnered national and global attention due to its frequent occurrences disregarding national or territorial boundaries. Amidst the complex dynamics of cybercrime, Illegal Access stands out as one of the increasingly prevalent forms of crime in the digital era. This condition underscores the necessity for robust legal frameworks to effectively handle cases of Illegal Access and prosecute hackers. Predictions of cybercrime becoming one of the largest criminal activities in the future further emphasize the urgency of addressing this issue. This journal will analyze a case of website hacking involving the defendant intentionally conducting Illegal Access to electronic systems with the aim of obtaining and modifying others' electronic information. This analysis is based on court decision number 41/Pid.Sus/2020/PN. Mar The research method used by researchers in this study is a qualitative approach with a descriptive method.. Consequently, this journal aims to clarify the legal implications and security ramifications arising from such cyber attacks. The importance of implementing and enforcing effective legal measures to respond to cybercrime threats is the focal point in addressing this challenge comprehensively.

Keywords : cyber, illegal access, hacker.

Abstrak

Kejahatan cyber telah menjadi perhatian nasional dan global karena sering terjadi tanpa memandang batas negara atau wilayah. Di tengah dinamika kompleks kejahatan cyber, Illegal Akses menonjol sebagai salah satu bentuk kejahatan yang semakin meningkat di era digital. Kondisi ini menunjukkan perlunya pilar hukum yang kokoh untuk menangani kasus-kasus Illegal Akses dan Mengadili Hacker dengan efektif. Prediksi akan mendudukinya kejahatan cyber sebagai salah satu kejahatan terbesar di masa mendatang memperkuat urgensi dalam menangani masalah ini. Jurnal ini akan menganalisis kasus peretasan situs web e-Dikbang Polri yang melibatkan terdakwa yang sengaja melakukan Illegal Akses terhadap sistem elektronik dengan tujuan memperoleh dan memodifikasi informasi elektronik milik orang lain. Analisis ini didasarkan pada putusan pengadilan Nomor 41/Pid.Sus/2020/PN. Mar. Metode penelitian yang digunakan peneliti dalam penelitian ini adalah pendekatan kualitatif dengan metode deskriptif. Dengan demikian, jurnal ini bertujuan untuk mengklarifikasi implikasi hukum dan keamanan informasi yang muncul akibat serangan siber tersebut. Pentingnya implementasi dan penegakan hukum yang efektif dalam

menanggapi ancaman kejahatan cyber menjadi fokus dalam upaya mengatasi tantangan ini secara menyeluruh.

Kata Kunci : Cyber, Illegal Akses, Hacker

1. Pendahuluan

Maraknya peretasan sistem dan *website* pemerintah yang dilakukan oleh *cracker* mengakibatkan kerugian pada masyarakat. C*racker* atau aktivitasnya disebut *cracking*, terhadap sistem elektronik (*website*) memiliki lingkup yang sangat luas, seperti pembajakan akun milik orang lain, aktivitas mata-mata (*probing*), menyebarkan virus, melumpuhkan target sasaran, hingga pembajakan situs web.[1] Setidaknya, *cracker* melakukan perubahan tampilan (*deface*) *website* sebagai petunjuk bahwa *cracker* telah berhasil masuk ke sistem yang diretas.

Perbuatan *cracker* menjadikan teknologi informasi (TI) sebagai sasaran dalam melakukan perbuatannya dengan tujuan mendapatkan keuntungan materil dari kemampuan dan pengetahuan yang mereka miliki atau memiliki tujuan tertentu lainnya.[2] Dari aktivitasnya tersebut, dapat dipahami bahwa *cracking* merupakan akses tidak sah yang dilakukan seseorang terhadap komputer, sistem elektronik hingga *website* milik individu, badan usaha, bahkan pemerintah, yang dilakukan dengan maksud dan tujuan tertentu.

Sebagai kejahatan, *cracking* dapat menyebabkan kerugian besar, baik dalam bentuk finansial maupun non-finasial. Tentunya setiap *website* mempunyai sebuah sistem atau jaringan agar bisa berjalan dengan lancar. Cara cracker dapat masuk kedalam server sebuah *website* adalah dengan mencari celah pada sistem keamanan dan merusaknya. Dampaknya menjadikan sistem yang sudah bangun tidak berjalan dengan lancar, pelayanan publik menjadi terhambat, menurunnya kepercayaan masyarakat, sampai harus mengadakan pemeliharaan ataupun perbaikan sistem yang memerlukan biaya mahal.

[1] Abidin, Dodo Zaenal. 2015. *Kejahatan Dalam Teknologi Informasi Dan Komunikasi*, Jurnal Ilmiah Media Processor Vol.10 No.2. ISSN 1907-6738, hlm.511

[2] Silic, Mario. Lowry, Paul Benjamin. 2019. *Breaking Bad in Cyberspace: Understanding why and how Black Hat Hackers Manage their Nerves to Commit their Virtual Crimes*. Springer. hlm. 330-331.

Jumlah kasus yang telah diterima Pusat Operasi Keamanan Siber Nasional Badan Siber Dan Sandi Negara tersebut mengindikasikan bahwa sistem elektronik pada sektor pemerintahan selalu memiliki daya tarik bagi para cracker untuk terus melakukan serangan hingga perusakan. Para pemilik sistem tentu tidak akan melaporkan serangan-serangan tersebut kepada Pusat Operasi Keamanan Siber Nasional Badan Siber Dan Sandi Negara apabila para cracker telah mendapat izin dari pemilik sistem. Dengan demikian, perbuatan para cracker tersebut masuk pada kategori "akses tidak sah (illegal access).

Secara aturan, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) menjamin perlindungan pada sistem elektronik, infromasi elektronik dan dokumen elektronik dari perbuatan akses tidak sah, lebih tepatnya pada Pasal 30 ayat (3) UU ITE yang menyatakan bahwa "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." Aturan ini dipertegas dengan adanya ketentuan pidana sebagaimana dituangkan pada Pasal 46 ayat (3) dengan ancama pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak banyak Rp800.000.000,00 (delapan ratus juta rupiah). Pada umumnya, kejahatan cracking tidak hanya sebatas membobol suatu sistem, akan tetapi juga memberikan gangguan pada sistem dan dokumen, sehingga rangkaian tindakan cracker dapat memenuhi unsur Pasal 32 dan Pasal 33 UU ITE.

Secara khusus, UU ITE memberikan perlindungan hukum terhadap website- website milik pemerintah dari berbagai akses tidak sah sebagaimana diatur pada Pasal 52 ayat (2) UU ITE; 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. Ketentuan ini tentu menjadikan perbuatan yang dilakukan oleh para cracker pada website milik

pemerintah termasuk kedalam tindak pidana yang terkualifikasi, dimana unsur "milik pemerintah untuk layanan publik" merupakan objek tertentu (khas) sehingga termasuk pada tindak pidana yang ancaman pidananya lebih berat.

Aparat penegak hukum berusaha dengan baik untuk menerapkan aturan tentang pemberatan pidana yang telah ditetapkan oleh negara terhadap para cracker yang melakukan cracking pada website-website milik pemerintah. Upaya tersebut dilakukan dalam kerangka penegakan hukum pidana sebagai suatu upaya penanggulangan kejahatan. Seperti dalam kasus cracking putusan Pengadilan Negeri Lamongan Nomor 86/Pid.Sus/2018/PN Lmg yang dilakukan oleh Trisna Handryanto alias MR.Bl4ckr053 terhadap website bareskrim POLRI. Dari perbuatannya tersebut, menjadikan website http://bareskrim.sipp.polri.go.id tidak dapat diakses sebagaimana mestinya serta terjadi perubahan pada tampilan (deface) website. Trisna didakwa secara alternatif yaitu Pasal 30 ayat (3) atau Pasal 32 ayat (1) UU ITE yang masing-masing pasal tersebut dikaitkan ke Pasal 52 ayat (2) UU ITE. Begitu juga pada kasus putusan Pengadilan Negeri Sleman Nomor 527/Pid.Sus/2020/PN Smn yang dilakukan oleh seorang cracker bernama Agus Dwi Cahyo alias Adhacker terhadap website-website milik beberapa instansi penyelenggara negara. Agus didakwa secara subsidair yaitu Pasal 32 ayat (2) dan Pasal 30 ayat (1) UU ITE. Masing-masing pasal tersebut dikaitkan ke Pasal 52 ayat (2) UU ITE.

Berbeda dengan kasus berikut yang semestinya dapat juga diterapkan Pasal 52 ayat (2) UU ITE sebagaimana kasus Trisna dan Agus diatas. Penerapan aturan pemberatan tersebut tidak selalu digunakan. Seharusnya pasal pemberatan pidana pada beberapa kasus cracking website milik pemerintah berikut juga dapat diterapkan, tapi pasal tersebut tidak ditemukan dalam dakwaan Jaksa Penuntut Umum. Seperti kasus pada putusan Pengadilan Negeri Marisa Nomor 41/Pid.Sus/2020/PN Mar oleh cracker Ramdan Yantu yang mengakses secara tidak sah dan merubah tampilan (deface) website http://e-dikbang.ssdm.polri.go.id milik POLRI, kasus pada putusan Pengadilan Negeri Bangil Nomor 16/Pid.Sus/2020/PN Bil oleh cracker Alfian

Buyung Suprapto alias Security 007 yang menerobos dan merubah tampilan (deface) website www.kemendagri.go.id milik Kementerian Dalam Negeri Republik Indonesia, dan juga kasus pada putusan Pengadilan Negeri Jember Nomor 17/Pid.Sus/2021/PN Jmr terkait penjebolan website milik Komisi Pemilihan Umum (KPU) Kabupaten Jember yang dilakukan oleh cracker David Ariansyah alias Chu404 dan menjual aksesnya kepada terdakwa lain yang merupakan anak berusia empat belas tahun.

Dakwaan terhadap Trisna Handryanto dan Agus Dwi Cahyo menggunakan UU ITE dan menerapkan Pasal 52 ayat (2) sebagai pemberatan pidananya. Sementara dakwaan terhadap Ramdan Yantu, Alfian Buyung Suprapto, dan David Ariansyah menggunakan UU ITE namun tidak menerapkan Pasal 52 ayat (2). Sementara perbuatan Ramdan, Alfian dan David sangat jelas ditujukan kepada website-website milik institusi pemerintah. Perbedaan dalam penerapan hukum seperti kasus yang telah dijabarkan tentu saja dapat mencederai keadilan dan kepastian hukum bagi masyarakat. Perbedaan perspektif aparat penegak hukum dalam objek cracker sebagai sistem elektronik milik orang lain, atau sebagai sistem elektronik milik pemerintah mengakibatkan perbedaan dalam penegakan hukum.

Perbedaan dalam penerapan Pasal 52 ayat (2) UU ITE kiranya perlu digali secara mendalam pada tulisan ini agar terlihat bagaimana penerapan unsur "milik pemerintah dan/atau yang digunakan untuk layanan publik". Unsur tersebut ditetapkan sebagai unsur pemberat pidana dalam UU ITE sehingga perlu ditinjau dari tujuan hukumnya. Landasan teori yang digunakan untuk menjawab pertanyaan penelitian adalah teori tujuan hukum yang pada intinya tiga tujuan hukum yaitu, keadilan, kemanfaatan, dan kepastian. Ahmad Ali dalam Viktorius Hamsa dari sudut pandang hukum positif-normatif, tujuan hukum dititik beratkan pada segi kepastian hukum.[3] Dari sudut pandang

[3] Hamsa, Iktorius. Tesis, 2013, "*Tinjauan Yuridis Persetujuan Tindakan Kedokteran Di Rumah Sakit Umum Daerah Salewangang Maros*". Program Pasca Sarjana Universitas Hasanuddin, Makassar. hlm. 39.

filsafat hukum, tujuan hukum dititik beratkan pada keadilan, sedangkan dari sudut pandang sosiologis hukum, tujuan hukum dititik beratkan pada kemanfaatannya. Teori yang konvensional ini menganggap tujuan hukum hanya untuk mewujudkan salah satunya saja dari tiga tujuan hukum, sedangkan teori prioritas yang dipelopori oleh Gustav Radbruch menerima ketiganya sekaligus sebagai tujuan hukum.

Penelitian ini berbeda dengan penelitian terdahulu yang membahas tentang kejahatan cracking yang dilakukan oleh cracker. Seperti penelitian yang dilakukan oleh Christiara Febriliani, Ismunarno, Diana Lukitasari "Kajian Etiologi Kriminal Tindak Pidana Cracking Sistem Operasi Windows Di Provinsi Daerah Istimewa Yogyakarta". Penyebab terjadinya tindak pidana cracking sistem operasi Windows di Provinsi Daerah Istimewa Yogyakarta adalah faktor ekonomi, sosial dan budaya, masyarakat dan hukum.[4] Penelitian lainnya berjudul "Penegakan Hukum Terhadap Tindak Pidana Peretasan Sebagai Bentuk Kejahatan Mayantara (Cyber Crime)". Penelitian ini membahas perbuatan hacking telah melanggar keseluruhan Pasal 30 UU ITE dan dapat diberikan sanksi pidana sesuai Pasal 46 UU ITE. Dalam upaya penanggulangan kejahatan dilakukan upaya preventif dan upaya represif. Penelitian berjudul "Sanksi Hukum Kejahatan Peretasan Website Presiden Republik Indonesia" yang melihat peretasan dalam perspektif hukum pidana islam. Tindak pidana peretasan sebagaimana diatur juga pada Pasal 30 ayat (1) UU ITE bisa dianalogikan seperti memasuki rumah orang lain tanpa izin. Persamaan unsur terlarang dari tindak pidana peretasan ini adalah unsur tanpa izin.[5]

Kasus peretasan situs web resmi Kepolisian Republik Indonesia (Polri) merupakan salah satu insiden yang menunjukkan kelemahan dalam sistem keamanan siber di Indonesia. Pada saat situs web Polri diretas, hal ini dapat

