Sibatik Journal
Jurnal Ilmiah Bidang Sosial, Ekonomi, Budaya, Teknologi, dan Pendidikan
E-ISSN: 2809-8544

PERTANGGUNGJAWABAN PIDANA TERHADAP TINDAK PIDANA MENJEBOL SISTEM PENGAMANAN DATA PRIBADI: STUDI PUTUSAN PENGADILAN NOMOR 809/PID.SUS/2023/PN.MDN

CRIMINAL LIABILITY FOR THE OFFENSE OF BREACHING PERSONAL DATA SECURITY SYSTEMS: A STUDY OF COURT DECISION NUMBER 809/PID.SUS/2023/PN.MDN

Hendrik Rahmat Syah Putra Sarumaha[1]*, Edi Yunara[2], Joiverdia Arifiyanto[3]
Universitas Sumatera Utara, Indonesia
***Email Correspondence:** Innosensiahulu24@gmail.com

Abstract

"Digital crime" (or "cybercrime") has become one of the most frequently used terms in society today. The prefix "cyber-" is attached to various terms to describe new societal forms or crime types based on cyberspace—such as cyber society, cyberspace, cyberattacks, cybercrime, and cyber-terrorism. The evolution of information technology and the internet has created the realm of cyberspace; this computer-based communication world offers a new reality known as virtual reality. This environment has given rise to the specific term "cybercrime." Some experts argue that computer crime, cybercrime, and telematics crime are essentially the same, differing only in nomenclature. The underlying argument is that while computers were initially used merely for data collection and storage—facilitating conventional crimes—subsequent developments saw crimes committed via the internet, such as Trojan horse attacks and data leakage. This terminological controversy has not sparked significant debate regarding usage; for the sake of consistency, the author employs the term "cybercrime." Advances in information technology—particularly in computing and the internet—have undeniably benefited human life. However, alongside the advantages and conveniences they offer, these technologies possess a dark side capable of destroying human life and culture. Information technology has become a "double-edged sword": while it contributes to human welfare, progress, and civilization, it also serves as an effective vehicle for unlawful acts. Data theft is one such act that can be easily and effectively perpetrated by exploiting technological advancements, particularly in the sectors of data management and the handling of Personal Data—an area requiring robust protection. Advances in information and communication technology have blurred the boundaries of privacy, making it increasingly easy for Personal Data to be disseminated. Information technology can thus be utilized to commit unlawful acts, such as the theft of users' Personal Data.

Keywords: Digital Crime, Personal Data, Security.

Abstrak

Kejahatan digital *(cyber)* menjadi istilah yang paling sering digunakan seluruh masyarakat saat ini. Kata *cyber* ditambahkan pada berbagai istilah untuk mengambarkan bentuk masyarakat atau jenis kejahatan baru berbasis siber, contohnya *cyber society*, *cyber space*, *cyber attacks*, *cyber crime*, *cyber terrorism*, dan lain-lain. Perkembangan teknologi informasi atau internet telah menciptakan dunia yang baru mengenai *cyber space*, dunia komunikasi yang berbasis komputer menawarkan realitas yang baru yaitu realitas virtual. Ini juga disebut dengan istilah yang menghasilkan bentuk lingkungan *cyber space* yang melahirkan istilah baru yaitu *cyber crime*.Beberapa pakar berbendapat baik kejahatan komputer (*computer crime*), kejahatan siber (*cyber crime*), dan kejahatan telematika merupakan kejahatan yang sama hanya saja penamaannya saja yang berbeda. Argumentasi yang melatarbelakangi bahwa pada awalnya komputer hanya sebagai pengumpulan dan penyimpanan data yang dapat digunakan untuk melakukan kejahatan konvensional, tetapi dalam perkembangan selanjutnya kejahatan komputer juga dilakukan melalui basis internet seperti *trojan horse hacking,* dan *data leakage.* Kontroversi pengistilahan, tidaklah menciptakan perdebatan mengenai penggunaan istilah yang digunakan. Karena itu, dengan alasan konsistensi penulis maka istilah yang

DOI: https://doi.org/10.47353/sibatik.v5i6.4874

sering digunakan adalah kejahatan siber (*cyber crime*).Kemajuan teknologi informasi terutama pada bidang komputer dan internet terbukti telah memberikan dampak positif bagi kemajuan kehidupan manusia. Namun, dibalik kelebihan dan kemudahan yang ditawarkan oleh komputer dan internet, ternyata memiliki sisi gelap yang dapat menghancurkan kehidupan dan budaya manusia itu sendiri. Teknologi informasi saat ini menjadi "pedang bermata dua" karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan, dan peradaban manusia sekaligus menjadi sarana efektif perbuatan melawan hukum. Pencurian data merupakan salah satu tindakan yang berpotensi dilakukan dengan mudah dan efektif dengan memanfaatkan perkembangan teknologi dan informasi juga pada sektor pengelolaan data dan informasi khususnya pada pengelolaan Data Pribadi yang membutuhkan pelindungan data. Sebab dengan kemajuan teknologi informasi dan komunikasi tersebut membuat batas privasi makin tipis sehingga berbagai Data-data Pribadi semakin mudah untuk tersebar. Teknologi informasi dapat digunakan untuk melakukan perbuatan melawan hukum seperti pencurian Data Pribadi pengguna.

Kata kunci: *Kejahatan Digital, Data Pribadi, Keamanan.*

PENDAHULUAN

Kejahatan digital *(cyber)* menjadi istilah yang paling sering digunakan seluruh masyarakat saat ini. Kata *cyber* ditambahkan pada berbagai istilah untuk mengambarkan bentuk masyarakat atau jenis kejahatan baru berbasis siber, contohnya *cyber society*, *cyber space*, *cyber attacks*, *cyber crime*, *cyber terrorism*, dan lain-lain. Perkembangan teknologi informasi atau internet telah menciptakan dunia yang baru mengenai *cyber space*, dunia komunikasi yang berbasis komputer menawarkan realitas yang baru yaitu realitas virtual. Ini juga disebut dengan istilah yang menghasilkan bentuk lingkungan *cyber space* yang melahirkan istilah baru yaitu *cyber crime*.

Beberapa pakar berbendapat baik kejahatan komputer (*computer crime*), kejahatan siber (*cyber crime*), dan kejahatan telematika merupakan kejahatan yang sama hanya saja penamaannya saja yang berbeda. Argumentasi yang melatarbelakangi bahwa pada awalnya komputer hanya sebagai pengumpulan dan penyimpanan data yang dapat digunakan untuk melakukan kejahatan konvensional, tetapi dalam perkembangan selanjutnya kejahatan komputer juga dilakukan melalui basis internet seperti *trojan horse hacking,* dan *data leakage.* Kontroversi pengistilahan, tidaklah menciptakan perdebatan mengenai penggunaan istilah yang digunakan. Karena itu, dengan alasan konsistensi penulis maka istilah yang sering digunakan adalah kejahatan siber (*cyber crime*).

Kemajuan teknologi informasi terutama pada bidang komputer dan internet terbukti telah memberikan dampak positif bagi kemajuan kehidupan manusia. Namun, dibalik kelebihan dan kemudahan yang ditawarkan oleh komputer dan internet, ternyata memiliki sisi gelap yang dapat menghancurkan kehidupan dan budaya manusia itu sendiri. Teknologi informasi saat ini menjadi "pedang bermata dua" karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan, dan peradaban manusia sekaligus menjadi sarana efektif perbuatan melawan hukum.

Pencurian data merupakan salah satu tindakan yang berpotensi dilakukan dengan mudah dan efektif dengan memanfaatkan perkembangan teknologi dan informasi juga pada sektor pengelolaan data dan informasi khususnya pada pengelolaan Data Pribadi yang membutuhkan pelindungan data. Sebab dengan kemajuan teknologi informasi dan

DOI: https://doi.org/10.47353/sibatik.v5i6.4874

komunikasi tersebut membuat batas privasi makin tipis sehingga berbagai Data-data Pribadi semakin mudah untuk tersebar.Teknologi informasi dapat digunakan untuk melakukan perbuatan melawan hukum seperti pencurian Data Pribadi pengguna.

Konsep tentang Pelindungan Data Pribadi pada awalnya bermula dari konsep hak atas privasi. Konsep hak atas privasi pertama kali dikembangkan oleh Warren dan Brandheis di dalam jurnal Harvard Law Review. Warren dan Brandheis menyatakan bahwa dengan adanya perkembangan dan kemajuan teknologi maka timbul suatu kesadaran masyarakat bahwa telah lahir suatu kesadaran bahwa ada hak seseorang untuk menikmati hidup. Hak untuk menikmati hidup tersebut diartikan sebagai hak seseorang untuk tidak diganggu kehidupan pribadinya baik oleh orang lain, atau oleh negara (*rights to be alone*).

Hak Pelindungan Data Pribadi berkembang dari hak untuk menghormati kehidupan pribadi atau disebut *the right to private life.* Konsep kehidupan pribadi tersebut berhubungan dengan manusia sebagai makhluk hidup. Dengan demikian orang perorangan adalah pemilik utama dari hak Pelindungan Data Pribadi.

Dalam putusan pengadilan No. 809/Pid.Sus/2023/PN.Mdn, misalnya, terdakwa, Lutfhi Bagas Kara, menyatakan bahwa setelah menggunakan ponsel Vivo 1910 berwarna hitam, ia menemukan bahwa ponsel tersebut milik korban, HANNA SELLY. Pada tanggal 11 Februari 2023, terdakwa mengubah nomor telepon menjadi 0813 2785 0192 dengan masuk ke Pengaturan Email dan memilih menu Ubah Nomor Telepon karena ia masih memiliki email di telepon tersebut. Terdakwa mengubah kata sandi untuk email hannaselly84@gmail.com menjadi engkos1510 setelah memilih menu Ubah Kata Sandi dan menerima kode verifikasi dari Google setelah nomor telepon yang tercantum dalam email diubah menjadi 0813 2785 0192.

Setelah terdakwa memperoleh akun Gojek milik saksi HANNA SELLY ELISABETH SILITONGA, SE, pada tanggal 11 Februari 2023 nomor telepon di akun Gojek tersebut dirubah oleh terdakwa menjadi nomor telepon 081327850192 lalu terdakwa belanja makanan sebesar 500 ribu dengan menggunakan Gopay PayLater yang terdapat di akun Gojek tersebut.

Bahwa pada tanggal 13 Februari 2023 nomor telepon di akun Gojek tersebut dirubah kembali oleh terdakwa dengan menggunakan nomor dari kartu Perdana TRI yang baru dibeli oleh terdakwa namun terdakwa lupa nomor nya dan yang di ingat hanya 3 angka terakhir yaitu 653.

Bahwa Akun Gojek, Indodax dan Facebook milik saksi HANNA SELLY ELISABETH SILITONGA, SE yang tertaut dengan email hannaselly84@gmail.com yang berhasil terdakwa ambil alih hanya Gojek sedangkan untuk akun Indodax dan Facebook tidak berhasil terdakwa ambil alih karena system keamanan 2 langkah di akun Indodax dan Facebook tersebut yang menggunakan email dan nomor Hand Phone milik saksi HANNA SELLY untuk verifikasi nya.

Adapun tuntutan jaksa terhadap terdakwan Lutfhi Bagas Kara terbukti secara sah dan meyakinkan bersalah melakukan Tindak Pidana “Dengan Sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa

DOI: https://doi.org/10.47353/sibatik.v5i6.4874

pundengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan", sebagaimana yang didakwakan yaitu melanggar Pasal 30 ayat (3) jo Pasal 46 ayat (3) UURI No. 19 Tahun 2016 tentang Perubahan atas UU RI No. 11 Tahun 2008 tentang ITEdalam Dakwaan Kesatu.

Amar putusan hakim adalah sebagai Terdakwa Luthfi Bagas Kara telah terbukti secara sah dan meyakinkan bersalah melakukan tindak pidana "Yang melakukan, yang menyuruh melakukan, dan yang turut serta melakukan perbuatan dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apapun dengan melanggar, menerobos, melampaui atau menjebol system pengamanan", sebagaimana dalam dakwaan kesatu; Menjatuhkan pidana terhadap Terdakwa oleh karena itu dengan pidana penjara selama 1 (satu) tahun dan 3 (tiga) bulan; Menetapkan masa penangkapan dan penahanan yang telah dijalani oleh Terdakwa, dikurangkan seluruhnya dari pidana yang dijatuhkan. Adapun rumusan masalah dalam penelitian ini sebagai berikut: Bagaimana Pengaturan Hukum Tentang Kejahatan Siber Khususnya Pembobolan Data?, Bagaimana Pertanggungjawaban Pidana Terhadap Tindak Pidana Menjebol Sistem Keamanan?, Bagaimana Pertimbangan Hukum Hakim Terhadap Putusan Pengdilan Nomor 809/ Pid.Sus/2023/PN.Mdn, Tentang Tindak Pidana Melanggar, Menjebol Sistem Keamanan?

METODE

Metode penelitian yang digunakan dalarn penelitian ini adalah jenis penelitian hukum normatif. Penelitian hukum normatif adalah penelitian yang dilakukan dengan cara meneliti bahan pustaka (data sekunder) atau penelitian hukum perpustakaan. Penelitian hukum normatif juga disebut sebagai penelitian perpustakaan atau studi dokumen, karena lebih banyak dilakukan terhadap data yang bersifat sekunder yang ada di perpustakaan. Pada Penelitian normatif data sekunder sebagai sumber/ bahan informasi dapat berupa bahan hukum primer, bahan hukum sekunder dan bahan hukum tersier.

HASIL DAN PEMBAHASAN

Pengaturan Hukum Tentang Kejahatan Siber Pembobolan Data

1. Dalam Kitab Undang-Undang Hukum Pidana (KUHP)

Pasal 332 Undang-Undang Nomor 1 Tahun 2023 Tentang Kitab Undang-Undang Hukum Pidana, yang menyatakan bahwa:

1) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apapun, dipidana dengan pidana penjara paling lama enam tahun atau pidana denda paling banyak kategori V.
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, dipidana dengan pidana penjara paling lama tujuh tahun atau pidana denda paling banyak kategori V.

DOI: https://doi.org/10.47353/sibatik.v5i6.4874

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, dipidana dengan pidana penjara paling lama delapan tahun atau pidana denda paling banyak kategori VI.

Pada pasal 332 KUHP baru yang mengatur mengenai tindak pidana *cyber crime* yang menggunakan sistem komputer sebagai alat kejahatan, tetapi dalam pasal ini unsur-unsur dari tindak pidana ransomware yang melakukan pemerasan belum terpenuhi dengan pasal ini. Maka pasal ini kurang relevan jika dikaitkan dengan tindak pidana ransomware. Oleh karena itu, dalam KUHP baru belum juga mengatur secara spesifik terkait dengan pertanggungjawaban pidana terhadap pelaku tindak pidana ransomware.

Berdasarkan seluruh aturan dalam UU ITE, KUHP lama maupun dalam UU Perlindungan Data Pribadi dan Undang-Undang Nomor 1 Tahun 2023 Tentang Kitab Undang-Undang Hukum Pidana, maka penulis berpendapat bahwa pengaturan terkait dengan tindak pidana ransomware masih mengalami kekaburan, yang dimana belum ada pasal yang menjelaskan secara spesifik terkait dengan tindak pidana jenis baru ini. Hal ini dikarenakan dalam UU ITE tidak memberikan batasan secara khusus yang mengatur mengenai "serangan ransomware", melainkan tindak pidana ransomware masih dikategorikan sebagai bentuk tindak pidana yang lain, seperti tindak pidana peretasan. Maka, menyebabkan tindak pidana ransomware sampai saat ini marak terjadi, bahkan modus operandinya terus berkembang dengan memanfaatkan teknologi, terutama melalui sistem komputer. Sehingga serangan ransomware ini semakin canggih dan kasusnya pun sulit untuk diungkap, bahkan sampai saat ini belum ada putusan pengadilan yang mengadili kasus tersebut.

Isitilah yang digunakan tindak pidana kejahatan komputer dalam Bahasa inggrispun sangat bermacam-macam. Banyak istilah yang digunakan seperti "computer misuse", "*computer abuse*", "*computer crime*", "computer fraud", "*computer-related crime*", dan "*computer-assisted crime*". Namum pada umumnya lebih banyak diterima dengan memakai istilah "computer crime", karena dianggap lebih luas dan telah lazim digunakan dalam hubungan internasional. Di negara Amerika contohnya menggunakan"*computer-related crime*" oleh The U.S Computer Crime. Sebaliknya penggunaan istilah '*computer misuse'* lebih tepat dari pada 'computer crime'karena sifatnya lebih membatasi pada perbuatan yang dilarang oleh undang- undang hukum pidana oleh Komisi Franken, meskipun perbuatan penyalahgunaan komputer juga dapat dilarang oleh undang-undang lainnya. Melihat istilah yang digunakan di Belanda dengan menyebut '*computer misbruik'* disamping '*computer criminaliteit'*. Di Indonesia sendiri istilah yang digunakan ialah penyalahgunaan komputer atau kejahatan komputer. Tapi istilah yang tampaknya lebih cocok ialah kejahatan komputer, karena penyalahgunaan komputer memiliki pengertian bahwa komputer merupakan alat untuk melakukan tindak pidana, padahal dalam kenyataannya komputer dan data komputer yang menjadi objek dari tindak pidana. Meski begitu kejahatan komputer memiliki pengertian yang lebih luas yaitu tindak pidana dimana komputer selain sebagai sarana untuk melakukan suatu tindak pidana, juga sebagai objek dari tindak pidana itu sendiri.

DOI: https://doi.org/10.47353/sibatik.v5i6.4874

2. Undang- Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 Tentang ITE

Permasalahan cybercrime di Indonesia telah diatur dalam UU ITE sehingga bersifat khusus atau lex specialit. Kebijaikan hukum terkait dengan masalah kriminalisasi dalam UU ITE tertuang dalam Bab XI tentang Ketentuan Pidana Pasal 45 sampai dengan Pasal 52 juncto Pasal 27 sampai dengan Pasal 36.

Walaupun dengan adanya Pasal-Pasal diatas yang merupakan pilar utama dalam mengatur terkat aktifitas cybercrime di Indonesia, nyatanya masih terdapat beberapa permasalahan terkait beberapa Pasal tersebut yang menimbulkan kontradiktif dalam lingkungan masyarakat terutama bagi para pengiat teknologi.

Dalam UU ITE tersebut, pasal yang mengatur terkait peretasan atau hacking dapat kita jumpai pada Pasal 30 jo Pasal 46 UU ITE dan juga pada Pasal 34 jo Pasal 50 UU ITE yang mana seperti dipaparkan:

1. Pasal 30

(1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun.

(2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun 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 apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

2. Pasal 34

(1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum memproduksi, menjual, mengadakan untukdigunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki:

a. perangkat keras atau perangkat lunak Komputer yang dirancang atau secara khusus dikembangkan untuk memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33;

b. sandi lewat Komputer, Kode Akses, atau hal yang sejenis dengan itu yang ditujukan agar Sistem Elektronik menjadi dapat diakses dengan tujuan memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33.

(2)Tindakan sebagaimana dimaksud pada ayat (1) bukan tindak pidana jika ditujukan untuk melakukan kegiatan penelitian, pengujian Sistem Elektronik, untuk perlindungan Sistem Elektronik itu sendiri secara sah dan tidak melawan hukum.

Walaupun dua Pasal diatas terlihat seperti tidak memiliki masalah dalam aturan hukumnya, nyatanya dua Pasal tersebutlah yang memiliki beberapa kontradiktif yang bisa dibilang terlalu menekan para peretas atau hacker tanpa pandang bulu, entah itu hacker yang memiliki etikat baik maupun tidak, dan bukan cuman hacker saja tetapi masyarakat awam atau orang-orang yang bahkantidak paham tentang peretasan pun bisa ikut terjerat karena terlalu abstraknya dua pasal tersebut.

DOI: https://doi.org/10.47353/sibatik.v5i6.4874

Dengan melihat konteks pasal 30 mulai dari ayat (1), ayat (2), dan ayat (3) menurut Budi Suhariyanto dapat dikategorikan jenis hacking yang dilarang oleh undang-undang ITE diantaranya: Memasuki atau mengakses komputer dan/atau Sistem Elektronik milik orang lain. Jenis ini dijelaskan oleh pasal 30 ayat (1), Di mana teks Ayat tersebut memiliki hal yang bias, oleh karena itu perlu dijelaskan mengenai kebiasaannya tersebut. Di antaranya: Pertama, Dicantumkannya kata "tanpa hak" dengan "melawan hukum" secara bersama-sama, padahal sebagaimana dikemukakan oleh Budi Suhariyanto dalam bukunya yang berjudul "TINDAK PIDANA TEKNOLOGI INFORMASI (CYBERCRIME)" di bagian awal penjelasan dari pasal 27 ayat (1) Mengenai frase kata "tanpa Hak" adalah semakna dengan kata "melawan hukum". Jadi jika keduanya disandingkan, meskipun penggabungan kedua kata tersebut adalah persamaan (dengan simbol kata penghubung "atau"), Menurut Budi adalah sebuah tindakan kelebihan kata-kata yang dapat dikategorikan sebagai over criminalization.

Pertanggungjawaban Pidana Terhadap Tindak Pidana Menjebol Sistem Keamanan

Pertanggungjawaban pidana dalam bahasa asing disebut dengan teorekenbaardheid atau criminal responsibility yang mengarah pada pemidanaan terhadap pelaku dengan tujuan untuk menentukan apakah seorang terdakwa atau tersangka dapat dimintai pertanggungjawaban atas suatu tindak pidana yang telah dilakukannya.

Berbicara tentang pertanggungjawaban pidana artinya, berbicara tentang orang yang melakukan perbuatan pidana. Hukum pidana memisahkan antara ciri-ciri perbuatan yang dijadikan tindak pidana dan ciri-ciri orang yang melakukan. Goerge P. Fletcher menyatakan:

Van Hamel, memberi pengertian mengenai pertanggungjawaban sebagai:

"..keadaan normal psikis dan fisik yang membawa tiga macam kemampuan, antara lain: 1) mampu untuk dapat mengerti makna serta akibat sungguh – sungguh dari perbuatan – perbuatan itu sendiri; 2) mampu untuk menginsyafi bahwa perbuatan – perbuatan itu bertentangan dengan ketertiban masyarakat; 3) mampu untuk menentukan kehendak berbuat".

Simons memberikan defenisi pertanggungjawaban pidana sebagai suatu keadaan psikis, sehingga penerapan suatu ketentuan pidana dari pandangan umum dan pribadi dianggap tepat. Menurutnya inti dari pertanggungjawaban pidana dalam hukum pidana adalah: 1) keadaan psikis atau jiwa seseorang; dan 2) hubungan antara keadaan psikologis dengan perbuatan yang dilakukan.

Dalam hal melaksanakan penegakan hukum khususnya pada bidang kejahatan dunia maya, kejahatan tersebut mempunyai jarak yang amat luas tanpa mengetahui perbatasan wilayah suatu negara sebab kejahatan ini sifatnya"transnasional".Pembobolan mewujudkan suatu perbuatan maupun aktivitas menjebolkan sesuatu. Membobol yang artinya "menjebol, mengacaukan, mendobrak, dan mengacaukan dengan kekejaman, atau mendobrak dengan suatu paksaan. Pertanggungjawaban pidana yang dasarnya menyimpan artitimbal balik atas tindakan si pembuat pidana atas kejahatan yang dilakukan. Maka, tanggung jawab kejahatan isinya unsur objek dan unsur subjek.

DOI: https://doi.org/10.47353/sibatik.v5i6.4874

Maksudnya, menurut pembuat kejahatan sudah berbuat delik kejahatan kriminalitas dimana secara individu yang membuat kejahatan pantas disalahkan atas delik yang dilakukan itu maka bisa dihukum". Kejahatan atau perbuatan tersebut ialah sebagai bentuk sebagai "perilaku menyimpang yang selalu ada dan melekat pada tiap bentuk masyarakat. Perilaku menyimpang itu merupakan suatu ancaman yang nyata atau ancaman terhadap norma-norma sosial yang mendasari kehidupan atau keteraturan sosial, dapat menimbulkan ketegangan individual maupun ketegangan-ketegangan sosial, dan merupakan ancaman riil atau potensi bagi berlangsungnya keteraturan sosial". Cracking adalah aktivitas membobol sistem computer yang bertujuan "mengambil keuntungan dengan cara merusak dan menghancurkan dengan motivasi tertentu. Cracker ialah istilah perengkah yang diajukan oleh Richard Stallman untuk mengacu kepada peretas yang cenderung melakukan kegiatan Black Hat Hacker. Cracker merupakan seseorang yang masuk tanpa izin atau illegal ke dalam sebuah sistem computer . Istilah Cracker memiliki kecenderungan hacker pada penjelasan "white hat Hacker". Hacker mempunyai kesamaan dan ketidaksamaan. Sama-sama melaksanakan aktivitas Hacking, tetapi tidak sama dari hal motivasi dan tujuan Hackingnya. Cracker cenderung melaksanakan hacking yang merusak, selain itu Hacker sejatinya merupakan spirit Tingkat internasional untuk membantu menyelesaikan masalah pada sistem computer . Dalam UU ITE tindak pidana Cracking telah diatur dan dirumuskan dalam pasal-pasal yang dapat menjerat pelaku tindak pidana Cracking. Pada dasarnya tindak pidana Cracking diatur secara umum pada Pasal 30 UU ITE yang berbunyi sebagai berikut:

"Pertama, Setiap Orang dengan sengaja dan tanpa sengaja melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun. Kedua, Setiap Orang dengan sengaja dan tanpahak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik. Ketiga, Setiap Orang dengan sengaja dan tanpa sengaja melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan." Pasal 30 ayat (1) UU ITE "Setiap orang dengan sengaja dan tanpa sengaja melawan hukum mengakses sistem dan/atau Sistem Elektronikmilik orang lain dengan cara apapun." Pasal 30 Ayat (2) UU ITE "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apapun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik". Pasal 30 ayat (3) UU ITE: "Setiap orang dengan sengaja dan tanpa sengaja melawan hukum mengakses computer dan/atau sistem elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan. Sanksi pidana yang ada pada ketentuan pidana Pasal 46 ayat (1) UU ITE: Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (1) dipidana dengan pidana penjara paling lama enam tahun dan/atau denda paling banyak enam ratus juta rupiah.

Sanksi pidana Pasal 30 ayat (3) terdapat pada Pasal 46 ayat (3) UU ITE: hukuman pidana penjara paling lama delapan tahun dan/atau denda paling banyak delapan

DOI: https://doi.org/10.47353/sibatik.v5i6.4874

ratus juta rupiah. Yang dapat dijerat oleh ketentuan pasal 46 ayat (3) ialah pihak yang melakukan tindakan yang dilarang sebagaimana dimaksud pada pasal tersebut seperti menjebol sistem keamanan yang membatasi dengan berdasarkan kategorisasi atau klasifikasi pengguna beserta kewenangan yang ditentukan."

Pertimbangan Hukum Hakim Terhadap Putusan Pengadilan Nomor 809/ Pid.Sus/ 2023/Pn.Mdn Tentang Tindak Pidana Menjebol Keamanan

Terdakwa Luthfi Bagas Kara telah terbukti secara sah dan meyakinkan bersalah melakukan tindak pidana "Yang melakukan, yang menyuruh melakukan, dan yang turut serta melakukan perbuatan dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apapun dengan melanggar, menerobos, melampaui atau menjebol system pengamanan", sebagaimana dalam dakwaan kesatu;Menjatuhkan pidana terhadap Terdakwa oleh karena itu dengan pidana penjara selama 1 (satu) tahun dan 3 (tiga) bulan.

Keadaan yang memberatkan:

Perbuatan Terdakwa dapat meresahkan masyarakat dan saksi korban; Keadaan yang meringankan:

a. Terdakwa belum pernah dihukum;
b. Terdakwa bersikap sopan dipersidangan;
c. Terdakwa merasa bersalah dan menyesali perbuatannya.

Teori keadilan ini dijadikan sebagai pisau analisis untuk menjawab rumusan masalah yang ketiga, yang dimana pada putusan tersebut data pribadi dari korban dibobol oleh terdakwa sehingga korban dirugikan secara materil tentunya dan pada putusan tersebut hakim memberikan hukuman sesuai pada pasal dalam UU ITE yang dimana perbuatan tersebut adalah terdapat dalam UU tersebut. Seperti halnya sudah terdapat pengaturan hukum tentang tindak pidan aini yang dimana diarapkan dengan aturan ini dapat terpenuhi nya keadilan bagi seluruh masyarakat yang apabila melakukan tindak pidana sesuai dengan perbuatan nya akan dijatuhan sanksi sesuai dengan aturan hukum yang mengaturnya.

Keadilan merupakan suatu hal yang abstrak, sehingga akan sulit mewujudkan suatu keadilan jika tidak mengetahui apa arti keadilan. Keadilan memiliki banyak makna, dimensi, bahkan pendekatan. Tidak hanya di satu negara saja, namun secara universal keadilan bisa jadi merupakan konsep yang sama di satu sisi, namun bisa juga berbeda di sisi yang lain. Berbagai pandangan tentang konsep keadilan pun berbeda-beda, dipengaruhi oleh perkembangan masyarakat, budaya, sosial, atau bahkan ideologi suatu negara.

Tindak pidana cracking tidak terlepas dari pertanggungjawaban pelaku dan penerapan sanksinya terhadap pertanggungjawaban pidana tindak pidana carding menggunakan teori Moeljatno dimana kesalahan tersebut terdiri dari kesengajaan (dolus) dimana kesengajaan atau dolus ditentukan dalam 3 (tiga bentuk yaitu kesengajaan dengan maksud (dolus directus), kesengajaan dengan kepastian (opzet bijt zekerheids bewotzjin) dan kesengajaan dengan kemungkinan (dolus eventualis) sedangkan kealpaan (culpa), terdiri dari kealpaan dengan kesadaran (bewuste schuld) dan kealpaan tanpa kesadaran (onbewuste schuld),

DOI: https://doi.org/10.47353/sibatik.v5i6.4874

artinya sanksi terhadap pelanggaran norma pidana yang dilakukan lebih ringan pidananya, dikarenakan kealpaan atau culpa adalah perbuatan yang merupakan tindak pidana yang tidak ada dasar niat untuk melakukan kejahatan tetapi karena kecerobohan atau kurang hati-hatinya yang mengakibatkan terjadinya kejahatan.

Permasalahan hukum dalam kejahatan cracking yaitu ketika terkait dengan penyampaian informasi, pengaturan, komunikasi dan transaksi secara elektronik, khususnya dalam pembuktian hal yang terkait dengan perbuatan hukum yang dilaksanakan melalui sistem elektronik. Cracking sendiri merupakan bagian cybercrime dalam transaksi online yang menggunakan sarana internet sebagai basis transaksi khususnya sistem layanan onlineMenurut G. P. Hoefnagels, mengemukakan bahwa sanksi dalam hukum pidana adalah semua reaksi terhadap pelanggar hukum yang ditentukan oleh undang-undang dimulai dari penahanan tersangka dan penuntutan terdakwa sampai pada penjatuhan vonis oleh hakim. Penetapan sanksi dalam hukum pidana merupakan suatu rangkaian kebijakan dalam suatu sistem pemidanaan.

PENUTUP

Kesimpulan

1. Pengaturan hukum terhadap tindak pidana siber terkhusus tentang pembobalan sistem keamanan data pribadi ini terdapat dalam pasal 30 Undang-Undang Informasi dan transaksi elektronik, yaitu setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun. Aturan ini mengaturmengenai akses illegal yang terdapat adanya pembatasan terhadap akses dalam sistem elektronik, yang mana ciri dari pembatasan akan akses adanya suatu pengamanan baik dari kode akses atau *password* tertentu atau dengan menggunakan bahasa pemograman untuk masuk dengan membobol sistem kemananan, disamping itu untuk mengetahui bahwa data elektronik tersebut merupakan akses publik atau tidak dengan melihat adanya suatu sistem keamanan.
2. Pertanggungjawaban pidana terhadap tindak pidana menjebol sistem keamanan (*unauthorized access*) pada dasarnya diatur dalam ketentuan perundang-undangan yang berlaku, khususnya dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagaimana telah diubah dengan UU Nomor 19 Tahun 2016. Dalam hal ini, pelaku yang secara sengaja dan tanpa hak melakukan akses terhadap sistem elektronik milik orang lain dapat dipidana berdasarkan Pasal 30 UU ITE, dengan ancaman pidana penjara dan/atau denda. Pertanggungjawaban pidana berlaku apabila terpenuhi unsur-unsur subjektif dan objektif, yaitu adanya kesengajaan dari pelaku (*mens rea*) serta tindakan melawan hukum yang menimbulkan kerugian atau ancaman terhadap keamanan sistem elektronik (*actus reus*). Selain itu, pelaku juga dapat dikenai pidana tambahan jika tindakannya menyebabkan terganggunya layanan publik, pencurian data, atau kerugian materiil yang signifikan.
3. Pertimbangan hukum hakim pada putusan pengadilan Nomor 809/ Pid.Sus/ 2023/ PN.MDN, Hakim akan menilai apakah perbuatan terdakwa memenuhi unsur-unsur dalam

DOI: https://doi.org/10.47353/sibatik.v5i6.4874

pasal pidana yang didakwakan. Dalam konteks ini, pasal yang biasanya digunakan adalah:Di Indonesia (UU ITE):Pasal 30 UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), yang telah diubah dengan UU No. 19 Tahun 2016, yaitu terdakwa Luthfi Bagas Kara telah terbukti secara sah dan meyakinkan bersalah melakukan tindak pidana "Yang melakukan, yang menyuruh melakukan, dan yang turut serta melakukan perbuatan dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apapun dengan melanggar, menerobos, melampaui atau menjebol system pengamanan", sebagaimana dalam dakwaan kesatu;Menjatuhkan pidana terhadap Terdakwa oleh karena itu dengan pidana penjara selama 1 (satu) tahun dan 3 (tiga) bulan.

Saran

1. Kepada pemerintah, untuk melakukan Penguatan Regulasi dan Penegakan Hukum, Pemerintah perlu terus memperbarui dan menguatkan regulasi yang mengatur tindak pidana siber, khususnya yang berkaitan dengan pelanggaran sistem keamanan. Selain itu, penegakan hukum harus dilakukan secara tegas dan konsisten agar dapat memberikan efek jera kepada pelaku. Pengembangan Sistem Keamanan Siber Nasional Pemerintah perlu mengembangkan dan memperkuat infrastruktur keamanan siber nasional, termasuk menyediakan teknologi canggih dan sumber daya manusia yang handal untuk mencegah dan mendeteksi upaya pembobolan sistem keamanan.Edukasi dan Kesadaran Masyarakat Pemerintah harus meningkatkan kampanye edukasi dan kesadaran kepada masyarakat, pelaku usaha, dan instansi pemerintah tentang pentingnya menjaga keamanan data dan sistem elektronik serta risiko hukum yang dihadapi jika melakukan atau membantu tindak pidana siber.Kerja Sama InternasionalMengingat kejahatan siber bersifat lintas negara, pemerintah perlu memperkuat kerja sama internasional dengan negara lain dalam bidang penegakan hukum, pertukaran informasi, dan pencegahan kejahatan siber.
2. Saran kepada aparat penegak hukum dalam menangani tindak pidana menjebol sistem pengamanan (*cybercrime/hacking*) perlu mencakup aspek penegakan hukum, pencegahan, peningkatan kapasitas, dan kolaborasi lintas sektor Penegakan Hukum yang Tegas dan ProporsionalTerapkan UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) beserta perubahannya secara konsisten dan proporsional, terutama Pasal 30–33 yang mengatur akses ilegal terhadap sistem elektronik.Pastikan penindakan tidak hanya menyasar pelaku utama, tetapi juga jaringan atau pihak yang memfasilitasi tindakan tersebut (misalnya penyedia alat atau jasa peretasan).Lakukan penyitaan digital forensik dengan standar hukum yang jelas agar bukti elektronik sah di pengadilan.
3. Hakim dapat menyarankan pelaku mengikuti program literasi keamanan siber atau memberikan kontribusi positif di bidang teknologi (seperti membantu penguatan sistem keamanan). Saran PemidanaanBentuk pidana: Penjara dengan masa tertentu atau pidana bersyarat (jika pelaku kooperatif, belum pernah dihukum, dan tidak menimbulkan kerugian besar). Penyitaan alat (komputer/laptop) yang digunakan untuk kejahatan

DOI: https://doi.org/10.47353/sibatik.v5i6.4874

digital. Terapkan Prinsip ProporsionalitasDalam memberikan hukuman, hakim sebaiknya mempertimbangkan tingkat kerugian yang ditimbulkan, niat pelaku (misalnya apakah untuk keuntungan pribadi, sabotase, atau hanya iseng), serta dampak sosial dari tindakannya. Hukuman harus proporsional agar tidak terlalu ringan tapi juga tidak berlebihan.

DAFTAR PUSTAKA

Aco Agus dan Riskawati. 2016. "Penanganan Kasus Cybercrime di Kota Makassar (Studi pada Kantor Kepolisian Resort Kota Besar Makassar)." Jurnal Supremasi, Vol. 10.

Adam Chazawi, Adami, Prija Djatmika, dan Ardi Ferdian. 2005. Tindak Pidana Pers: Penyerangan Terhadap Kepentingan Hukum yang Dilindungi dengan Mempublikasikan Tulisan. Bandung: Mandar Maju.

Agus Raharjo. 2002. Cybercrime: Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi. Cetakan Pertama. Bandung: Citra Aditya Bakti.

Al. Wisnubroto. 2011. Konsep Hukum Pidana Telematika. Cetakan Pertama. Yogyakarta: Universitas Atma Jaya.

Anantia Ayu D., dkk. 2019. Perlindungan Hak Privasi atas Data Diri di Era Ekonomi Digital. Jakarta: Pusat Penelitian dan Pengkajian Perkara dan Pengelolaan Perpustakaan Kepaniteraan dan Sekretariat Jenderal Mahkamah Konstitusi.

Brisilia Tumalun. 2018. "Upaya Penanggulangan Kejahatan Komputer dalam Sistem Elektronik Menurut Pasal 30 Undang-Undang Nomor 11 Tahun 2008." Jurnal Lex et Societatis, Vol. 6, No. 2.

Ediwarman. 2016. Monograf Metodologi Penelitian Hukum. Yogyakarta: Genta Publishing.

Fitri Sucia. 2022. "Pertanggungjawaban Pidana terhadap Pelaku Hacker dengan Tujuan Pemesanan Fiktif." Jurnal Dialektika Hukum, E-ISSN 2808-5191, P-ISSN 2808-5876, Vol. 4, No. 2.

Irhamni Ali. 2012. "Kejahatan terhadap Informasi (Cyber Crime) dalam Konteks Perpustakaan Digital." Jurnal Visi Pustaka, Vol. 14, No. 1.

Isharyanto. 2016. Teori Hukum: Suatu Pengantar dengan Pendekatan Tematik. Jakarta: WR Penerbit.

Joiverdia Arifiyanto. 2024. Perlindungan Data Pribadi dan Regulasi Fintech: Penerapan di Perancis dan Indonesia. Medan: PT Tri Selaras Cendekia.

Muhammad Hasan Rumlus dan Hanif Hartadi. 2020. "Kebijakan Penanggulangan Pencurian Data Pribadi dalam Media Elektronik." Jurnal HAM, Vol. 11, No. 2.

Moeljatno. 2008. Asas-Asas Hukum Pidana. Jakarta: Rineka Cipta.

Priyatno, Admaja. 2004. Kebijakan Legislasi tentang Sistem Pertanggungjawaban Pidana Korporasi di Indonesia. Bandung: CV Utomo.

Raharjo, Satjipto. 2006. Ilmu Hukum. Bandung: Citra Aditya Bakti.

Saleh, Roeslan. 1981. Perbuatan Pidana dan Pertanggungjawaban Pidana: Dua Pengertian Dasar dalam Hukum Pidana. Jakarta: Aksara Baru.

Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana.

DOI: https://doi.org/10.47353/sibatik.v5i6.4874

Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

Wahyudi Djafar dan Asep Komarudin. 2014. Perlindungan Hak atas Privasi di Internet: Beberapa Penjelasan Kunci. Terbitan Pertama. Jakarta: ELSAM.

Wahyudi Djafar, Bernhard Ruben, dan Blandina. 2016. Perlindungan Data Pribadi: Usulan Pelembagaan Kebijakan dari Perspektif Hak Asasi Manusia. Publis Pertama. Jakarta: Lembaga Studi dan Advokasi Masyarakat (ELSAM).

Widodo. 2013. Aspek Hukum Pidana Kejahatan Mayantara. Cetakan Pertama. Yogyakarta: Aswaja.