

**PENGATURAN HUKUM PERETASAN SITUS WEBSITE
YANG DILAKUKAN OLEH WNA DITINJAU DARI
UNDANG-UNDANG NOMOR 19 TAHUN 2016 TENTANG
PERUBAHAN ATAS UNDANG-UNDANG NOMOR 11 TAHUN
2008 TENTANG INFORMASI DAN TRANSAKSI
ELEKTRONIK**

**Anak Agung Gde Putera Semadi^{1*)}, Agus Surya Manika²⁾, I Gede Manik
Harisandhi³⁾**

Universitas Dwijendra, Denpasar, Indonesia

*) e-mail: puterasemadi60@gmail.com

Abstrak

Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik pada Pasal 1 angka 21 bahwa yang dimaksud Orang adalah orang perseorangan, baik warga negara Indonesia, warga negara asing, maupun badan hukum, sehingga aturan tersebut dapat menjerat pelaku yang merupakan warga negara asing. Adapun tujuan penelitian ini adalah untuk mengetahui pengaturan peretasan situs website menurut Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan transaksi Elektronik serta akibat hukum bagi seorang peretas situs website yang merupakan warga negara asing. Metode penelitian yang digunakan adalah metode penelitian normatif yang bertumpu pada pendekatan konsep dan norma serta perundang undangan dengan teknik pengumpulan data melalui studi pustaka. Pengaturan peretasan situs website menurut Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik telah diatur dalam Pasal 30 ayat 1, 2 , dan 3 Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik sementara Akibat hukum bagi seorang peretas situs website yang merupakan warga negara asing dapat dikenakan sanksi berdasarkan Pasal 46 Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

Kata Kunci : Peretasan; Web; Orang Asing

Abstract

Law Number 19 of 2016 concerning Information and Electronic Transactions in Article 1 number 21 that what is meant by Persons are individuals, both Indonesian citizens, foreign citizens, and legal entities, so that these rules can ensnare perpetrators who are foreign citizens. The purpose of this study is to determine the regulations for hacking websites according to Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions and the legal consequences for a website hacker who is a foreign citizen. The research method used is a normative research method that relies on the approach of concepts and norms and laws with data collection techniques through literature study. Arrangements for hacking websites according to Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions are regulated in Article 30 paragraphs 1, 2 and 3 of Law Number 19 of 2016 concerning Amendments to Laws -Law Number 11 of 2008 Concerning Information and Electronic Transactions Temporary Legal consequences for a website hacker who is a foreign citizen may be subject to sanctions based on Article 46 of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions.

Keywords: *Hacking; Web; Foreign Citizen*

PENDAHULUAN

Saat ini ilmu pengetahuan telah mengalami kemajuan yang pesat, begitu juga dengan kemajuan teknologi informasi dan komunikasi. Sejalan dengan perkembangan itu maka berimplikasi pada perubahan sosial (*sosial change*) yang menuju pada pembentukan masyarakat modern (Bungin, 2019). Perubahan pola hidup karena adanya kemajuan tersebut memudahkan masyarakat dalam menjalani kehidupan sehari-hari. Kemudahan yang dirasakan masyarakat yakni lebih mudah dan cepat mengakses berbagai macam hal melalui media sosial atau media *online*, hanya dengan sebuah *smartphone* (telepon genggam berkemampuan tinggi) dapat mengakses berbagai macam hal yang diinginkan, seperti melihat berita terkini, mencari informasi guna menambah wawasan, komunikasi jarak jauh sambil bertatap muka, membagikan foto/video, berbelanja dari rumah, dan lain sebagainya. Namun kenyataannya perkembangan teknologi ini dapat menyebabkan munculnya peluang untuk terjadinya tindak pidana.

Istilah tindak pidana merupakan terjemahan dari *strafbarfeit* yang diartikan sebagai suatu perbuatan yang dapat dikenakan hukuman karena telah melanggar ketentuan peraturan perundang-undangan yang memuat sanksi pidana didalamnya (Prasetyo, 2020). Berdasarkan pemahaman tersebut tindak pidana merupakan suatu perbuatan yang dilarang dan terdapat sanksi pidana apabila dilanggar. Kata

pidana sendiri berasal dari bahasa Belanda yakni *straf* yang diartikan sebagai suatu penderitaan (nestapa) yang sengaja dikenakan/dijatuhkan kepada seseorang yang telah terbukti bersalah melakukan suatu tindak pidana (Khair, 2020). Dalam hal kaitannya dengan kebijakan hukum pidana, salah satu bagian dari dimensi kehidupan sosial saat ini yang perlu kebijakan hukum pidana yakni dampak teknologi informasi yang sangat berkembang dengan pesat menyebabkan banyak perubahan pada segi kehidupan sosial masyarakat, baik ekonomi, sosial politik. Sistem komunikasi dan interaksi, pendidikan, termasuk juga hukum. Teknologi informasi, internet pada awalnya dikembangkan semata-mata untuk memudahkan manusia dalam menjalankan rutinitas kehidupannya (Djanggih, 2013)

Teknologi Informasi dan Komunikasi (TIK) di dalam masyarakat global saat ini merupakan suatu hal yang digunakan oleh masyarakat dalam mempermudah mereka melakukan aktifitas sehari-hari. Salah satu produk teknologi yang saat ini digunakan untuk menguasai serta membantu hampir dari seluruh aspek kehidupan masyarakat pada umumnya adalah internet. Internet adalah jaringan dari seluruh jaringan yang terdiri dari jutaan jaringan yang lebih kecil milik domestik, akademi, bisnis, pemerintahan, militer, non pemerintahan, yang secara bersama-sama membawa berbagai informasi dan pelayanan, seperti surat elektronik (*email*), *online chat*, pengiriman *file*, dan halaman-halaman *web* yang saling terhubung serta sumber lain dari *world wide web* (*www*).

Kemajuan teknologi yang merupakan hasil budaya manusia disamping membawa dampak positif, dalam arti dapat digunakan untuk kepentingan umat manusia juga dapat membawa dampak negatif terhadap perkembangan kejahatan. Pemanfaatan kemajuan teknologi informasi dan komunikasi apabila dipergunakan dengan bijak maka akan berdampak baik, seperti memudahkan pekerjaan sehingga dapat meningkatkan kesejahteraan masyarakat. Sebaliknya apabila kemajuan tersebut digunakan dengan tidak bertanggungjawab maka hal itu dapat disalahgunakan dan dijadikan salah satu alat bantu untuk melakukan suatu tindak pidana yang menyerang kepentingan hukum orang, masyarakat, dan negara (Ferdian, 2018). Salah satu kejahatan yang ditimbulkan oleh perkembangan dan kemajuan teknologi informasi atau telekomunikasi adalah kejahatan yang berkaitan dengan aplikasi internet, kejahatan ini dalam istilah asing disebut dengan *cyber crime*.

Cyber crime berbeda dengan kejahatan tradisional pada umumnya, adapun beberapa perbedaan yang sangat mencolok antara *cyber crime* dengan kejahatan tradisional karena *cyber crime* atau kejahatan komputer dapat dilakukan secara anonim dan anonimitas merupakan cirinya yang utama, kejahatan komputer dapat pula mengakibatkan kerugian finansial yang luar biasa banyaknya dibandingkan kejahatan tradisional pada umumnya, serta kejahatan komputer dapat dilakukan dari tempat yang tidak dapat dideteksi oleh penegak hukum.

Cyber crime sebenarnya secara umum merupakan bentuk kejahatan biasa, hanya saja mengalami perkembangan dengan menggunakan teknologi. Menurut

Dikdik M. Arief Mansur dan Elisatriis Gultom jenis-jenis kejahatan yang termasuk *Cyber crime* dapat dikategorikan sebagai berikut: *cyber-terorisme*, *cyber-pornography*, *cyber-harrasment*, *cyber-stalking*, *cracking*, *carding* dan *hacking* (Gultom, 2005). *Hacking* dapat diartikan sebagai penggunaan *programming abilities* dengan maksud yang bertentangan dengan hukum. Contohnya kasus peretasan pada situs website yang menimbulkan kerusakan digital, ataupun mencuri data-data penting pribadi seseorang (Raharjo, 2002).

Peretas sejati menyebut orang-orang ini *cracker* dan tidak suka bergaul dengan mereka. Peretas sejati memandang *cracker* sebagai orang malas, tidak bertanggung jawab, dan tidak terlalu cerdas. Peretas sejati tidak setuju jika dikatakan bahwa dengan menerobos keamanan seseorang telah menjadi peretas. *Crackers* atau *criminal minded hackers*, pelaku kejahatan ini biasanya memiliki motivasi untuk mendapatkan keuntungan finansial, sabotase dan pengrusakan data. Tipe kejahatan ini dapat dilakukan dengan bantuan orang dalam, biasanya staf yang sakit hati atau datang dari kompetitor dalam bisnis sejenis. *Cracker* adalah Seseorang yang dapat dan dapat menembus jaringan dan mencuri / merusak jaringan.

Teknologi informasi di yakini membawa keuntungan yang besar bagi negara-negara di dunia. Maka dari itu lahir suatu rezim hukum baru untuk melindungi kepentingan dan keuntungan tersebut. Tindakan peretasan ini tentu merupakan suatu pelanggaran terhadap Pasal 30 ayat (1) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagaimana diubah dan ditambah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yang menyatakan bahwa:

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

Sanksi pidana terhadap tindak pidana peretasan ini juga telah diatur dalam Pasal 46 ayat (1) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang berbunyi:

“Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp 600.000.000,00 (enam ratus juta rupiah)”.

Dijelaskan dalam Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik pada Pasal 1 angka 21 bahwa yang dimaksud Orang adalah orang perseorangan, baik warga negara Indonesia, warga negara asing, maupun badan hukum, sehingga aturan hukum pada pasal 30 Ayat 1 Undang-Undang

Nomor 19 Tahun 2016 Tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dapat menjerat pelaku yang merupakan warga negara asing. Namun dalam pasal tersebut tidak memperjelas mengenai apakah pasal tersebut juga menjerat apabila pelaku tersebut berlokasi di luar negeri, dan bagaimanakah tindakan yang dilakukan untuk menjerat pelaku yang melakukan peretasan namun berlokasi di luar negeri, sehingga tidak jelas tindakan apa yang dilakukan Indonesia terhadap pelaku tersebut. Disini terjadi kekaburan norma dalam pasal 30 Ayat 1 Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Mengingat kejadian *hacking* belakangan ini sering terjadi di Indonesia, maka permasalahan tersebut harus segera ditemukan solusinya dan diterapkan demi mencegah pelaku lolos dari jeratan hukum. Berdasarkan latar belakang permasalahan yang diuraikan diatas, maka penulis merumuskan permasalahan sebagai berikut 1. Bagaimanakah Pengaturan peretasan situs website menurut Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan 2. Bagaimanakah akibat hukum bagi seorang peretas situs website yang merupakan warga negara asing?

METODE

Jenis penelitian yang dipergunakan dalam penelitian ini adalah jenis penelitian hukum normatif (*normative law research*) Pada penelitian ini dimana dalam pasal 30 Ayat 1 Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dapat menjerat pelaku yang merupakan warga negara asing. Namun dalam pasal tersebut tidak memperjelas mengenai apakah pasal tersebut juga menjerat apabila pelaku tersebut berlokasi di luar negeri, dan bagaimanakah tindakan yang dilakukan untuk menjerat pelaku yang melakukan peretasan namun berlokasi di luar negeri, sehingga tidak jelas tindakan apa yang dilakukan Indonesia terhadap pelaku tersebut. Disini terjadi kekaburan norma dalam pasal 30 Ayat 1 Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

HASIL DAN PEMBAHASAN

Pengaturan Peretasan Situs Website Menurut Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

Kemajuan teknologi pada saat ini telah berkembang dengan pesat sehingga menyebabkan dunia yang tanpa batas dan secara langsung maupun tidak langsung mengubah pola hidup dan perilaku masyarakat di dunia yang dapat menyebabkan

perubahan dalam hidup mereka misalnya perubahan sosial, ekonomi, budaya dan tidak menutup kemungkinan dalam hal penegakan hukum di dunia. Perkembangan dan pemanfaatan teknologi informasi, media dan komunikasi misalnya komputer, *handphone*, *facebook*, *email*, internet dan lain sebagainya telah mengubah perilaku masyarakat dan peradaban manusia secara global. Teknologi informasi dan komunikasi ini telah dimanfaatkan dalam kehidupan sosial masyarakat dalam berbagai sektor kehidupan baik sektor pemerintahan, bisnis, perbankan, pendidikan, kesehatan, kehidupan pribadi dan lain sebagainya.

Peranan teknologi informasi dan komunikasi pada era globalisasi telah menempatkan pada posisi yang amat strategis karena menghadirkan suatu dunia tanpa batas, jarak, ruang, dan waktu, yang berdampak pada peningkatan produktivitas dan efisiensi. Pengaruh globalisasi dengan penggunaan sarana teknologi informasi dan komunikasi telah mengubah pola hidup masyarakat, dan berkembang dalam tatanan kehidupan baru dan mendorong terjadinya perubahan sosial, ekonomi, budaya, pertahanan, keamanan, dan penegakan hukum.

Teknologi informasi dan komunikasi ini dapat memberikan manfaat yang positif, namun di sisi yang lain, juga perlu disadari bahwa teknologi ini memberikan peluang pula untuk dijadikan media melakukan tindak pidana atau kejahatan-kejahatan yang disebut secara populer sebagai *Cyber crime* (kejahatan di dunia maya) sehingga diperlukan (*Cyber Law*) hukum dunia maya (Suharjo, 2024).

Cyber crime adalah sebuah bentuk kriminal yang mana menggunakan internet dan komputer sebagai alat atau cara untuk melakukan tindakan *criminal*. Jadi, *cyber crime* merupakan bentuk kriminal yang menggunakan internet dan komputer sebagai alat atau cara untuk melakukan tindakan kriminal. Dalam definisi lain, kejahatan dunia maya adalah istilah yang mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer menjadi alat, sasaran atau tempat terjadinya kejahatan.

Hal yang perlu diperhatikan bahwa *cyber crime* ini selain dikenal dengan istilah *hacking* maupun *hacker*, ada juga istilah lainnya ialah *cracking* maupun *cracker* yang mana hal ini mempunyai persamaan dan perbedaan antara *hacking* dengan *cracking*. Kejahatan yang dilakukan oleh *cracking* ataupun *cracker* salah satunya ialah *Phising* karena kejahatan ini tujuannya untuk menguntungkan diri sendiri dan tentunya merugikan pihak lain jika menjadi korban dari *cyber crime* dalam bentuk *phising* ini. Dalam ruang lingkup keamanan komputer, *phising* adalah salah satu kejahatan elektronik dalam bentuk penipuan. Dimana proses *phising* ini bermaksud untuk menangkap informasi yang sangat sensitif seperti *username*, *password* dan detil kartu kredit dalam bentuk meniru sebagai sebuah entitas yang dapat dipercaya/*legitimate organization* dan biasanya berkomunikasi secara elektronik (Rachmawati, 2014).

Perkembangan khususnya pasca amandemen konstitusi Undang-Undang Dasar 1945, hak atas privasi termasuk di dalamnya perlindungan data pribadi

diakui sebagai salah satu hak konstitusional warga negara. Hal ini sejalan dengan dimasukkannya bab khusus tentang hak asasi manusia (*bill of rights*) dalam konstitusi, yakni di bab XA Pasal 28A sampai dengan Pasal 28J. Ketentuan mengenai jaminan perlindungan data pribadi dapat ditemukan di dalam Pasal 28G ayat (1), berbunyi:

“Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi.”

Di era perkembangan digital saat ini, Indonesia telah memiliki aturan soal perlindungan data pribadi, namun belum cukup untuk meminimalisir persoalan-persoalan yang muncul seperti peretasan dan pembobolan data pribadi pengguna. Adapun aturan-aturan itu dituangkan dalam bentuk Peraturan Menteri (PERMEN) Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi (PDP) ditetapkan pada 7 November 2016, diundangkan dan berlaku sejak 1 Desember 2016. Permen ini adalah satu dari 21 Permen yang merupakan turunan dari Peraturan Pemerintah (PP) No 82 Tahun 2012 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE) yang diundangkan dan berlaku sejak 15 Oktober 2012. Pada Oktober lalu, Kominfo mengeluarkan Peraturan Pemerintah nomor 71 tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE), yang merupakan pembaharuan dari Peraturan Pemerintah Nomor 82 tahun 2012. Revisi aturan ini menimbulkan kritikan dari banyak pihak. Termasuk beberapa komisi I DPR RI, karena dalam aturan itu pemerintah melalui Kemenkominfo mengizinkan data-data tertentu dapat disimpan di luar Indonesia.

Perlindungan data pribadi sangat penting saat melakukan transaksi online karena data pribadi terkait dengan keamanan pengguna. Karena posisi pengguna yang rentan, ia harus dilindungi secara hukum (tri Celina K. S., 2011). Di dalam Kamus Besar Bahasa Indonesia, memberikan definisi perlindungan ialah sesuatu hal (perbuatan dan sebagainya) dengan tujuan memperlindungi, sedangkan data adalah keterangan yang benar dan nyata atau dalam artian informasi dalam bentuk yang dapat diproses oleh komputer, seperti representasi digital dari teks, angka, gambar grafis, atau suara. Sedangkan pengertian dari pribadi adalah keadaan manusia sebagai perseorangan. Maka kemudian dapat disimpulkan bahwa perlindungan data pribadi ialah suatu perlindungan yang diberikan kepada seseorang atas segala keterangan dan informasi yang benar dan nyata. Dalam kajian ini, perlindungan yang diberikan kepada pengguna ialah perlindungan data pribadi di aktivitas transaksi *online Marketplace*, perlindungan yang diberikan untuk jaminan dan keamanan data pribadi pengguna dari serangan dan peretasan oleh pihak yang tidak bertanggungjawab, sebut saja *hacker*.

Perlu diketahui bahwa perlindungan data pribadi ini merupakan hak yang dimiliki oleh setiap individu/ setiap orang untuk disimpan dan dirahasiakan hal-hal yang bersifat pribadi. Untuk itu salah satu bentuk perlindungan data pribadi ini

ialah dengan cara hadirnya negara sebagai pelindung masyarakat. Pasal 28 G Undang-Undang Dasar 1945 memberikan amanat kepada negara perihal Perlindungan data pribadi ini untuk mengandung penghormatan atas nilai-nilai Hak Asasi Manusia dan nilai-nilai persamaan serta penghargaan atas hak perseorangan sehingga perlu diberikan landasan hukum untuk lebih memberikan keamanan privasi dan data pribadi dan menjamin terselenggaranya iklim dunia usaha yang kondusif.

Peretasan situs web telah diatur dalam Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Undang-Undang No. 19 Tahun 2016 yang merupakan perubahan atas Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang merupakan piranti hukum terbesar yang diharapkan dapat mengakomodir segala jenis pelanggaran dalam bidang IT. Disamping terdapat perlindungan hukum, disana juga terdapat ancaman sanksi pidana atas pelanggaran yang dilakukan.

Tindak pidana peretasan situs web telah diatur dalam Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik yaitu dalam Pasal 30 Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

Berdasarkan Pasal 30 Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, berbunyi:

- (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. Dan,
- (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.

Pasal 30 ayat (1) UU ITE: “setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apapun”. Dalam pasal ini sudah jelas tertera unsur setiap orang, unsur dengan sengaja dan tanpa hak melawan hukum, unsur mengakses komputer dan/atau sistem elektronik milik orang lain, serta unsur dengan cara apapun.

- a. Unsur setiap orang.

Dalam unsur ini setiap orang yang dimaksud adalah orang sebagai subjek hukum yang dapat bertanggungjawab dan cakap hukum berdasarkan atas Perundang-Undangan.

- b. Unsur dengan sengaja dan tanpa hak melawan hukum.

Unsur ini merujuk pada niat atau kesengajaan dan penuh dengan kesadaran dari orang tersebut dalam melakukan suatu tindakan yang melawan hukum.

- c. Unsur mengakses komputer dan/ atau sistem elektronik milik orang lain.

Unsur ini memberi gambaran bahwa sistem elektronik milik orang lain itu berarti hal yang bersifat pribadi milik orang lain dan bukan bersifat untuk umum.

- d. Unsur dengan cara apapun.

Dengan cara apapun yang dimaksud dalam hal ini adalah baik peretas tersebut masuk menggunakan perangkat milik korban yang diretas atau melalui perangkat atau jaringan internet.

Sanksi pidana yang dapat menjerat pelaku peretasan tersebut telah diatur secara jelas dalam pasal 46 ayat 1 Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik yakni “setiap orang yang memenuhi unsur sebagaimana dimaksud dalam pasal 30 ayat (1), dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/ atau denda paling banyak Rp.600.000.000,00(enam ratus juta rupiah).

Berdasarkan Pasal 30 ayat (2) Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik ini memiliki unsur yang sama seperti pada pasal 30 ayat (1), namun ayat (2) terdapat unsur memperoleh informasi elektronik dan/ atau dokumen elektronik, hal tersebut berarti orang yang mencoba masuk kedalam sistem tersebut memilikitujuan untuk mencuri suatu data atau informasi elektronik yang terdapat dalam sistem milik korban. Pasal 30 ayat (2) ini berkaitan langsung dengan pasal 46 ayat (2) Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik mengenai ancaman pidana jika melanggar ketentuan pasal 30 ayat (2), yang berbunyi: “Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam pasal 30 ayat (2), dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/ atau denda paling banyak Rp.700.000.000,00 (tujuh ratus juta rupiah)”.

Unsur dalam pasal 30 ayat (3) Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik terdapat unsur dengan melanggar, menerobos, melampaui, atau menjebol sistem keamanan. Unsur ini memberi indikasi bahwa pelaku peretasan atau hacker melakukan tindakan tersebut dengan cara menerobos

sistem keamanan komputer tersebut. Untuk sanksi pidananya sendiri telah diatur dalam pasal 46 ayat (3) dimana untuk pelanggaran tersebut dikenakan hukuman kurungan penjara seberat-beratnya 8 (delapan) tahun dan/atau membayar denda sebanyak-banyaknya Rp.800.000.000,00 (delapan ratus juta rupiah).

Pasal 32 ayat 1 Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, yang berbunyi: (1) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik orang lain atau milik publik.

Aturan lainnya, Pasal 22 huruf B Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi yang berbunyi Setiap orang dilarang melakukan perbuatan tanpa hak, tidak sah, atau memanipulasi akses ke jaringan telekomunikasi; dan atau akses ke jasa telekomunikasi; dan atau akses ke jaringan telekomunikasi khusus.

Akibat Hukum Bagi Seorang Peretas Situs Website Yang Merupakan Warga Negara Asing

Akibat hukum adalah akibat yang diberikan oleh hukum atas suatu peristiwa hukum atau perbuatan dari subjek hukum. Berdasarkan Kamus Bahasa Indonesia, akibat memiliki arti sesuatu yang menjadi kesudahan atau hasil suatu peristiwa, persyaratan, atau keadaan yang mendahuluinya. Menurut Jazim Hamidi. Kata dampak hukum / akibat hukum mengandung maksud dampak atau akibat hukum secara langsung, kuat, atau eksplisit. Dalam kepustakaan ilmu hukum dikenal tiga jenis akibat hukum, yaitu sebagai berikut:

- a. Akibat hukum berupa lahirnya, berubahnya, atau lenyapnya suatu keadaan hukum tertentu;
- b. Akibat hukum berupa lahirnya, berubahnya, atau lenyapnya suatu hubungan hukum tertentu;
- c. Akibat hukum berupa sanksi, yang tidak dikehendaki oleh subjek hukum (perbuatan melawan hukum).

Hukum berfungsi sebagai perlindungan kepentingan manusia, agar kepentingan manusia terlindungi, maka hukum harus dilaksanakan. Pelaksanaan hukum dapat berjalan dan berlangsung secara normal, damai, tetapi dapat juga terjadi pelanggaran hukum, Dalam hal ini, hukum yang dilanggar itu harus ditegakkan.

Mochtar Koesoemaatmadja mengatakan bahwa tujuan pokok penerapan hukum apabila hendak direduksi pada satu hal saja adalah ketertiban (*order*). Ketertiban adalah tujuan pokok dan pertama dari segala hukum, kebutuhan akan ketertiban ini, merupakan syarat pokok (fundamental) bagi adanya masyarakat

yang teratur, di samping itu tujuan lainnya adalah tercapainya keadilan yang berbeda-beda isi dan ukurannya, menurut masyarakat pada zamannya.

Konsep dasar hukum penataan ruang, tertuang di dalam pembukaan UUD 1945 alinea keempat potongannya yang berbunyi “kemudian dari pada itu untuk membentuk suatu Pemerintahan Negara Indonesia yang melindungi segenap bangsa Indonesia dan seluruh tumpah darah Indonesia dan untuk memajukan kesejahteraan umum, mencerdaskan kehidupan bangsa...” ketentuan ini menegaskan bahwa “kewajiban negara” dan “tugas pemerintah” untuk melindungi segenap sumber-sumber insani Indonesia dalam lingkungan hidup Indonesia, yakni segenap bangsa Indonesia sebagai “komponen manusia” dan seluruh tumpah darah Indonesia sebagai komponen sumber daya alam hayati sebagai “komponen fisik” dalam lingkungan hidup Indonesia. Tujuannya adalah untuk kebahagiaan seluruh rakyat Indonesia dan semua umat manusia pada umumnya.

Aturan hukum, baik tertulis maupun tidak tertulis berisi aturan-aturan yang bersifat umum yang menjadi pedoman bagi individu bertingkah laku dalam masyarakat dan menjadi batasan bagi masyarakat dalam membebani atau melakukan tindakan terhadap individu. Adanya aturan semacam itu dan pelaksanaan aturan tersebut menimbulkan kepastian hukum. Jadi dapat disimpulkan bahwa kepastian hukum secara normatif adalah ketika suatu peraturan dibuat dan diundangkan secara pasti karena mengatur secara jelas dan logis, sehingga tidak menimbulkan keragu-raguan (multi-tafsir), logis dan mempunyai daya prediktabilitas.

Peradaban dunia pada masa kini dicirikan dengan fenomena kemajuan teknologi informasi dan komunikasi yang berlangsung hampir di semua bidang kehidupan. Revolusi yang dihasilkan oleh teknologi informasi dan komunikasi biasanya dilihat dari sudut pandang penurunan jarak geografis, penghilangan batas-batas negara dan zona waktu serta peningkatan efisiensi dalam pengumpulan, penyebaran, analisis dan mungkin juga penggunaan data. Revolusi tersebut tidak dapat dipungkiri menjadi ujung tombak era globalisasi yang kini melanda hampir seluruh dunia. Apa yang disebut dengan globalisasi pada dasarnya bermula dari awal abad ke-20, yakni pada saat terjadi revolusi transportasi dan elektronika yang menyebarluaskan dan mempercepat perdagangan antar bangsa, disamping penambahan dan kecepatan lalu lintas barang dan jasa. Teknologi informasi dan media elektronika dinilai sebagai simbol pelopor, yang akan mengintegrasikan seluruh sistem dunia, baik dalam aspek sosial budaya, ekonomi dan keuangan. Dari sistem-sistem kecil lokal dan nasional, proses globalisasi dalam tahun-tahun terakhir bergerak cepat, bahkan terlalu cepat menuju suatu sistem global.

Pemanfaatan teknologi internet juga tidak dapat dipungkiri membawa dampak negatif yang tidak kalah banyak dengan manfaat positif yang ada. Internet membuat kejahatan yang semula bersifat konvensional seperti pengancaman, pencurian, pencemaran nama baik, pornografi, perjudian, penipuan hingga tindak

pidana terorisme kini melalui media internet beberapa jenis tindak pidana tersebut dapat dilakukan secara on line oleh individu maupun kelompok dengan resiko tertangkap yang sangat kecil dengan akibat kerugian yang lebih besar baik untuk masyarakat maupun negara.

Kejahatan mayantara (*cyber crime*) yang timbul akibat adanya kemajuan teknologi yang begitu pesat banyak mengakibatkan dampak negatif dan positif dari adanya teknologi tersebut. Dampak positif dapat berupa adanya e-mail, internet banking, serta hal-hal lain. Namun, perkembangan ini juga membawa pengaruh negatif seperti adanya tindak pidana peretasan (*hacking*) yang dilakukan guna untuk memperoleh informasi atau data-data penting lainnya. Tindakan ini dilakukan tidak hanya semata-mata untuk mencari keuntungan dan menemukan titik lemah dari si target. Kejahatan ini dapat digolongkan lebih relatif baru jika dibandingkan dengan kejahatan konvensional lainnya. Meskipun kejahatan jenis ini telah muncul pada awal tahun 1961, ia tak sepopuler kejahatan konvensional yang selalu mudah dijangkau oleh telinga masyarakat. Sekalipun telah lama ada, namun belum ada kesepakatan para ahli untuk memberikan definisi baik itu kejahatan mayantara (*cyber crime*) maupun tindak pidana peretasan itu sendiri. Kendati demikian, telah banyak yang memakai istilah siber, kejahatan dunia maya, kejahatan firtual, dan bahkan tetap menggunakan istilah *cyber crime*.

Kemampuan membuat suatu program yang disalahgunakan oleh seseorang yang tidak bertanggungjawab menyebabkan terjadinya sebuah pelanggaran norma atau hukum yang berlaku guna merugikan beberapa pihak yang telah sejak awal menjadi target sasaran. Salah satu contohnya adalah tindakan meretas situs web atau akun media sosial yang bersifat pribadi milik orang lain. Ketentuan yang secara khusus mengatur mengenai tindak pidana peretasan telah termuat dalam pasal 30 ayat (1), (2), dan (3) Undang-Undang ITE. Pasal ini menjelaskan bahwa setiap orang yang mencoba masuk atau mengakses sistem elektronik milik orang lain dengan cara apapun dengan sengaja dan tanpa hak melawan hukum. Pasal ini berkaitan langsung dengan pasal 46 ayat (1), (2), dan (3) Undang-Undang ITE yang mengatur mengenai sanksi pidana atas pelanggaran yang tercantum dalam pasal 30 tersebut diatas.

Melakukan penegakan hukum khususnya dalam bidang kejahatan mayantara, kejahatan ini memiliki jangkauan yang sangat luas tanpa mengenal batas wilayah teritorial suatu negara karena kejahatan ini bersifat transnasional. Tipe kejahatan yang tak mengenal batas ini mengharuskan yurisdiksi suatu negara terlibat langsung di dalamnya karena sangat jauh dari jangkauan suatu negara. Jika tanpa melakukan kerja sama antar negara dalam melakukan pemberantasan serta penegakan hukum yang sebagaimana mestinya, kejahatan yang bersifat transnasional ini akan menimbulkan masalahnya sendiri berkenaan dengan yurisdiksi.

SIMPULAN

Pengaturan peretasan situs website menurut Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik telah diatur dalam Pasal 30 yaitu pada ayat (1) memuat “Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apapun”, pada ayat (2) memuat "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" , dan ayat (3) yang memuat "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apapun dengan melanggar, menerobos, melampaui, atau menjebol system pengamanan”.

Akibat hukum bagi seorang peretas situs website yang merupakan warga negara asing dapat dikenakan sanksi berdasarkan Pasal 46 Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik yang memiliki sanksi yang berbeda tergantung pada tindakannya diantaranya pada ayat (1) memuat “Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam pasal 30 ayat (1), dipidana dengan pidana penjara paling lam 6 (enam) tahun dan/atau denda paling banyak Rp 600.000.000,00 (enam ratus juta rupiah)”. Pada ayat (2) memuat “Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam pasal 30 ayat (2), dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp 700.000.000,00 (tujuh ratus juta rupiah)”, dan pada ayat (3) memuat “Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (3), dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp800.000.000,00 (delapan ratus juta rupiah)”.

DAFTAR PUSTAKA

- Arief Mansur dan Elisatris Gultom, Dikdik M. 2005. *Cyber Law: Aspek Hukum Teknologi Informasi*. PT. Refika Aditama. Bandung.
- Bungin, B. 2019. *Konstruksi Sosial Media Massa*. Kencana. Jakarta.
- Chazawi, Adami dan Ardian Ferdian. 2018. *Tindak Pidana Informasi dan Transaksi Elektronik*. Bayumedia Publishing. Malang.
- Djanggih, H. (2013). Kebijakan Hukum Pidana Dalam Penanggulangan Cybercrime di Bidang Kesusilaan. *Jurnal Media Hukum*. Vol.1 No.2
- Ekaputra, Mohd, dan Abdul Khair. 2020. *Sistem Pidana di Dalam KUHP dan Pengaturannya Menurut Konsep KUHP Baru*. USU Press. Medan.
- Prasetyo, Teguh. 2020. *Hukum Pidana Edisi Revisi*. Raja Grafindo Persada. Jakarta.
- Raharjo, Agus. 2002. *Cyber Crime Pemahaman Dana Upaya Pencegahan Kejahatan Berteknologi*. Citra Aditya. Bandung.

- Rachmawati, D. (2014). Phising Sebagai Salah Satu Bentuk Ancaman Dalam Dunia Cyber. *Jurnal Saintikom Vol, 13*(3), 210.
- Suharjo, I., & Setyaningsih, P. W. (2024). Identifikasi Dan Analisis Terjadinya Peretasan Pada Domain Website dari Data Google Cache. *Teknologi: Jurnal Ilmiah Sistem Informasi, 14*(1), 61-70.
- Tri Siwi Kristiyanti, Celina. 2011. *Hukum. Perlindungan Konsumen*. Sinar Grafika. Jakarta.