[4] Febriliani, Christiara. Ismunarno, Lukitasari, Diana. *Kajian Etiologi Kriminal Tindak Pidana Cracking Sistem Operasi Windows Di Provinsi Daerah Istimewa Yogyakarta*, Recidive Volume 8 No. 3, Sept. - Des. 2019, pp.221 ISSN: 24

[5] Nugroho, Irzak Yuliardy. "*Sanksi Hukum Kejahatan Peretasan Website Presiden Republik Indonesia*", Al-Daulah: Jurnal Hukum Dan Perundangan Islam, Vol. 5, No. 1, April 2015; ISSN 2089-0109, pp.171- 203

menimbulkan dampak yang serius, tidak hanya bagi institusi kepolisian itu sendiri, tetapi juga bagi keamanan nasional dan citra negara secara keseluruhan. Peretasan situs web Polri bisa terjadi karena berbagai faktor, mulai dari kurangnya pembaruan sistem keamanan, lemahnya pemantauan terhadap aktivitas mencurigakan, hingga minimnya kesadaran akan pentingnya keamanan siber. Serangan ini bisa berupa pencurian data, penyebaran informasi palsu atau *malware*, serta akses ilegal ke informasi rahasia yang dapat membahayakan keamanan publik. Selain merugikan secara finansial dan reputasi, peretasan situs web Polri juga dapat memberikan sinyal negatif terhadap kemampuan pemerintah dalam melindungi data dan informasi yang dimiliki. Hal ini menjadi perhatian serius karena sistem keamanan siber yang lemah dapat dimanfaatkan oleh pihak-pihak yang tidak bertanggung jawab untuk melakukan tindakan kriminal dan merugikan banyak pihak.

Kasus peretasan situs web Polri juga mencerminkan pentingnya peningkatan kesiapan dalam menghadapi ancaman siber di era digital ini. Perkembangan teknologi yang pesat mengharuskan pihak-pihak terkait untuk terus mengevaluasi dan memperkuat sistem keamanan mereka agar mampu menangkal serangan siber secara efektif. Penyusupan ke dalam situs web Polri harus dianggap sebagai peringatan serius untuk meningkatkan proteksi data dan informasi penting. Menyikapi kasus peretasan situs web Polri, langkah-langkah yang akan diambil diharapkan dapat mencakup peningkatan keamanan sistem, pelatihan bagi personil yang terkait dengan keamanan siber, pemantauan terkait aktivitas tidak sah secara lebih intensif, dan penguatan mekanisme investigasi untuk mengidentifikasi pelaku dan mencegah serangan serupa di masa depan. Kolaborasi antara pihak internal dan eksternal juga diperlukan guna memperkuat pertahanan siber secara menyeluruh. Keseluruhan permasalahan yang muncul akibat peretasan situs web Polri memerlukan penanganan yang komprehensif dan terintegrasi antara berbagai pihak terkait. Memberikan perhatian yang lebih serius terhadap keamanan siber bukan hanya menjadi tugas Polri sebagai institusi kepolisian, tetapi juga tanggung jawab

bersama bagi seluruh pihak terkait untuk menjaga keamanan dan ketertiban dalam dunia maya.

2. Metode Penelitian

Metode penelitian yang digunakan peneliti dalam penelitian ini adalah pendekatan kualitatif dengan metode deskriptif. Metode penelitian yang digunakan adalah metode kualitatif. "Metodologi adalah proses, prinsip, dan prosedur yang kita gunakan untuk mendekati problem dan mencari jawaban"[6]. Menurut Sugiyono, metode penelitian kualitatif merupakan suatu penelitian yang digunakan untuk meneliti pada objek yang alamiah dimana peneliti adalah sebagai instrumen kunci, teknik pengumpulan data dilakukan secara gabungan, analisis data bersifat induktif, dan hasil penelitian kualitatif lebih menekankan makna daripada generalisasi[7]. Tujuan dari penelitian deskriptif ini adalah untuk membuat deskripsi, gambaran atau lukisan secara sistematis, faktual dan akurat mengenai fakta-fakta, sifat-sifat serta hubungan antar kasus yang diselidiki. Peneliti menggunakan metode penelitian normatif dengan pendekatan perundang-undangan[8], dan pendekatan kasus.

[6] Mulyana, Dedy. (2008). *Metodologi Penelitian Kualitatif.* Bandung: PT Remaja Rosdakarya, hlm. 146.

[7] Sugiyono. (2007). *Metode Penelitian Kuanitatif, Kualitatif, dan R&D*. Bandung: Alfabeta. Hlm. 2.

[8] Panjaitan, Ananda Chrisna D.. (2023). *Penegakan Hukum Pidana Internasional di Yaman*. *Jurnal Aktual Jusice Vol. 8, No. 2*

3. Hasil Dan Pembahasan

a. Klasifikasi Illegal Akses Sebagai Penyebab Ketidakamanan Sistem Elektronik

Dalam Klasifikasi *Cybercrime*, salah satu tindakan melanggar yang sangat disoroti adalah akses ilegal terhadap komputer atau sistem elektronik milik orang lain serta manipulasi terhadap informasi elektronik atau dokumen elektronik yang dimiliki orang lain atau publik. akses yang melanggar hukum adalah tindakan virtual yang memiliki dampak yang jelas, meskipun buktinya bersifat elektronik. Oleh karena itu, pelaku yang secara jelas mendedikasikan subjek hukum juga harus dikualifikasikan sebagai individu yang melakukan tindakan demonstrasi. Pemanfaatan regulasi *cybercrime* dalam mengkoordinir warga melalui regulasi pidana pada dasarnya merupakan bagian dari strategi dalam mencapai tujuan tertentu. Ini dipisahkan dari strategi perbaikan umum itu sendiri dan dilakukan untuk memastikan bahwa setiap pendekatan yang diambil dalam konteks hukum pidana selalu terkait dan tidak dapat dipisahkan dari tujuan kemajuan masyarakat itu sendiri; hal ini merupakan sarana untuk menciptakan rasa aman bagi warga. Undang-undang ini pada dasarnya harus dapat mengakomodasi kecepatan kemajuan dalam informasi dan inovasi web. Dalam perspektif mekanis, regulasi hukum harus mampu menanggapi dengan cepat kemajuan dalam pergantian peristiwa yang inovatif, daripada hanya mencoba untuk mengatasi kesalahan yang terjadi saat ini dengan menggunakan peraturan yang sudah ada. Sementara itu, meskipun negara ini belum sepenuhnya mampu mengatasi bencana yang sangat besar, masih sedikit tindakan yang diambil oleh para pembuat kebijakan di Indonesia untuk mengatasi masalah ini.

Pasal 30 ayat (1) dan (3) UUITE mengatur bahwa akses tanpa izin terhadap komputer atau sistem elektronik milik orang lain dengan cara melanggar sistem pengamanan merupakan tindakan yang dilarang. Sementara itu, Pasal 32 ayat (1) UUITE menjelaskan bahwa setiap tindakan yang mengubah, menambah,

mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, atau menyembunyikan informasi elektronik atau dokumen elektronik milik orang lain atau publik tanpa hak atau melawan hukum juga dilarang. maraknya kasus tersebut juga dapat dilihat dari sederet penyebab situs pemerintah yang memang rentan diretas oleh hacker, termasuk aplikasi generik yang rentan, tak memiliki perimeter keamanan yang memadai, hingga aplikasi tak dilakukan update.[9] Insiden web defacement yang paling umum terjadi pada sektor akademik, diikuti oleh situs swasta, pemerintah daerah, dan pemerintah pusat. Penyebab utamanya adalah kerentanan pada aplikasi generik, seperti framework aplikasi yang digunakan. Kurangnya perimeter keamanan dan visibilitas memadai juga berkontribusi pada rentannya situs pemerintahan terhadap peretasan. Selain itu, kurangnya pembaruan aplikasi secara berkala dan penyelesaian kasus pembobolan secara tuntas menyebabkan situs tetap rentan. Terdapat kemungkinan peretas telah menanam backdoor untuk tetap memiliki akses ke server. Oleh karena itu, penting bagi pemangku kepentingan untuk memperkuat keamanan, melakukan pengujian keamanan secara berkala, menanggapi insiden dengan cermat, menonaktifkan sistem yang tidak digunakan, dan memperbarui keamanan secara berkala.

a. Analisis Illegal Akses Berdasarkan pada putusan Nomor 41/ Pid.Sus / 2020/PN Mar.

Seperti kasus yang terjadi yaitu kasus Illegal Akses pada putusan Nomor 41/Pid.Sus/2020/PN Mar. Dalam analisis kasus yang kompleks ini, Terdakwa melakukan serangkaian tindakan yang melanggar hukum terkait akses dan manipulasi terhadap website e-dikbang Polri. Terdakwa, dengan sengaja dan tanpa izin, mengakses website tersebut dan merubah tampilannya secara drastis, menggantinya dengan pesan "*HACKED* BY DEDEN RAMADHANI GOBEL (UP) KASUS NOVEL BASWEDAN HANYA PENGALIHAN ISU DARI KASUS

[9] Badan Siber dan Sandi Negara (BSSN), dilansir dari https: //www. Cnn indonesia. com/ t eknologi /20211122123922-185-724359 /bssn –ungkap -sebab-situs- pemerintah -rentan- diretas/amp

MEGA KORUPSI JIWASRAYA, KETAHUAN BOONGYA gr333tz hacker newbie community". Proses ini dilakukan dengan cara masuk ke website, memasukkan nomor NRP Polri secara acak, dan mengunggah file 404 php yang kemudian diganti namanya serta membuat file indeks baru dengan pesan pribadi. Meskipun awalnya Terdakwa bermaksud untuk memberitahu admin tentang celah keamanan, namun tindakan ini tetap merupakan pelanggaran hukum yang serius.

Penting untuk dicatat bahwa Terdakwa menggunakan perangkat teknologi yang cukup lengkap tapi terbilang normal, termasuk laptop merek Lenovo dengan hardisk internal dan eksternal berkapasitas besar. Akses internet yang digunakan terdakwa adalah akses internet tidak sah, dimana Terdakwa menggunakan akses internet milik Abdulrahman Sapo yang disediakan secara gratis dan tanpa izin. Analisa log file menunjukkan penggunaan Windows 10 dalam proses manipulasi ini. Isi yang diunggah ke dalam website termasuk Php shell Alfa Php dengan domain bastardlabs.info milik Terdakwa.

Meskipun tampilan *website* akhirnya dikembalikan ke kondisi semula, tindakan tersebut tetap merupakan pelanggaran karena dilakukan tanpa izin dan atas kemauan sendiri. Selain *website* e-dikbang Polri, Terdakwa juga melakukan tindakan serupa pada *website* Pemerintah Gorontalo, dimana Terdakwa menemukan celah keamanan dan memberitahukan kepada admin. Meskipun tidak ada data yang diubah atau dihapus oleh Terdakwa, tindakan tersebut tetap dianggap sebagai pelanggaran hukum yang melanggar prinsip keamanan informasi dan memiliki konsekuensi hukum yang serius sesuai dengan peraturan yang berlaku.

Penegakan hukum terhadap kasus ini diatur dalam Pasal 48 ayat (1) UU ITE, (1) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (1) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp2.000.000.000,00 (dua miliar rupiah). Hal ini menunjukkan seriusnya negara dalam menangani pelanggaran terkait keamanan dan integritas data elektronik, serta memberikan sinyal kuat bahwa tindakan

semacam itu tidak akan ditoleransi.

Dimana kami menganalisis berdasarkan Undang-undang Nomor 1 Tahun 2023 tentang Kitab Undang-undang Hukum Pidana (KUHP Nasional) sebagai komparasi dinyatakan di Pasal 332 ayat (1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/ atau sistem elektronik milik Orang lain dengan cara apa pun, dipidana dengan pidana penjara paling lama 6 (enam) tahun atau pidana denda paling banyak kategori V yaitu Rp500.000.000,00 (lima ratus juta rupiah), denda kategori V berdasarkan pasal 79 ayat (1) huruf e. Sehingga Dalam perbandingannya antara Undang-Undang Nomor 11 Tahun 2008 Informasi dan Transaksi Elektronik terakhir dirubah dengan Undang-undang Nomor 1 Tahun 2024 (UU ITE) serta Kitab Undang-Undang Hukum Pidana (KUHP), dapat diamati bahwa terdapat perbedaan terkait Ruang Lingkup nya, yaitu:

1. Pertama, UU ITE: Menetapkan berbagai tindak pidana terkait dengan penggunaan akses ilegal ke perangkat dan sistem elektronik, seperti akses ilegal, perusakan, manipulasi data, dan lain-lain, sedangkan kedua, KUHP Nasional: Memuat pasal-pasal yang mengatur tentang penggunaan akses ilegal dan sistem elektronik, namun juga mencakup tindak pidana lain yang tidak terkait dengan teknologi informasi.
2. Kedua delik dalam UU ITE dan KUHP Nasional juga menetapkan sanksi yang serupa, yakni pidana penjara dan denda. Namun, perbedaan signifikan muncul dalam skala sanksinya. UU ITE menegaskan hukuman yang lebih berat dengan ancaman penjara hingga maksimal 8 tahun serta denda yang dapat mencapai 2 miliar rupiah. Di sisi lain, KUHP menetapkan pidana penjara maksimal 6 tahun dan denda maksimal 500 juta rupiah. Dengan demikian, perbandingan ini menyoroti perbedaan substansial dalam tingkat keparahan sanksi yang diterapkan oleh kedua undang-undang tersebut. Diputuskan dalam sidang permusyawaratan Majelis Hakim Pengadilan Negeri Marisa, pada hari Kamis, tanggal 30 Juli 2020, terdakwa Ramdan Yantu bin Maskur Yantu dinyatakan secara sah

dan meyakinkan bersalah atas tindak pidana yang dilakukan, yaitu mengubah informasi elektronik milik orang lain secara sengaja dan melawan hukum. Sebagai akibatnya, terdakwa dijatuhi pidana penjara selama 1 (satu) tahun dan denda sebesar Rp50.000.000,00 (lima puluh juta rupiah). Jika denda tersebut tidak dibayar, akan diganti dengan pidana kurungan selama 1 (satu) bulan.

Upaya Represif adalah suatu upaya dalam penanggulangan tindak kejahatan secara konsepsional yang ditempuh setelah terjadinya suatu tindak kejahatan[10]. Penanggulangan dengan upaya represif dimaksudkan untuk menindak para pelaku kejahatan sesuai dengan perbuatannya. Selain upaya represif juga bertujuan untuk memperbaiki kembali agar pelaku sadar bahwa perbuatan yang dilakukannya merupakan perbuatan yang melanggar hukum dan merugikan masyarakat.[11] Hukum pidana bertujuan untuk memulihkan kembali keadaan korban, keadaan lingkungan sosial sehingga hukum pidana bukanlah ajang untuk membalas dendam[12].

Kejahatan peretasan selain merugikan perorangan melainkan juga merugikan hak privasi, hak dasar seseorang. Peretasan mengincar data pribadi seseorang untuk disalahgunakan.[13] Penyalahgunaan hak orang lain adalah perbuatan melawan hukum, dan penyalahgunan wajib mempertanggungjawabkan perbuatannya kepada korban[14]. KUHP Nasional memberikan perlindungan bagi korban untuk memulihkan keadaan korban pasca traumatik terhadap perbuatan pidana[15]

---

[10] Hariyanto, Bayu Puji. 2018. *Pencegahan Peredaran Narkoba di Indonesia.* Jurnal Daulat Hukum, 1(1). Hlm. 209

[11] Wiyadnyana, I Ketut Pande. dan Sukardi, Ni Made Rai. (2023*) Patroli Cyber Guna Pencegahan Judi Online. Jurnal Aktual Justice Vol. 8, No. 2. Hlm. 154-167*

[12] Prasetyo, Teguh. Ginting, Yuni Priskila. Karo, Rizky Karo. (2023). *Hukum Pidana*. Depok: RajaGrafindo.

[13] Rizky PP Karo Karo, dan Teguh Prasetyo. *Pengaturan Perlindungan Data Pribadi di Indonesia: Perspektif Teori Keadilan Bermartabat*. Jakarta: Nusa Media

[14] Soelistyo, Henry. *Bad Faith Dalam Hukum Merek.* Yogyakarta: Maharsa Artha Mulia

[15] Sinaga, Dahlan. Prasetyo, Teguh. Kameo, Jeferson. *Keadilan Restoratif sebagai Kaidah Hukum: Menurut Teori Keadilan Bermartabat dan Mempertimbangkan UU No. 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana*. Depok: RajaGrafindo.

4. Kesimpulan

Dalam klasifikasi *cybercrime*, akses ilegal terhadap komputer atau sistem elektronik milik orang lain serta manipulasi terhadap informasi elektronik atau dokumen elektronik merupakan tindakan melanggar hukum yang sangat disoroti. Tindakan semacam itu memiliki dampak yang jelas, meskipun buktinya bersifat elektronik, sehingga pelaku yang secara jelas mendedikasikan subjek hukum juga harus dikualifikasikan sebagai individu yang melakukan tindakan demonstrasi. Pemanfaatan regulasi cybercrime dalam mengkoordinir warga melalui regulasi pidana pada dasarnya merupakan bagian dari strategi dalam mencapai tujuan tertentu, seperti menciptakan rasa aman bagi masyarakat. Undang-undang cybercrime harus mampu mengakomodasi kecepatan kemajuan dalam informasi dan inovasi web, serta mampu menanggapi dengan cepat kemajuan dalam pergantian peristiwa yang inovatif, daripada hanya mencoba untuk mengatasi kesalahan yang terjadi saat ini dengan menggunakan peraturan yang sudah ada. Maraknya kasus akses ilegal dan manipulasi informasi elektronik dapat dilihat dari sederet penyebab situs pemerintah yang rentan diretas oleh *hacker*, seperti aplikasi generik yang rentan dan kurangnya pembaruan aplikasi secara berkala. Situs-situs pemerintah rentan terhadap serangan *web defacement* karena kurangnya perimeter keamanan, visibilitas yang memadai, dan pembaruan aplikasi yang tidak teratur. Untuk memperkuat keamanan, diperlukan tindakan seperti melakukan pengujian keamanan secara berkala, menanggapi insiden dengan cermat, menonaktifkan sistem yang tidak digunakan, dan memperbarui keamanan secara berkala.

Pada kasus Illegal Akses pada putusan Nomor 41/Pid.Sus/2020/PN Mar melibatkan Terdakwa yang melakukan manipulasi terhadap *website* e-dikbang Polri dan *website* Pemerintah Gorontalo tanpa izin, dengan ancaman hukuman maksimal 8 tahun penjara dan denda Rp2 miliar menurut UU ITE. Terdakwa, Ramdan Yantu bin Maskur Yantu, dijatuhi hukuman penjara selama 1 tahun dan denda Rp50 juta oleh Pengadilan Negeri Marisa. Kasus ini menegaskan seriusnya penegakan hukum terhadap pelanggaran keamanan data elektronik.

Daftar Pustaka

BUKU

Karo, R. P. K., & Prasetyo, T. (2020). *Pengaturan perlindungan data pribadi di Indonesia: perspektif teori keadilan bermartabat*. Nusa Media.

Mulyana, Dedy. (2008). *Metodologi Penelitian Kualitatif.* Bandung: PT Remaja Rosdakarya

Prasetyo, T. Ginting, Y.P, & Karo, R.K. (2023). *Hukum Pidana.* Depok: RajaGrafindo.

Sinaga, Dahlan. Prasetyo, T,. Kameo, J. (2023). *Keadilan Restoratif sebagai Kaidah Hukum: Menurut Teori Keadilan Bermartabat dan Mempertimbangkan UU No. 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana.* Depok: RajaGrafindo.

Soelistyo, Henry. (2017). *Bad Faith Dalam Hukum Merek.* Yogyakarta: Maharsa Artha Mulia

Sugiyono. (2007). *Metode Penelitian Kuanitatif, Kualitatif, dan R&D*. Bandung: Alfabeta.

JURNAL

Bambang. H (2013). HACKER DALAM PERSPEKTIF HUKUM INDONESIA DI DUNIA MAYA. *Jurnal Sistem Informasi Universitas Suryadarma.*

Febriliani, C. Ismunarno, Diana. L, Kajian Etiologi Kriminal Tindak Pidana Cracking Sistem Operasi Windows Di Provinsi Daerah Istimewa Yogyakarta, Recidive Volume 8 No. 3, Sept. - Des. 2019, pp.219-226 ISSN: 24

Abidin, D, Z. Kejahatan Dalam Teknologi Informasi Dan Komunikasi, Jurnal Ilmiah Media Processor Vol.10 No.2 Oktober 2015 ISSN 1907-6738.

Gaven, G. Tumbol, A. Febriawan, D. (2023). Penegakan Hukum Kejahatan Siber Terhadap Akses Ilegal Terhadap Perbankan Online di Indonesia. Jurnal Kajian Hukum dan Pendidikan Kewarganegaraan. https://media.neliti.com/media/publications/4639-ID-hacker-dalam-perspektif-hukum-indonesia.pdf

Hamsa, I. Tesis, 2013, "Tinjauan Yuridis Persetujuan Tindakan Kedokteran Di Rumah Sakit Umum Daerah Salewangang Maros", Program Pasca Sarjana Universitas Hasanuddin, Makassar.

Hariyanto, B. P. 2018. *Pencegahan Peredaran Narkoba di Indonesia.* Jurnal Daulat Hukum, 1(1).

Sari, I. (2023). MENGENAL HACKING SEBAGAI SALAH SATU KEJAHATAN

Nugroho, I. Y. "Sanksi Hukum Kejahatan Peretasan Website Presiden Republik Indonesia", Al-Daulah: Jurnal Hukum Dan Perundangan Islam, Vol. 5,

No. 1, April 2015; ISSN 2089-0109, pp.171-203

Silic, M. Lowry, P. B. Breaking Bad in Cyberspace: Understanding why and how Black Hat Hackers Manage their Nerves to Commit their

Panjaitan, Ananda Chrisna D.. (2023). Penegakan Hukum Pidana Internasional di Yaman. *Jurnal Aktual Jusice Vol. 8, No. 2* Virtual Crimes, Published online: 4 September 2019, Springer.

Wiyadnyana, I Ketut Pande, dan Ni Made Rai Sukardi. (2023) Patroli Cyber Guna Pencegahan Judi Online. *Jurnal Aktual Justice Vol. 8, No. 2*. Hlm. 154-167

Online/*World Wide Web:*

CNN INDONESIA. (2021). *BSSN Ungkap Sebab Situs Pemerintah Rentan Diretas*. https://www.cnnindonesia.com/teknologi/ 20211122123922-185-724359/ bssn –ungkap –sebab –situs– pemerintah –rentan-diretas/ amp

Undang-undang/Peraturan

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) UU No. 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana.