Journal of Science and Social Research ISSN 2615 – 4307 (Print)
May 2025, VIII (2): 1707 – 1717 ISSN 2615 – 3262 (Online)
Available online at http://jurnal.goretanpena.com/index.php/JSSR

PERTANGGUNGJAWABAN PIDANA TERHADAP PELAKU HACKING YANG DENGAN SENGAJA DAN TANPA HAK ATAU MELAWAN HUKUM DALAM TINDAK PIDANA CYBER CRIME (DITINJAU DARI UNDANG-UNDANG NOMOR 1 TAHUN 2024 TENTANG PERUBAHAN KEDUA ATAS UNDANG-UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK)

Ray Arnata Sembiring[1], M. Eka Putra[2], Joiverdia Arifiyanto[3]
Universitas Sumatera Utara, Medan
e-mail: [1]rayarnatasembiring@gmail.com, [2]moh.ekaputra@gmail.com,
[3]joiverdia@gmail.com

Abstract: *The crime of hacking is a crime committed by entering another person's electronic system that is private, in any way so that it is a prohibited act. Hacking is categorized as one of the crimes in cyberspace because hackers are people who master programming who can hack or hack security systems on computers or networks for certain purposes. The problems in this study are how to regulate hacking in Indonesia, what are the obstacles and efforts in overcoming hacking that is intentional and without rights or against the law in Indonesia, how is the criminal responsibility of hacking perpetrators based on the decision of the Pelaihari District Court Number 9 / Pid.Sus / 2021 / PN.Pli and the decision of the Cikarang District Court Number 515 / Pid.Sus / 2021 / PN.Ckr. The research method used is the normative legal research method by analyzing court decisions. The types of research data are primary data and secondary data and are arranged systematically and analyzed qualitatively and draw conclusions deductively. Based on the research results, it can be seen that the legal regulation of hacking acts in Indonesia is regulated in Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions. The obstacle in overcoming hacking that is intentional and without rights or against the law in cyber crime is in the aspect of digital evidence that is easily removed if not handled in a timely manner.*

Keywords: *Criminal Liability, Hacking, Cyber Crime.*

Abstrak: Tindak pidana peretasan (hacker) merupakan tindak pidana yang dilakukan dengan cara masuk ke dalam sistem elektronik milik orang lain yang bersifat pribadi, dengan cara apapun sehingga merupakan tindakan terlarang. Hacking dikategorikan sebagai salah satu kejahatan di dunia maya karena hacker merupakan orang yang menguasai pemrograman yang dapat melakukan hacking atau peretasan sistem keamanan pada komputer atau jaringan dengan tujuan tertentu. Permasalahan dalam penelitian ini adalah bagaimana pengaturan perbuatan hacking di Indonesia, bagaimana hambatan dan upaya dalam penanggulangan hacking yang dengan sengaja dan tanpa hak atau melawan hukum di Indonesia, bagaimana pertanggungjawaban pidana pelaku hacking berdasarkan putusan Pengadilan Negeri Pelaihari Nomor 9/Pid.Sus/2021/PN.Pli dan putusan Pengadilan Negeri Cikarang Nomor 515/Pid.Sus/2021/PN.Ckr. Metode penelitian yang digunakan adalah metode penelitian hukum normatif dengan menganalisis putusan Pengadilan. Jenis data penelitian ini adalah data primer dan data sekunder dan disusun secara sistematis dan dianalisis secara kualitatif serta menarik kesimpulan secara deduktif. Berdasarkan hasil penelitian dapat diketahui bahwa pengaturan hukum perbuatan hacking di Indonesia diatur dalam Undang-Undang Nomor 19 tahun 2016 tentang tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Hambatan dalam penanggulangan terhadap hacking

yang dengan sengaja dan tanpa hak atau melawan hukum dalam tindak pidana cyber crime adalah pada aspek barang bukti digital mudah dihilangkan jika tidak ditangani dengan tepat waktu.

Kata kunci: Pertanggungjawaban Pidana, Hacking, Cyber Crime.

PENDAHULUAN

Globalisasi telah menjadi pendorong lahirnya era perkembangan teknologi informasi. Fenomena kecepatan perkembangan teknologi informasi ini telah merebak di seluruh belahan dunia. Tidak hanya negara maju saja, namun negara berkembang juga telah memacu perkembangan teknologi informasi pada masyarakatnya masing-masing, sehingga teknologi informasi mendapat kedudukan yang penting bagi sebuah kemajuan bangsa. Seiring dengan perkembangan kebutuhan masyarakat di dunia, teknologi informasi (information technology) memegang peran penting, baik di masa kini maupun di masa mendatang.

Perkembangan yang pesat dalam teknologi internet menyebabkan kejahatan baru di bidang itu juga muncul, misalnya kejahatan manipulasi data, spionase, sabotase, provokasi, money laundry, hacking, pencurian software maupun perusakan hardware dan berbagai macam lainnya. Kejahatan cyber crime dibagi menjadi 2 (dua) kategori, yakni cyber crime dalam pengertian sempit dan dalam pengertian luas. Cyber crime dalam pengertian sempit adalah kejahatan terhadap sistem komputer, sedangkan cyber crime dalam arti luas mencakup kejahatan terhadap sistem atau jaringan komputer dan kejahatan yang menggunakan sarana komputer.

Permasalahan yang muncul kemudian adalah masalah keamanan dan beraktivitas dengan melalui media elektronik, bahkan aktivitas ini telah menimbulkan dimensi kejahatan baru. Kejahatan dalam bidang telematika ini merupakan sisi gelap dari kemajuan teknologi yang memiliki dampak luas bagi seluruh bidang kehidupan modern saat ini. Kejahatan siber ini memiliki banyak jenis yang beberapa di antaranya sebagai berikut : Carding, Hacking, Cracking, Defacing, Phising, Spamming, Malware.

Hacking sebagai sebuah bentuk kegiatan telah ada dan berkembang bersama perkembangan teknologi komputer dan internet. Kemajuan teknologi komputer dan internet saat ini tidak akan terlepas dari hacking. Sebab awal mulanya hacking merupakan suatu bentuk kegiatan seorang hacker (pelaku hacking biasa disebut hacker) untuk meningkatkan performa, menguji sistem, atau mencari bug suatu program komputer dan internet. Oleh karena itu, hacking diperlukan dengan mengoprek, mengubah-ubah, bongkar-pasang sistem, software atau hadware komputer yang telah dimiliki.

Hacking merupakan tindakan kriminal memasuki atau menembus sistem jaringan komputer tanpa izin atau tanpa sepengetahuan pemilik sistem jaringan komputer yang dikunjungi. Pembajakan telah menimbulkan banyak kerugian material maupun non material bagi para korban itu sendiri. Hacking jenis ini tidak hanya dilakukan pada website, tetapi juga pada akun media sosial milik individu. Diantara sekian banyak sisi gelap kemajuan teknologi, teknologi masih memiliki banyak manfaat positif, seperti email, e-commerce, online banking, dan lain-lain.

Budaya hacking di kalangan pengguna teknologi memberikan manfaat, sebab dengan hacking dapat diketahui kelemahan suatu sistem atau produk software maupun hardware sehingga tidak heran jika perusahan besar komputer mulai melirik orang-orang yang memiliki keahlian hacking untuk direkrut. Merekrut hacker bukanlah tanpa maksud dan tujuan, melainkan untuk menguji sistem,

meningkatkan kualitas produk dan lainnya.

Berdasarkan penjelasan di atas, maka hacker bisa berbentuk invidual ataukomunitas yang terorganisir. Lambat laun, dengan semakin berkembangnya teknologi komputer dan internet dan semakin mudahnya orang mempelajari teknologi informasi, memberi dampak munculnya hacker-hacker baru yang tidak boleh diremehkan keahliannya, walaupun sebagian besar hacker belajar secara otodidak.

Tindak pidana peretasan (hacker) merupakan tindak pidana yang dilakukan dengan cara masuk ke dalam sistem elektronik milik orang lain yang bersifat pribadi, dengan cara apapun sehingga merupakan tindakan terlarang. Kejahatan hacking atau peretasan terhadap media sosial baik lembaga maupun milik pribadi berdampak pada kerugian materil dan imateril yang akan dialami oleh korban. Kasus peretasan bertujuan untuk mengambil data-data tertentu yang dimiliki target. Namun, ada juga peretasan yang bertujuan menghancurkan data atau sistem tertentu sehingga berdampak seperti kerusakan digital. Dalam peraturan juga disebutkan kasus kejahatan hacking terkait dengan pengambilan data atau sistem elektronik.
Sebagai contok kasus yang peretasan yang pernah terjadi di Indonesia dan telah berkekuatan hukum tetap adalah : Putusan Pengadilan Negeri Pelaihari Nomor 9/Pid.Sus/2021/PN.Pli dan Putusan Pengadilan Negeri Cikarang Nomor 515/Pid.Sus/2021/PN Ckr.

Berdasarkan putusan di atas, maka jelaslah kejahatan peretasan masih sering terjadi dikalangan masyarakat khususnya yang beraktifitas di dunia maya. Pemerintah dalam menunjukkan komitmennya dalam penegakan hukum terhadap pelaku kejahatan cybercrime telah mengeluarkan produk regulasi yang khusus terkait kejahatan teknologi dan informasi yang diatur dalam UU ITE. Komitmen ini juga sekaligus sebagai bentuk pertanggungjawaban pemerintah terhadap masyarakat yang juga perwujudan tugas negara untuk memberikan perlindungan terhadap warga negaranya.

Tindak pidana hacking yang telah diatur dan dirumuskan dalam pasal-pasal yang dapat menjerat pelaku tindak pidana hacking diakomodir dalam Pasal 30 UU ITE yang menyebutkan :

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.

Konstruksi pasal ini dengan jelas menyebutkan bahwa tindakan illegal yang dilakukan seseorang (criminal) terhadap sistem elektronik orang lain dengan tujuan untuk memperoleh informasi/dokumen elektronik dan/atau upaya pembobolan, penerobosan, dan penjebolan yang melanggar dan melampaui sistem pengamanan adalah sesuatu yang terlarang.
Pelaku tindak pidana tersebut dikenakan sanksi pidana berdasarkan Pasal 46 UU ITE yang menyebutkan :

1. 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).
2. 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).

3. 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 Rp.800.000.000,00 (delapan ratus juta rupiah).

Akses ilegal dan intersepsi yang selama ini diatur dalam Pasal 30 jo. Pasal 46 UU ITE, materi muatan tersebut kemudian dicabut oleh Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-undang Hukum Pidana (UU KUHP).

Undang-Undang Nomor 1 Tahun 2023 Tentang Kitab Undang-Undang Hukum Pidana yang telah disahkan menggantikan KUHP lama ini mencakup materi muatan tentang Cyberlaw khususnya tentang Cybercrime. Pasal Cybercrime UU ITE yang dicabut oleh UU KUHP, yaitu Pasal 27 ayat (1), Pasal 27 ayat (3), Pasal 28 ayat (2), Pasal 30, Pasal 31 ayat (1), Pasal 31 ayat (2), Pasal 36, Pasal 45 ayat (1), Pasal 45 ayat (3), Pasal 45A ayat (2), Pasal 46, Pasal 47, dan Pasal 51 ayat (2). Pasal-pasal ini secara variatif-normatif direkonstruksi, direformulasi, dan dikodifikasi ke dalam UU KUHP. UU KUHP telah diundangkan pada 2 Januari 2023 dan mulai berlaku efektif setelah masa transisi 3 tahun, terhitung sejak tanggal diundangkan.

METODE

Metode Penelitian yang dipakai dalam penulisan ini yaitu jenis penelitian hukum normatif dengan sifat penelitian deskriptif analitis. Bentuk pendekatan penelitian yang digunakan dalam penelitian ini adalah pendekatan perundang-undangan (statute approach). Sumber data dalam penelitian ini meliputi bahan hukum primer, sekunder dan tersier. Teknik pengumpulan data kepustakaan (library research). Untuk menganalisis seluruh bahan hukum yang telah terkumpul, dalam penelitian ini menggunakan analisis data kualitatif.

HASIL DAN PEMBAHASAN

Pengaturan Perbuatan Hacking Di Indonesia

Teknologi telekomunikasi telah membawa manusia kepada suatu peradaban baru dengan struktur sosial beserta tata nilainya. Artinya, masyarakat berkembang menuju masyarakat baru yang berstruktur global. Sistem tata nilai dalam suatu masyarakat berubah, dari yang bersifat lokal-partikular menjadi global universal. Hal ini pada akhirnya akan membawa dampak pada pergeseran nilai, norma, moral, dan kesusilaan. Dampak pergeseran tersebut ditemukanya perkembangan dan kemajuan ilmu pengetahuan dan teknologi, terjadilah konvergensi antara keduanya.

Perkembangan teknologi merupakan salah satu faktor yang dapat menimbulkan kejahatan, sedangkan kejahatan itu sendiri telah ada dan muncul sejak permulaan zaman sampai sekarang dan masa yang akan datang. Bentuk-bentuk kejahatan yang ada pun semakin hari semakin bervariasi. Suatu hal yang patut untuk diperhatikan bahwa kejahatan sebagai gejala sosial sampai sekarang belum diperhitungkan dan diakui untuk menjadi suatu tradisi atau budaya, padahal jika dibandingkan dengan berbagai budaya yang ada, usia kejahatan tentulah lebih tua.

Cybercrime atau kejahatan dunia maya dalam peraturan perundang-undangan di Indonesia juga sering disebut dengan kejahatan tindak pidana yang berkaitan dengan teknologi informasi, hal ini sejalan dengan pengertian yang diberikan oleh Donn B. Parker yang memberikan definisi mengenai penyalahgunaan komputer :“Computer abuse is broadly defined to be any incident associated with computer technology in which a victim suffered or could suffered loss and a perpetrator by

intention made or could have gain", dan diterjemahkan oleh Andi Hamzah sebagai "penyalahgunaan computer didefinisikan secara luas sebagai suatu kejadian yang berhubungan dengan teknologi komputer yang seorang korban menderita atau akan telah menderita kerugian dan seorang pelaku dengan sengaja memperoleh keuntungan atau akan telah memperoleh keuntungan".

Kejahatan di dunia maya atau cyber crime adalah tindak pidana kriminal yang dilakukan pada teknologi internet (cyber space), baik yang menyerang fasilitas umum maupun kepemilikan pribadi. Secara teknik dapat dibedakan menjadi offline crime, semi online crime, dan cyber crime. Contoh dari offline crime adalah dengan cara yang sederhana misal mencuri dompet seseorang untuk kemudian diambil kartu kreditnya, atau bekerjasama dengan kasir untuk mencatat nomor kartu kredit seseorang kemudian menduplikatnya. Contoh teknik semi online crime adalah memasang skimming di mesin ATM untuk mencuri informasi kartu debit korban. Sedangkan untuk cyber crime orang pelaku dan korban tidak perlu bertatap muka, dan bersentuhan, yaitu dengan menggunakan teknologi yang canggih, seperti penggunaan situs palsu klik BCA, dan lain-lain Masing-masing teknik memiliki karakter tersendiri, namun perbedaan utama diantara ketiganya adalah keterhubungan dengan jaringan informasi publik (internet).

Tindakan yang dapat digolongkan menjadi tindakan kejahatan dunia maya/cyber crime adalah melakukan Denial of Service Attack (DoS Attack), Hacking, menulis dan menyebarluaskan virus, cyberterrorism, information warefare/perang informasi, cyberstalking dan online harassment fraud, pencurian identitas/Phising, hacking dan spoofing. Meluasnya jaringan global internet mengisyaratkan adanya harapan akan terjadinya perubahan ruang dan jarak. Perkembangan tersebut jga akan menuju pada terbentuknya sistem tingkah laku tertentu melalui unsur-unsur dominan berupa pengalaman dan budaya dalam penggunaan informasi.

Dunia hukum sebenarnya sudah sejak lama memperluas penafsiran asas dan normanya ketika menghadapi persoalan benda tidak berwujud, misalnya dalam kasus pencurian listrik sebagai perbuatan pidana. Dalam keyataan kegiatan cyber tidak lagi sederhana karena kegiatannya tidak lagi dibatasi oleh wilayah suatu negara, yang mudah diakses kapan pun dan dari mana pun. Kerugian dapat terjadi baik pada pelaku transaksi maupun pada orang lain yang tidak pernah melakukan transaksi, misalnya pencurian kartu kredit melalui pembelanjaan internet.

Berdasarkan Pasal 30 Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik yang mengatur tentang tindak pidana hacking ini dapat dijelaskan unsur-unsur yang termuat dalam tindak pidana hacking tersebut yaitu Pasal 30 Ayat (1) : "Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apapun."

Tindak pidana hacking telah diatur dan dirumuskan dalam pasal-pasal yang dapat menjerat pelaku tindak pidana hacking. Tindak pidana hacking pada dasarnya diatur secara umum pada Pasal 30 Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

Unsur-unsur tindak pidana dalam Pasal 30 Ayat (2) sama seperti pada ayat (1) namun dalam Ayat (2) ini ditambahkan unsur "dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik". Disini dapat diterangkan bahwa seseorang dalam hal mengakses komputer dan/atau sistem elektronik orang lain tanpa hak dan dengan cara apapun dimaksudkan untuk suatu tujuan tertentu, yaitu memperoleh informasi elektronik dan/atau dokumen

elektronik. Kejahatan ini dapat berupa pencurian data atau dokumen elektronik yang digunakan untuk tujuan terntentu. Perbuatan mencuri, merusak, menipu, dan sejenisnya merupakan kejahatan yang sangat merugikan dan terkadang banyak oknum memanfaatkanya guna mencari keuntungan.

Hacking merupakan salah satu kegiatan yang bersifat negatif, meskipun awalnya hacking memiliki tujuan mulia yaitu untuk memperbaiki sistem keaman-an yang telah dibangun dan memper-kuatnya. Tetapi dalam perkembangannya hacking digunakan untuk keperluan-ke-perluan lain yang bersifat merugikan. Hal ini tidak lepas dari pengguna internet yang semakin meluas sehingga penyalah-gunaan kemampuan hacking juga meng-ikuti luasnya pemanfaatan internet. Hacking merupakan permasalahan yang penting dalam jaringan internet global. Hacking dapat diartikan sebagai tindakan dari seorang hacker yang sedang mencari kelemahan dari sebuah sistem komputer. Dimana hasilnya dapat berupa program kecil yang dapat digunakan untuk masuk ke dalam sistem komputer ataupun memanfaatkan sistem tersebut untuk suatu tujuan tertentu tanpa harus memiliki user account. Hacker adalah istilah yang digunakan untuk menggambarkan beberapa tipe kepandaian dalam komputer. Hacker merupakan orang yang melakukan kegiatan hacking.

Undang-undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua 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 ITE. Disamping terdapat perlindungan hukum, disana juga terdapat ancaman sanksi pidana atas pelanggaran yang dilakukan.

Hambatan dan Upaya Penanggulangan Hacking Yang Dengan Sengaja Dan Tanpa Hak Atau Melawan Hukum Di Indonesia

Penegakan hukum kejahatan di dunia maya tidak terlepas dari kebijakan penanggulangan kejahatan atau yang biasa dikenal dengan istilah politik kriminal. Menurut Sudarto politik kriminal merupakan suatu usaha yang rasional dari masyarakat dalam menanggulangi kejahatan. Dari sudut criminal policy, upaya penegakan hukum kejahatan yaitu cybercrime tidak dapat dilakukan semata-mata secara parsial dengan hukum pidana (sarana penal), tetapi harus ditempuh pula dengan pendekatan integral/sistematik. Sebagai salah satu bentuk high tech crime yang dapat melampaui batas-batas negara (bersifat transnational/transborder), merupakan hal yang wajar jika upaya penegakan hukum cybercrime juga harus ditempuh dengan pendekatan teknologi (techno prevention).

Pencegahan kejahatan melalui sarana hukum pidana (politik hukum pidana) harus dilakukan dalam rangka mencapai tujuan kesejahteraan dan perlindungan masyarakat. Perbuatan hacking yang dengan sengaja dan tanpa hak atau melawan hukum termasuk cyber crime yang sanksinya diatur dalam Pasal 27 ayat (3) Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

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.

Menggakses komputer dan/atau sistem elektronik dengan cara apa pun dengan tujuan untuk memperoleh informasi elektronik dan/atau dokumen elektronik.

Mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

Hukum pidana bukan merupakan

solusi utama dalam menanggulangi kejahatan, karena dalam hukum pidana sendiri masih diragukan atau dipermasalahkannya efektivitas sarana penal dalam mencapai tujuan politik kriminal seperti yang dikemukakan oleh Schultz yang menyatakan "Naik turunnya kejahatan disuatu negara tidaklah berhubungan dengan perubahan-perubahan di dalam hukumnya atau kecenderungan-kecenderungan dalam putusan pengadilan, tetapi berhubungan dengan bekerjanya atau berfungsinya perubahan-perubahan kultural yang besar dalam kehidupan masyarakat.

Faktor pihak manajemen pengadilan ikut menambah sulitnya unsur penegakan hukum di lapangan. Sebagai contoh dapat dilihat dalam faktor-faktor penghambat lamanya proses penyelesaian dalam peradilan yaitu banding dan kasasi, terlampau banyak kasus, berkas yang tidak lengkap, rumitnya perkara, kurangnya komunikasi antar lembaga pengadilan, kurangnya sarana atau fasilitas dan adanya tugas sampingan para hakim menambah sulitnya penegakan hukum. Terdapatnya hambatan di dalam penyelesaian perkara bukan semata-mata disebabkan karena banyaknya perkara yang harus segera diselesaikan, sedangkan waktu untuk mengadilinya dan juga usaha menyelesaikannya adalah terbatas. Kalau yang dilakukan hanyalah dengan menambah jumlah hakim untuk menyelesaikan perkara, maka hal itu hanyalah mempunyai dampak yang sangat kecil terutama dalam jangka panjang.
Kesadaran hukum dapat diartikan sebagai kesadaran seseorang atau suatu kelompok masyarakat kepada aturan-aturan atau hukum yang berlaku. Kesadaran hukum sangat diperlukan oleh suatu masyarakat. Hal ini bertujuan agar ketertiban, kedamaian, ketenteraman, dan keadilan dapat diwujudkan dalam pergaulan antar sesama.

Penyidikan yang dilakukan oleh kepolisian akan menelusuri sumber dokumen elektronik tersebut. Praktiknya, biasanya pertama-tama penyidik akan melacak keberadaan pelaku dengan menelusuri alamat Internet Protocol (IP Address) pelaku berdasarkan logIP Address yang tersimpan dalam server pengelola website/hompage yang dijadikan sarana pelaku dalam melakukan tindak pidana hacking.

Permasalahannya adalah, penyidik akan menemui kesulitan jika website/homepage tersebut pemiliknya berada diluar wilayah yuridiksi Indonesia (seperti facebook, google, twitter, yahoo dan lain sebagainya). Meskipun saat ini aparat penegak hukum (polisi maupun Penyidik Pegawai Negeri Sipil Kementerian Komunikasi dan Informatika) telah bekerja sama dengan beberapa pengelola website/homepage di luar wilayah Indonesia, dalam praktiknya tidak mudah untuk mendaptkan IP Address seorang pelaku yang diduga melakukan tindak pidana dengan menggunakan layanan website/homepage tertentu. Hal ini disebabkan adanya perbedaan prosedur hukum antar negara. Permasalahan yuridiksi inilah yang sering menjadi penyebab tidak dan diprosesnya kejahatan cybercrime.

Kepolisian juga sering mengalami hambatan terutama pelaksanaan Pasal 43 ayat (6) Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik yang berbunyi, "Dalam hal melakukan penangkapan dan penahanan, penyidik melalui penuntut umum wajib meminta penetapan ketua Pengadilan Negeri setempat dalam waktu satu kali dua puluh empat jam."

Permasalahan timbul setelah dilakukan penangkapan dan penahanan terhadap kasus cyber crime, karena penangkapan dilakukan pada hari sabtu dan kepolisian mengalami kendala pada saat meminta surat penetapan dari pengadilan stempat. Sedangkan kantor Kejaksaan dan Pengadilan pada hari Sabtu dan Minggu tutup. Karena surat penetapan penangkapan dan penahanan tidak didapat maka proses penangkapan dan penahanan tersebut tidak syah dan perkara dinyatakan tidak lengkap oleh

jaksa penuntut umum.

Pertanggungjawaban Pidana Pelaku Hacking Berdasarkan Putusan Pengadilan Negeri Pelaihari Nomor 9/Pid.Sus/2021/Pn.Pli Dan Putusan Pengadilan Negeri Cikarang Nomor 515/Pid.Sus/2021/Pn.Ckr

Konsep pertanggungjawaban pidana sesungguhnya tidak hanya menyangkut soal hukum semata-mata melaikan juga menyangkut soal nilai-nilai moral atau kesusilaan umum yang dianut oleh suatu masyarakat atau kelompok-kelompok dalam masyarakat, hal ini dilakukan agar pertanggungjawaban pidana itu dicapi dengan memenuhi keadilan. Pertanggungjawaban pidana adalah suatu bentuk untuk menentukan apakah seorang tersangka atau terdakwa dipertanggungjawabkan atas suatu tindak pidana yang telah terjadi. Dengan kata lain pertanggungjawaban pidana adalah suatu bentuk yang menentukan apakah seseornag tersebuut dibebasakan atau dipidana.

Beban pertanggungjawaban dibebankan kepada pelaku pelanggaran tindak pidana berkaitan dengan dasar untuk menjatuhkan sanksi pidana. Seseorang akan memiliki sifat pertanggungjawaban pidana apabila suatu hal atau perbuatan yang dilakukan olehnya bersifat melawan hukum, namun seseorang dapat hilang sifat pertanggungjawabannya apabila didalam dirinya ditemukan suatu unsur yang menyebabkan hilangnya kemampuan bertanggungjawab seseorang.

Dasar dari perbuatan pidana adalah asas legalitas (Pasal 1 ayat (1) KUHP) yang menyatakan bahwa tiada suatu perbuatan yang dapat dipidana kecuali atas peraturan perundang-undangan yang telah ada sebelumnya", sedangkan dasar daripada dipidananya pelaku adalah asas tiada pidana tanpa kesalahan (geen straf zonder shculd).

Menentukan ada atau tidaknya kesalahan pada pelaku tindak pidana, pertama-tama harus ditentukan apakah terdakwa mempunyai kemampuan untuk bertanggung jawab atau tidak atas tindak pidana yang dilakukannya. Kemampuan beratanggung jawab terdakwa berkenaan dengan keadaan jiwa/bathin terdakwa yang sehat ketika melakukan tindak pidana,

Menentukan mampu bertanggung jawab atau tidaknya pelaku dalam melakukan perbuatan pidana diperlukan adanya kerjasama antara dokter/psikiater dan hakim, karena sudah menjadi tugas dan wewenang dokter/psikiater dalam menentukan ada atau tidaknya sebab-sebab ketidakmampuan bertanggung jawab, sedangkan hakim yang menilai apakah karena sebab-sebab tersebut terdakwa mampu bertanggung jawab atau tidak.

Unsur kesalahan merupakan unsur utama dalam pertanggungjawaban pidana. Dalam pengertian perbuatan tindak pidana tidak termasuk hal pertanggungjawaban pidana. Perbuatan pidana hanya menunjuk kepada apakah perbuatan tersebut melawan hukum atau dilarang oleh hukum, mengenai apakah seseorang yang melakukan tindak pidana tersebut kemudian dipidana tergantung kepada apakah seseorang yang melakukan perbuatan pidana tersebut memiliki unsur kesalahan atau tidak.

Kesalahan yang dalam bahasa asing disebut dengan schuld adalah keadaan psikologi seseorang yang berhubungan dengan perbuatan yang ia lakukan yang sedemikian rupa sehingga berdasarkan keadaan tersebut perbuatan tersebut pelaku dapat dicela atas perbuatannya. Pengertian kesalahan di sini digunakan dalam arti luas. Kesalahan dalam KUHP digunakan dalam arti sempit yaitu dalam arti kealpaan sebagaimana dapat dilihat dalam rumusan bahasa Belanda yang berada dalam Pasal 359 dan 360.

Kemampuan bertanggung jawab juga berhubungan dengan umur tertentu bagi pelaku tindak pidana. Artinya hanya pelaku yang memenuhi batas umur tertentu yang memilki kemampuan bertanggung jawab serta memilki kewajiban pertanggung jawaban atas perbuatan yang telah dilakukan, hal ini

dikarenakan karena pada umur tertentu secara psycologi dapat mempengaruhi seseorang untuk melakukan suatu perbuatan. Pada dasar nya anak pada umur tertentu belum dapat menyadari dengan baik apa yang telah dilakukan, artinya anak pada umur tertentu juga tidak dapat memisahkan mana yang baik dan mana yang salah tentu juga hal ini mempengaruhi anak tidak dapat menginsafkan perbuatannya. Apabila anak pada tertentu melakukan tindak pidana dan oleh karena perbuatannya dilakukan proses pidana makan secara psycologi anak tersebut akan terganggu dimasa dewasanya

Hakim dalam proses pemidanaannya wajib memcari dan membuktikan apakah pelaku memiliki unsur kemampuan bertanggung jawab, sebab apabila pelaku tidak memiliki kemampuan bertanggung jawab baik karena usia yang belum cukup umur, atau dikarenakan keadaan psykologi seseorang terganggu maka orang tersebut tidak dapat diminta pertanggung jawabanya.
Seorang pelaku tindak pidana dalam keadaan tertentu tidak dapat melakukan tindakan lain selain melakukan perbuatan tindak pidana, meskipun hal itu tidak di inginkan. Sehingga dengan perbuatan tersebut pelaku nya harus menghadi jalur hukum. Hal itu tidak dihindari oleh pelaku meskipun hal itu tidak diinginkan oleh dirinya sendiri. Hal itu dilakukan oleh seseorang karena faktor-faktor dari luar dirinya.

Faktor-faktor dari luar dirinya atau batinnya itulah yang menyebabkan pembuat tindak oidana tidak dapat berbuat lain yang mengakibatkan kesalaahannya menjadi terhapus. Artinya, berkaitan dengan hal ini pembuat tindak pidana terdapat alasan penghapusan pidana, sehingga pertanggujawaban berkaitan dengan hal ini ditunggukan smapai dapat dipastikan ada tidaknya unsur alasan pemaaf dalam diri pelaku pembuat tindak pidana tersebut. Sekalipun pelaku pembuat tindak pidana dapat dicela namun celaan tersebut tidak dapat dilanjutkan kepadanaya karena pembuat tindak pidana tidak dapat berbuat lain selain melakukan tindak pidana tersebut

Alasan pembenar dalam doktrin hukum pidana adalah suatu alasan yang menghapus sifat melawan hukumnya suatu perbuatan. Alasan pembenar dan alasan pemaaf ini dibedakan karena keduanya memiliki fungsi yang berbeda. Adanya perbedaan ini karena alasan pembenar adalah suatu alasan "pembenaran" atas suatu tindak pidana yang melawan hukum sedangkan alasan pemaaf berujung pada pemaafan terhadap seseorang sekalipun telah melakukan pelanggar hukum atas tindak pidana yang telah diperbuat.

SIMPULAN

Berdasarkan hasil penelitian yang telah dijabarkan sebelumnya, maka terdapat kesimpulan dalam penelitian ini sebagai berikut:

1 Pengaturan perbuatan hacking di Indonesia diatur dalam Undang-Undang Nomor 19 tahun 2016 tentang tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Hacking dikategorikan sebagai salah satu kejahatan di dunia maya karena hacker merupakan orang yang menguasai pemrograman yang dapat melakukan hacking atau peretasan sistem keamanan pada komputer atau jaringan dengan tujuan tertentu. Pasal 30 jo. Pasal 46 UU ITE dijadikan sebagai dasar bagi Jaksa untuk merumuskan dakwaan dan tuntutan terhadap pelaku hacking.
2 Hambatan dalam penanggulangan terhadap hacking yang dengan sengaja dan tanpa hak atau melawan hukum dalam tindak pidana cyber crime adalah pada aspek barang bukti digital mudah dihilangkan jika tidak ditangani dengan tepat waktu, terbatasnya sarana dan prasarana yang ada, dan luasnya yurisdiksi

yang ada, pelaku menggunakan akun atau identitas palsu, pelaku menggunakan fasilitas umum dalam melakukan tindak pidana cyber crime. keberadaan para saksi tidak di tempat yang sama dengan korban dan pelaku Upaya mengatasinya adalah sosialisasi UU ITE, peningkatan kesadaran masyarakat dalam menggunakan sosial media serta pemberatan sanksi pidana.

3 Pertanggungjawaban pidana pelaku hacking berdasarkan putusan Pengadilan Negeri Pelaihari Nomor 9/Pid.Sus/2021/PN.Pli bahwa majelis hakim tidak menemukan hal-hal yang dapat menghapuskan pertanggungjawaban pidana, baik sebagai alasan pembenar yang dapat menghilangkan sifat melawan hukum dari perbuatan terdakwa maupun alasan pemaaf yang dapat menghapuskan kesalahan terdakwa, maka dengan demikian terdakwa harus mempertanggungjawabkan perbuatan pidana yang telah dilakukannya. Demikian juga pada putusan Pengadilan Negeri Cikarang Nomor 515/Pid.Sus/2021/PN.Ckr bahwa majelis hakim tidak menemukan hal-hal yang dapat menghapuskan pertanggungjawaban pidana, baik sebagai alasan pembenar dan atau alasan pemaaf, maka Terdakwa harus mempertanggungjawabkan perbuatannya.

DAFTAR PUSTAKA

Amrani Hanafi. dan Mahrus Ali. 2017 Sisitem Pertanggung Jawaban Pidana, Rajawali Pers, Jakarta, 2015.Andi Zainal Abidin, Asas-Asas Hukum Pidana Bagian Pertama, Alumni, Bandung.

Andi. 2018. Kamus Lengkap Dunia Komputer, Wahana Komputer, Yogyakarta.

Arief, Barda Nawawi. 2016. Tindak Pidana Mayantara dan Perkembangan Kajian Cyber Crime di Indonesia, Rajawali Pers. Jakarta.

Arisandi, Yogi Oktafian. "Penegakan Hukum terhadap Cyber Crime Hacker", Indonesian Journal of Criminal Law and Criminology (IJCLC), Vol. 1, No. 2.

DM, Mohd. Yusuf, Suryadi, Robi Hami. 2022. "Analisis Kejahatan Hacking Sebagai Bentuk Cyber Crime Dalam Sistem Hukum yang berlaku di Indonesia", Jurnal Pendidikan dan Konseling, Volume 4 Nomor 6 Tahun 2022.

Gatra, Sandro. 2023. "Pasal-Pasal Cyber Crime UU ITE Dicabut oleh UU KUHP Baru". diunduh melalui https://nasional.kompas.com. diakses Senin, 04 September 2023.

Hamzah, Andi. 2018. Hukum Pidana yang berkaitan dengan komputer. Sinar Grafika Offset. Jakarta.

Hasil wawancara dengan Kompol Chandra Yudha, Penyidik Unit 3 Subdit Indag Ditreskrimsus Kepolisian Daerah Sumatera Utara, Rabu 13 November 2024 Pukul 10.00 Wib.

Hukum Online. "Jerat Hukum Peretasan oleh Hacker". diunduh melalui https://www.hukumonline.com. diakses Senin, 04 September 2023.

Magdalena, Merry dan Maswigrantoro Roes Setyadi. 2017. Cyberlaw Tidak Perlu Takut. Andi. Yogyakarta.

Maskun. 2018. Kejahatan Cyber Crime, Kencana. Jakarta.

Mohode, Noldy. 2020. "Kejahatan Hacking Melalui Jaringan Internet Di Indonesia",.Jurnal Ilmu Hukum, Vol.1 No. 1.

Nugroho, I.Y. 2020. "Sanksi Hukum Kejahatan Peretasan Website Presiden Republik Indonesia". Jurnal Hukum Dan Perundangan Islam,hlm, Vol.1 Nomor 1.

Subagto, Agus. 2019. "Sinergi Dalam Menghadapi Ancaman Cyber Warfare Synergy in Facing of Cyber Warfare Threat", Jurnal Pertahanan Volume 5 Nomor 1.

Suhariyanto, Budi. 2021. Tindak Pidana

Teknologi Informasi (Cybercrime), RajaGrafindo Persada. Jakarta.

Suseno, Sigit dan Syarif A. Barmani. 2020. "Kebijakan Pengaturan Carding Dalam Hukum Pidana di Indonesia," Junal Sosiohumaniora, Vol 1 Nomor 6.

Sutrisno, Nandang, 2020. "Cyber Law: Problem dan Prospek Pengaturan Aktivitas Internet". Jurnal Hukum No. 16. Vo1.8.

Taidi, F. Yerusalem R. Pembuktian Dalam Penegakan Hukum Tindak Pidana Teknologi Informasi. Lex Crimen Vol. II/No. 6/Oktober/2019.

Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

Wahid, Abdul dan Mohammad Labib. 2015. Kejahtan Mayaantara (Cybercrime, Refika Aditama. Bandung.

Wahyudi, Dheny. 2019. "Perlindungan Hukum Terhadap Korban Kejahatan Cyber Crime Di Indonesia". Jurnal Ilmu Hukum Vol. 4, No. 1.

Widodo. 2021. Aspek Hukum Pidana Kejahatan Mayantara. Aswaja Pressindo. Yogyakarta. 2017.Budi Suhariyanto. Tindak Pidana Teknologi Informasi (Cybercrime), RajaGrafindo Persada, Jakarta.