e-ISSN : 2986-1624
Jurnal Profile Hukum
Volume 3 Nomor 1 Edisi Januari 2025

FAKTOR PENYEBAB DAN PENANGGULANGAN TERJADINYA PERETASAN WHATSAPP

Henny Saida Flora
Fakultas Hukum Universitas Katolik Santo Thomas, Medan
Email : hennysaida@yahoo.com

ABSTRAK

Peretasan merupakan suatu perbuatan /Pembobolan terkait jaringan, sistem, atau komputer tanpa izin dari pengguna. Cybercrime ialah kejahatan yagn dilakukan melalui media virtual yang bisa dilakukan oleh teknologi cyber dan dapat dikategorikan sebagai tindakan kriminal. Kemampuan membuat suatu program yang disalahgunakan oleh seseorang yang tidak bertanggung jawab menyebabkan terjadinya sebuah pelanggaran norma atau hukum yang berlaku guna merugikan beberapa pihak yang telah sejak awal menjadi target sasaran. Faktor penyebab terjadinya peretasan whatsapp secara tidak sengaja korban menyetujui verifikasi sistem keamanan dua langkah atau two factor authentication, dengan cara peretas perlu nomor baru untuk mengaktifkan nomor sasaran dan kemudian diverifikasi melalui kode one time password yang bisa juga dilakukan melalui fitur pengalihan panggilan. Dampak negatif dari penggunaan aplikasi WhatsApp adalah masihmemungkinkan untuk terjadinya proses penyadapan dimana melibatkan dua device yaitu windows dan android. Dengan melakukan proses penyadapan pada aplikasi WhatsApp, pelaku kejahatan bisa mengetahui hal-hal yang penting dan bisa saja melakukan pembobolan data yang didapatkan melalui kode verifikasi *WhatsApp*

Kata Kunci : Penyebab dan Penanggulangan, Peretasan, Whatsapp, Cybercrime

ABSTRACT

Hacking is an act/break-in related to a network, system or computer without permission from the user. Cybercrime is a crime committed through virtual media that can be carried out by cyber technology and can be categorized as a criminal act. The ability to create a program that is misused by someone who is not responsible causes a violation of applicable norms or laws to harm several parties who have been the target from the start. The factor that causes WhatsApp hacking is that the victim accidentally agrees to two-step security system verification or two-factor authentication, by means of which the hacker needs a new number to activate the target number and then verifies it via a one-time password code which can also be done via the call diversion feature. The negative impact of using the WhatsApp application is that it is still possible for the tapping process to occur which involves two devices, namely Windows and Android. By carrying out the tapping process on the WhatsApp application, criminals can find out important things and can hack data obtained through the WhatsApp verification code.

Keywords: Causes and Countermeasures, Hacking, WhatsApp, Cybercrime

PENDAHULUAN

Seperti yang telah diketahui, bahwa perkembangan teknologi saat ini semakin pesat seiring dengan perkembangannya waktu. Salah satu hal yang paling mendasar adalah mulainya muncul aplikasi yang

berbasis media sosial salah satu nya adalah aplikasi WhatsApp. Pada saat ini pengiriman pesan dengan mengandalkan serta menggunakan SMS sudah jarang sekali digunakan. Para pengguna lebih memilih pengiriman pesan secara instan hanya dengan menggunakan aplikasi WhatApp. Penggunaan dari aplikasi WhatsApp pun tergolong tidak begitu sulit dalam pengoprasiannya.

Perkembangan teknologi informasi yang makin pesat seiring berjalannya waktu membuat teknologi dan informais menjadi hal yang sentral dalam masyarakat. Dalam hal ini juga menjadi kebutuhan pokok bagi masyarakat untuk meningkatkan produktivitas keseharian mereka dengan akses yang cepat dalam memperoleh informasi, yang membuat kemajuan teknologi informasi dan komunikasi menjadi pengubah pola hidup masyarakat dan memicu terjadinya perubahan sosial, budaya, ekonomi, pertahanan, keamanan, dan penegakan hukum

Teknologi informasi dan komunikasi telah dimanfaatkan dalam kehidupan sosial masyarakat, dan telah memasuki berbagai faktor kehidupan baik sektor pemerintahan, bisnis, perbankan, pendidikan, kesehatan, dan kehidupan pribadi. Manfaat teknologi informasi dan komunikasi selain memberikan dampak positif juga disadari memberi peluang untuk dijadikan sarana melakukan kejahatan baru (cyber crime). sehingga dapat dikatakan bahwa teknologi informasi dan komunikasi bagaikan pedang bermata dua, dimana selain memberikan kontribusi positif bagi peningkatan kesejahteraan, kemajuan, peradaban manusia, juga menjadi sarana potensial dan sarana efektif untuk melakukan perbuatan melawan hukum. [1]

Cyber crime dapat diartikan sebagai kegiatan illegal dengan perantara komputer yang dapat dilakukan melalui jaringan elektronik global. Pada jaringan kmputer seperti internet, masalah kriminalitas menjadi semakin kompleks karena ruang lingkupnya yang luas. Kriminalitas dalam internet atau cyber crime pada dasarnya adalah suatu tindak pidana yang berkaitan degnan cyber space,baik yang menyerang fasilitas umum di dalam cyber space ataupun kepemilikan pribadi.

Bermacam-macam kejahatan yang dapat timbul dari permainan internet seperit penipuan, penghinaan, pornografi bahkan kejahatan terhadap keamanan negara seperti pembocoran rahasia negara. Money Laundering dan terorisme juga dapat dilakukan melalui internet, terutama dengan penyertaan dan permufakatan jahat. Sehubungan dengan itu asas berlakunya hukum pidana terutama asas universalitas semestinya diperluas terhadap beberapa bentuk delik baru tersebut.

Kejahatan dalam internet ini dapat dibedakan menjadi tiga bagian, yaitu pelanggaran, akses, pencurian data dan penyebaraan informasi untuk tujuan kejahatan seperti melakukan penipuan melalui internet.

Peretasan Aplikasi Whatsapp merupakan kejahatan yang marak terjadi saat ini. Pengguna internet yang semakin meningkat ternyata membuka kesempatan yang lebih besar bagi para hacker online untuk melakukan tindakan yang merugikan banyak pihak pengguna aplikasi Whatsapp.

Cyber crime dapat diartikan sebagai kegiatan ilegal dengan perantara komputer yang dapat dilakukan melalui jaringan elektronik global. Pada jaringan komputer seperti internet, masalah kriminalitas menjadi semakin kompleks karena ruang lingkupnya

[1] Sunarso Siswanto, 2009, H*ukum Informasi dan Transaksi Elektronik, Studi Kasus Prita Mulyasari*, Rineka Cipta, Jakarta, hlm.. 4.

yang luas. Kriminalitas dalam internet atau cyber crime pada dasarnya adalah suatu tindak pidana yang berkaitan dengan cyber space baik yang menyerang fasilitas umum di dalam cyber space atau pun kepemilikan pribadi.

Kejahatan di internet ini dapat dibedakan menjadi tiga bagian yaitu pelanggaran,akses, pencurian data, dan penyebaran informasi untuk tujuan kejahatan seperti melakukan penipuan melalui internet.

Peretasan aplikasi whatsapp merupakan kejahatan yang marak terjadi saat ini. Pengguna internet yang semakin meningkat ternyata membuka kesempatan yang lebih besar bagi para hacker online untuk melakukan tindakan yang merugikan banyak pihak pengguna aplikasi Whatsapp. Peretasan aplikasi bisa dilakukan dengan berbagai modus. Biasanya pelaku akan membajak akun-akun yang dianggap menguntungkan seperti akun whatsapp orang -orang yang memiliki kedudukan tinggi. Jika sudah mampu dibajak maka hacker dapat melakukan aksi-aksi yang merugikan korban seperti melakukan penipuan secara online, memanipulasi data,bahkan pencemaran nama baik. Undang-undang yang mengatur permasalahan tindak pidana peretasan (hacking) ini adalah Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yaitu Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang perubahan atas UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang diundangkan pada tanggal 25 November 2016. sebenarnya dahulu pada tahun 1999 Indonesia ada membuat UU Nomor 36 Tahun 1999 tentang Telekomunikasi, namun UU ini dianggap kurang mampu untuk menjerat peretasan (hacking). hal ini disebabkan oleh substansi dalam UU Nomor 36 Tahun 1999 ini tidak ada memuat aturan yang jelas dan nyata tentang larangan melakukan perbuatan peretasan (hacking) di Indonesia. Peratasan aplikasi Whatsapp bisa dikatakan sebagai kejahatan yang cukup serius sehingga memerlukan penanganan yang tepat mengingat potensi terjadinya kejahatan ini sangatlah besar.

PEMBAHASAN

1. Pengertian Tindak Pidana Peretasan

Perkembangan teknologi informasi telah mengubah hampir semua sisi kehidupan. Pada satu sisi teknologi komputer memberikan keuntungan berupa kesempatan untuk mendapatkan informasi, pekerjaan, berpartisipasi dalam politik dan kehidupan berdemokrasi serta keuntungan lain. Akan tetapi pada sisi lain ia akan semakin menggerogoti kehidupan nyata yang telah lama digeluti dengan segala peninggalan yang harus dipecahkan sebelum ia bergerak lebih jauh menyusuri jalan dan lorong-lorong cyberspace. Bagi mereka yang memanfaatkan teknologi informasi ini untuk kegiatan bisnis, pelayanan publik dan media hiburan dengan membangun situs-situs yang dapat dikunjungi oleh masyarakat. Tetapi harus berhati-harti karena tidak semua masyarakat yang berkunjung ke dunia maya menikmati realitas virtual yang ditawarkan pada situs-situs, seperti halnya dalam kehidupan nyata di sana juga ada kejahatan yang dampaknya akan dirasakan dalam kehidupan nyata.

Peraturan perundang-undangan di Indonesia tidak mengenal istilah hacking. Secara harafiah hacking berasal dari katan hack dari bahasa Inggris yang berarti mencincang atau membacok. Namun dalam kejahatan internet pengertian peretasan (hacking) adalah suatu perbuatan penyambungan dengan cara menambah terminal komputer baru pada sistem jaringan komputer tanpa izin/secara melawan hukum dari pemilik sah jaringan komputer tanpa izin/secara melawan hukum dari pemilik sah jaringan komputer tersebut dan pelakunya

disebut dengan istilah hacker. Namun bagi komunitas hacker istilah penjahat komputer disebut dengan cracker, bedanya hacking membuat sesuatu, sedangkan cracking menghancurkan/merusaknya.

Secara lebih spesifik hacker didefinisikan sebagai seseorang yang memiliki keinginan untuk melakukan eksplorasi dan penetrasi terhadap sebuah sistem operasai dan kode komputer pengaman lainnya, tetapi tidak melakukan tindakan pengrusakan apapun, tidak mencuri uang atau informasi. Sedangkan cracker adalah sisi gelap dari hacker dan memiliki ketertarikan untuk mencuri informasi, melakukan berbagai macam pengrusakan dan sekali waktu juga melumpuhkan keseluruhan sistem komputer. Perbedaan terminologi antara hacker dan cracker terkadang menjadi bias dan hilang sama sekali dalam perspektif media massa dan masyarakat umu. Para cracker juga tidak jarang menyebut diri mereka sebagai hacker sehingga menyebabkan citra hacking menjadi buruk. [2]

Para cracker ini memanfaatkan informasi dari hacker dan memanfaatkan informasi itu untuk melakukan kegiatan peretasan (hacking) atau disesuikan dengan istilah pelakunya dinamakan dengan cracking. Cracker tidak harus atau tidak selalu memiliki kemampuan seperti yang dimiliki oleh hacker (seperti pemprograman). Masyarakat yang berada di luar komunitas internet, baik media massa, maupun masyarakat umum,lebih familiar menggunakan istilah hacker untuk setipa perilaku eksplorasi dan penetrasi sebuah sistem komputer yang dilakukan secara ilegal dan cenderung bersifat merugikan pihak lain.

Kemampuan membuat suatu program yang disalahgunakan oleh seseorang yang tidak bertanggung jawab 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 oranglain. Dengan adanya teknologi internet akan menghilangkan batas wilayah negara yang menjadikan dunia ini begitu dekat dan sempit, saling berhubungan antara jaringan yang satu dengan yang lain memudahkan pelaku kejahatan untuk melakukan aksinya. [3]

Hacking merupakan suatu seni dalam menembus sistem komputer untuk mengetahui seperti apa sistem tersebut dan bagaimana fungsinya, sebagaimana dikatakan Revalation Loa Ash dalam bukunya Maskun" Hacking adalah ilegal karena masuk dan membaca data seseorang dengan tanpa izin atau secara sembunyi-sembunyi sama saja dengan phissing people off atau membodohi orang sehingga para hacker/phreake selalu menyembunyikan identitas mereka. [4]

Hacking (peretasan) merupakan suatu proses menganalisis, memodifikasi, menerobos masuk ke dalam komputer dan jaringan komputer, baik untuk keuntungan atau dimotivasi oleh tantangan. [5] hacker sebutan bagi seorang yang melakukan aktivitas ini berupaya mencari celah komputer atau jaringan komputer guna mencari keuntungan tertentu.

Peretasan (hacking) dikategorikan sebagai tindak pidana karena dianggap mengganggu ketertiban dalam masyarakat karena dapat menimbulkan kerugian berupa

[2] Richadr Mansfield, 200, *Hacker* Attac,Sybex, Manhaattan, hlm. 23.

[3] Maidin Gultom& Juna Kaban, 2021, *Suatu Tinjauan Tentang Tindak PIdana yang berkaitan dengan Informasi dan Transaksi Elektronik (cybercrime)* Bina Media Perintis, Medan, hlm. 21.

[4] Maskun, 2013, *Kejahatan Cyber Crime*, Kencana, Jakarta, hlm. 46.

[5] Hari Murti, 2005, *Cbyercrime Jurnal teknologi Informasi Dinamik*, hlm. 38.

materil maupun moril. Kerugian materil bisa saja berupa hilangnya uang yang berada dalam satu rekening bank, rusaknya website seseorang yang mengakibatkan orang tersebut harus membiayai perbaikan website tersebut dan sebagainya. Sedangkan kerugian berupa moril dapat berupa tercemarnya nama baik seseorang atau institusi tertentu akibat dari diubahnya informasi dalam website seseorang tanpa izin dari pemiliknya. Pada dasarnya teori sub culture membahas dan menjelaskan bentuk kenakalan remaja serta perkembangan berbagai tip gang. [6]

2. Faktor Penyebab Terjadinya Peretasan

Faktor-faktor yang menyebabkan terjadinya tindak pidana dunia maya (cybercrime) yang merupakan induk dari tindak pidana peretasan (hacking). Faktor-faktor tersebut adalah :

a) Akses internet yang tidak terbatas, dengan menggunakan internet, setiap orang diberikan kenyamanan dalam mengakses segala sesuatu tanpa ada batasannya. Dengan kenyamanan itulah yang merupakan faktor utama bagi sebagian orang untuk melakukan tindak pidana dunia maya (cyber crime) dengan mudahnya.
b) Kelalaian pengguna komputer. Dimana orang-orang menggunakan fasilitas internet selalu memasukkan semua data penting ke dalam internet, sehingga memberikan kemudahan bagi sebagian orang untuk melakukan tindak pidana tersebut.
c) Mudah dilakukan dengan risiko keamanan yang kecil dan tidak diperlukan peralatan yang super modern. Walaupun tindak pidana dunia maya mudah untuk dilakukan tetapi akan sangat sulit untuk melacaknya, sehingga hal ini yang mendorong para pelaku tindak pidana untuk terus melakukan hal ini.
d) Pera pelaku merupakan orang yang pada umumnya cerdas, mempunyai rasa ingin tahu yang besar dan fanatik akan teknologi komputer. Pengetahuan pelaku tindak pidana peretasan tentang cara kerja sebuah komputer jauh di atas rata-rata orang pada umumnya.
e) Sistem keamanan jaringan yang lemah.
f) Kurangnya perhatian masyarakat.

Faktor-faktor penyebab terjadinya tindak pidana peretasan (hacking) terbagi menjadi 2 faktor yaitu :

1) Faktor-faktor internal penyebab terjadinya peretasan (hackig)
   a. Tindak pidana peretasan (hacking) dilakukan oleh pelaku karena didorong motif dendam, iseng, dan atau hanya untuk memenuhi kepuasan pribadi
   b. Tindak pidana peretasan (hacking) dilakukan atas dasar kepentingan pribadi baik yang bersifat materi maupun non materi.
   c. Tindak pidana peretasan (hacking) tidak melakukan tindakan pengrusakan apapun tetapi hanya melakukan eksplorasi dan penetrasi terhadap sebuah sistem operasi dan kode komputer pengaman lainnya.
2) Faktor-faktor eksternal penyebab terjadinya peretasan (hacking):
   a. Kurangnya pengetahuan penegakn hukum di negara Republik Indonesia dalam mengatasi masalah peretasan (hacking)
   b. Sistem keamanan jaringan yang belum bisa mencegah terjadinya tindak pidana peretasan (hacking) dan
   c. Belum adanya badan-badan khusus bentukan pemerintah yang bisa

[6] Henny Saida Flora, 2020, *Kriminologi Faktor Penyebab dan Penanggulangan Kejahatn*, USU PRess, Medan, hlm. 98.

memberikan bantuan terhadap terjadinya tindak pidana peretasan (hacking).

3. Modus Tindak Pidana Peretasan (Hacking)

Modus atau cara yang dilakukan pelaku kejahatan sering berbeda dalam melaksanakan niat jahatnya. Perbedaan modus suatu tindak pidana dengan tindak pidana yang lain disebabkan karena beberapa faktor yakni tempat terjadinya kejahatan, waktu terjadinya kejahatan, maupun dari faktor korban.

Modus tindak pidana peretasan (hacking) jelas berbeda dengan tindak pidana lain. Hal ini disebabkan karena tempat terjadinya tindak pidana peretasan (hacking) jelas berbeda dengan tindak pidana lain pada umumnya.

Tindak pidana pada umumnya terjadi di dunia nyata yang bisa dilihat secara kasat mata, dirasakan ataupun didengar sedangkan tindak pidana peretasan (hacking) terjadi di tempat yang dinamakan dunia maya yaitu suatu tempat yang tidak dapat dilihat langsung, tidak dapat didengar secara langsung, namun bisa dirasakan nyata hasil dari perbuatan tersebut.

Hal ini memang menyebabkan tindak pidana peretasan (hacking) ini sulit untuk diidentifikasi perbuatannya, namun tidak berarti masalah tindak pidana peretasan (hacking) tidak bisa untuk ditanggulangi oleh penegak hukum di negara kita. Masalah tindak pidana peretasan (hacking) hanya dapat dilihat dan didengar melalui bantuan komputer dan sistem elektronik. Adapun modus atau cara terjadinya sebuah tindak pidana peretasan (hacking) adalah :

a. Footprinting , proses mencari informasi tentang korban atau target yang sebanyak-banyaknya. Hal ini dilakukan dengan cara mencari data-data melalui internet, koran atau surat kabar dan media lainnya.
b. Scanning, proses lanjutan dengan menganalisa layanan (service) yang dijalankan dengan server dan router di internet. Biasanya dilakukan dengan ping atau nmap.
c. Enumeration Proces, lanjutan dengan mencoba koneksi ke mesin target
d. Gaining Access, Percobaan hak akses jika telah berhasil masuk ke dalam sistem pada server atau router
e. Covering Tracks, proses menghapus jejak segala macam log pada server atau router agar tidak bisa dilacak
f. Creating Back Doors, menciptakan sebuah jalan rahasia dari sebuah sistem router atau server agar bisa memasuki sistem kembali.
g. Denialof Service, sebuah upaya dilakukan oleh seorang hacker untuk menguasai sistem sudah dilakukan tetapi gagal. Dengan demikian hacker mengambil langkah terakhir yaitu Denial of Service yang merupakan wujud keputusan seorang hacker. Denial of service lebih dikenal dengan Dos yang mana hal ini bisa menyebabkan server atau router mengalami restart bahkan rusak (crash). [7]

4. Upaya Penanggulangan Peretasan melalui Whatsapp

Ketentuan secara khusus mengatur tindak pidana peretasan telah termuat dalam pasal 30 ayat (1) dan (2) dan (3) UU 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 dengan Pasal 46 ayat (1) , (2), dan (3) UU ITE yang mengatur mengenai sanksi pidana atas

[7] M. Linto Herlambang, 2009, B*uku Putih Cracker*, Andi Offeset, LUmajang. Hlm. 1.

pelanggaran yang tercantum dalam pasal 30 tersebut.

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

Seringkali masalah ini menjadi sangat pelik karena kendala sebuah teritorial batas negara. Yurisdiksi dalam hal ini telah mencakup dan bertanggung jawab atas orang benda atau peristiwa hukum yang terjadi di dalamnya. Hukum internasional telah membagi beberapa prinsip yang dapat menjadi acuan dalam masalah yurisdiksi yakni prinsip territorial,prinsip nasionalitas, prinsip perlindungan serta prinsip universal.

a. Prinsip terorrial : prinsip ini tergolong pada prinsip yang paling utama dan fundamental dalam suatu kasus yurisdiksi dimana negara berhak atas segala kasus yang terjadi dan berada dalam wilayahnya.
b. Prinsip nasionalitas : dalam prinsip ini negara dianggap berhak untuk mengadili setiap warganegaranya terhadap segala kejahatan yang dilakukannya dimanapun warga negara tersebut berada.
c. Prinsip perlindungan; prinsip ini lebih bersifat melindungi kepentingan vital negaranya.
d. Prinsip universal: prinsip ini lebih bersifat umum dan sebagian dapat diterima oleh masyarakat umum, dimana dalam yurisdiksi ini setiap negara dianggap berhak atau dapat mengadili suatu kejahatan tertentu yang dianggap membahayakan masyarakat dalam lingkup internasional.

Salah satu cara yang dapat dilakukan oleh negara yang memiliki yurisdiksi terhadap pelaku kejahatan yang berada di negara lain adalah dengan meminta kepada negara di tempat pelaku tersebut berada di negara lain adalah dengan meminta kepada negara di tempat pelaku tersebut berada agar dapat menangkap pelaku tersebut. Yurisdiksi terhadap kejahatan mayantara (cybercrime) khususnya dalam tindak pidana peretasan (hacking) dapat dilaksanakan melalui kerja sama internasional berupa ekstradisi, bantuan hukum timbal balik, dan kerjasama antar penegak hukum.

Mengenai ruang lingkup berlakunya hukum pidana dalam kejahatan mayantara ini telah diatur dalam KUHP Indonesia dalam Bab 1 Kesatu KUHP mengenai batas-batas berlakunya suatu aturan dalam hukum pidana, yang mana hal tersebut termuat sembilan pasal dimulai dari pasal 1 sampai dengan Pasal 9. Dalam Pasal 1 tersebut diatur megenai batas berlakunya suatu hukum pidana berdasarkan waktu, sedangkan untuk Pasal 2 sampai dengan Pasal 9 memuat mengenai batas berlakunya hukum pidana berdasarkan atas tempat terjadinya.

Berkenaan dengan hal tersebut, penegakan hukum mengenai tindak pidaan peretasan yang masuk ke dalam ranah kejahatan mayantara dapat dimulai dan dibangun melalui kesadaran masyarakatnya sendiri. Dengan karakteristik yang berbeda dibandingkan dengan kejahatan seperti pembunuhan, pemerkosaan, dan kejahatan lainnya, menyebabkan dalam mengungkap kejahatan ini diharuskan menggunakan teknologi.

Undang-Undang Nomor 19 Tahun 2016 yang merupakan perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang informasi dan transaksi elektronik

yang merupakan piranti hukum terbesar yang diharapkan dapat mengakomodir segala jenis pelanggaran dalam bidang IT. Di samping terdapat perlindungan hukum, disana juga terdapat ancaman sanksi pidana atas pelanggaran yang dilakukan.

Tindak pidana peretasan yang diatur dalam Pasal 30 ayat (1), (2) dan (4) mengandung unsur sebagai berikut :

Pasal 30 ayat 1 UU ITE :"setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik oranglain dengan cara apapun".

Dalam pasal tersebut 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 bertanggung jawab dan cakap hukum berdasarkan atas perundang-undangan.
b. Unsur dengan sengaja dan tanpa hak melawan hukum. Unsur ini merujuk pada niat atau kesengajaaan dan penuh dengan kesadaran dari orang tersebut dalam melakukan suatu tindakan yang melawan hukm
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.

Dalam pasal 30 ayat (1) ini setiap orang dilarang secara tegas masuk ke dalam sistem elektronik milik orang lain yang bersifat privasi atau pribadi. Sanksi pidana yang dapat menjerat pelaku peretasan tersebut telah diatur secara jelas dalam pasal 46 ayat (1) yakni "setiap orang yang memenuhi unsur sebagaimana dimaksud dalam pasal 46 ayat (1) yakni :"setiap orang yang memenuhi unsur sebagaimana dimaksud dalam pasal 30 ayat (1) dipidana dengan idana penjara paling lama 6 tahun dan/atau denda paling banyak Rp. 600.000.000 (enam ratus juta rupiah).

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.

Dalam pasal 30 ayat (2) 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 ke dalam sistem tersebut memiliki tujuan untuk mencuri suatu data atau informasi elektronik yang terdapt dalam sistem milik korban. Pasal 30 ayat (2) ini berkaitan langsung degnan Pasal 46 ayat (2) mengenai ancaman pidana jika melanggar ketentuan pasal 30 ayat (2): "Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (2), dipidana dengan pidana penjara paling lama 7 tahun dana/atau denda paling banyak Rp. 700.000.000 (tujuh ratus juta rupiah)".

Unsur lain dalam Pasal 30 ayat (3) 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 sendirit elah diatur dalam Pasal 46 ayat (3) dimana untuk pelanggaran tersebut dikenakan hukuman kurungan penjara seberat-beratnya

8 tahun dan/atau membayar denda sebanyak-banyaknya Rp. 800.000.000 (delapan ratus juta rupiah).

Pemberatan penjatuhan pidana bagi pelaku peretasan berdasarkan atas objek dan subjek dari tindak pidana yang bersangkutan yaitu :

1. Berdasarkan objek tindak pidana peretasan atau hacking
   a. Pasal 52 ayat (2) UU ITE, dalam pasal ini apabila objek dari pelanggaran ini adalah sistem elektronik yang dimiliki oleh pemerintah atau sistem yang dipergunakan untuk pembayaran publik.
   b. Pasal 52 ayat (3) UU ITE . Pemberatan dalam pasal ini dapat dijatuhkan apabila pelaku peretasan menyerang situs web milik pemerintah yang berhubungan langsung dengan keamanan atau stabilitas negara
2. Berdasarkan objek tindak pidana peretasan atau hacking.
   a. Pasal 52 ayat (2) UU ITE Jurnal Konstruksi Hukum Vol. 1 No 2, 2020,338 Dalam Pasal ini pemberatan penjatuhan hukuman pidana bagi pelaku tindak pidana peretasan apabila objek dari pelanggaran ini adalah sistem elektronik yang dimiliki oleh pemerintah atau sistem yang dipergunakan untuk pelayanan publik.
   b. Pasal 52 ayat (3) UU ITE. Pemberatan dalam pasal ini dapat dijatuhkan apabila pelaku peretasan menyerang situs web milik pemerintah yang berhubungan langsung dengan keamanan atau stabilitas negara.
   c. Berdasarkan atas subjek tindak pidana peretasan atau hacking Pasal 52 ayat (4) UU ITE, pemberatan dapat dijatuhkan apabila terbukti bahwa peretasan tersebut dilakukan oleh korporasi.

Pemerintah dalam melakukan upaya menanggulangi kejahatan mayantara dengan skala nasional telah menerapkan peraturan perundang-undangan yang mengatur secara khusus mengenai IT. Undang-Undang Nomor 19 Tahun 2016 perubahan atas UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik . Kejahatan yang tanap mengenal batas ini bisa saja sangat membahayakan jika tidak ditanggulangi dan tidak memiliki payung hukum yang kuat untuk mengakomodirnya.

Upaya penanggulangan kejahatan tersebut dapat berupa upaya preventif dan upaya represif.

1. Upaya preventif, upaya ini merupakan upaya pencegahan yang dilakukan guna mencegah timbulnya suatu kejahatan di dalam lingkup masyarakat. Beberapa hal yang dapat dilakukan guna mencegah terjadinya suatu kejahatan adalah dengan melakukan edukasi terhadap masyarakat, melakukan pemblokiran, membentuk badan siber dan sandi negara (BSSN).
2. Upaya represif. Upaya ini merupakan salah satu upaya yang bersifat konsepsional, dimana upaya ini dilakukan setelah terjadinya suaut kejahatan. Upaya ini bertujuan untuk menindak pelaku kejahatan seperti penjatuhan sanksi atau penjatuhan pidana sesuai dengan pelanggaran yang telah dilakukan.

KESIMPULAN

1. Faktor penyebab terjadinya peretasan whatsapp secara tidak sengaja korbam menyetujui verifkasi sistem keamanan dua langkah, peretas asal menebak kode OTP akun whatsapp sasaran, peretas bisa menyusupi serangan malware atau trojan di perangkat sasaran, meretas akun whatsapp korban dengan duplikasi

nomor, peretas bisa melakukan aksi dengan cara mengirimkan tautan, menyadap komunikasi handphone korban, baik dengan cara pencegatan aktif atau pasif (active/passive intercept), melakukan peretasan kepada pihak ketiga penyedia layanan SMS Blast yang mengirimkan kode OTP ke handphone korban, melalui akses fisik kepada smarthphone korban, peretas dapat menggunakan perangkat mata-mata untuk mengambil alih semua informasi di smartphone korban, termasuk akun whatsapp miliknya

2. Upaya penanggulangan peretasan whatsapp mengacu pada UU ITE dan berbagai upaya lain seperti upaya preventif seperti pemblokiran , edukasi terhadap masyarakat, dan hal-hal positif lainnya yang dapat mencegah terjadinya suatu kejahatan serta melakukan upaya represif yang mana upaya ini dilakukan setelah terjadinya suatu tindak pidana, seperti penjatuhan sanksi terhadap pelaku.

DAFTAR PUSTAKA

Ariman Rasyid dan Fahli Raghib, 2015, Hukum Pidana, Setara Press, Malang

Chazawi, Adami, 2010, Hukum Pidana Bagian I, Stelsel Pidana, Tindak Pidana, Teori-teori Pemidanaan & Batas Berlakunya Hukum Pidana, Raja Grafindo Persada, jakarta.

Flora, Henny Saida, 2020, Kriminologi Faktor Penyebab dan Penanggulangan Kejahatan, USU Press, Medan

Gultom Maidin, & Juna Kaban,2021, (Suatu Tinjauan tentang Tindak Pidana yang Berkaitan dengan Informasi dan Transaksi Cyber Crime), Bina Media, Medan

Herlambang, M. Linto, 2009, Buku Puti Cracker, Andi Offset, Lumajang

Marzuki, Peter Mahmud, 2010, Penelitian Hukum Revisi, Kencana Predana Media Grup, Jakarta

Maskun, 2013, Kejahatan Cyber Crime, Kencana, Jakarta

Moeljatno, 2000, Asas- Asas Hukum Pidana, Rineka Cipta, Jakarta

Muhammad, Abdulkadir, 2004, Hukum dan Pneelitian Hukum, Citra Aditya Bakti, Bandung

Lumintang, PAF, 2002, Dasar-dasar Hukum Pidana Indonesia, Cetakan ke3 , Storia Grafika, Bandung.

Poernomo, Bambang, 1992, Asas-Asas Hukum Pidana, Ghalia Indonesia, Jakarta

Richard Mansfield, 2000, Hacker Attack Sybe, Manhattan

Roni, Wijanto, 2012, Asas- Asas Hukum Pidana Indonesia, Mandar Maju , bandung

Sudarto, 1981, Kapita Selekta Hukum Pidana, Alumni, Bandung

Sunarso, Siswanto, 2009, Hukum Informasi dan Transaksi Elektronik, Studi Kasus Prita Mulyasari, Rineka Cipta, Jakarta

Republik Indonesia, Undang-Undang Dasar Negara Tahun 1945

----------, Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik.