Jurnal Pendidikan dan Konseling
Volume 4 Nomor 6 Tahun 2022
E-ISSN: 2685-936X dan P-ISSN: 2685-9351
Universitas Pahlawan Tuanku Tambusai

Analisis Kejahatan *Hacking* Sebagai Bentuk *Cyber Crime* Dalam Sistem Hukum yang berlaku di Indonesia

MOHD. Yusuf DM[1], Suryadi[2], Robi Hamid[3]
[1,2,3] Ilmu Hukum, Fakultas Hukum, Universitas Lancang Kuning
Email: boyke457@gmail.com

Abstrak

Perkembangan teknologi informasi menimbulkan dampak positif dan dampak negatif. Dampak positifnya adalah dapat menambah trend perkembangan teknologi dunia dengan segala bentuk kreatifitas manusia. Sedangkan dampak negatifnya adalah kemajuan teknologi informasi tersebut telah menciptakan kemungkinan-kemungkinan baru dalam melakukan kejahatan, khususnya kejahatan penyalahgunaan teknologi informasi, yang sering disebut *cyber crime* Salah satu bentuk *Cyber Crime* ialah kejahatan *Hacking.* Kejahatan *Hacking* merupakan kegiatan penyusupan atau menerobos program komputer milik orang. Metode penelitian yang digunakan dalam penelitian ini adalah metode penelitian hukum normatif yang dilakukan dengan penelitian kepustakaan. Tujuan dari penelitian ini adalah untuk memeberikan solusi bahwa dalam menangani tindak pidana *Hacking,* diperlukan penegakan Hukum yang kuat untuk melindungi hak korban kejahatan *Hacking* agar dapat mengurangi kasus *Cyber Crime* di Indonesia.
Kata Kunci: *Cyber Crime, Hacking,* Hukum.

Abstract

The development of information technology has both positive and negative impacts. The positive impact is that it can add to the trend of world technology development with all forms of human creativity. While the negative impact is that advances in information technology have created new possibilities in committing crimes, especially the crime of misuse of information technology, which is often called cyber crime. One form of Cyber Crime is the crime of Hacking. Hacking crime is an activity of infiltrating or breaking through someone's computer program. The research method used in this study is a normative legal research method carried out by library research. The purpose of this study is to provide a solution that in dealing with hacking crimes, strong law enforcement is needed to protect the rights of victims of hacking crimes in order to reduce cyber crime cases in Indonesian.
Keywords: *Cyber Crime, Hacking, Law.*

PENDAHULUAN

Dalam bidang teknologi, internet adalah sebuah mahakarya yang sangat luar biasa karena dapat mempertemukan antara individu dengan komponen mesin dalam sebuah jaringan vitual sehingga menghasilkan suatu dunia baru yang disebut dengan dunia maya (*cyberspace*), dimana manusia dapat memerintahkan kepada komponen mesin untuk melakukan sesuatu yang kemudian komponen mesin menginformasikan apa yang telah diinformasikan ke dalam bentuk audio-visual.

Seiring dengan perkembangan internet yang begitu pesatnya, disisi lain juga diikuti dengan timbulnya permasalahan baru yang sukar untuk dipecahkan. Selain itu juga internet telah membawa perubahan besar terhadap perilaku dan pola hidup daripada individu yang cenderung untuk memilih

melakukan segala sesuatu serba cepat dan serta dapat berinteraksi dengan individu yang lainnya tanpa harus bertatap muka secara langsung. Salah satu hal yang meresahkan para pengguna internet adalah semakin maraknya aktivitas hacking yang dilakukan oleh seorang atau sekelompok orang dengan maksud dan tujuan tertentu. Proses Hacking ini sendiri sangat bervariasi tergantung teknik, keahlian serta perangkat lunak (*software*) dan perangkat keras (*hardware*) yang digunakan.

Pesatnya perkembangan teknologi informasi, memang dirasakan banyak dampak positif dan dampak negatifnya. Dampak positifnya adalah dapat menambah trend perkembangan teknologi dunia dengan segala bentuk kreatifitas manusia. Sedangkan dampak negatifnya adalah kemajuan teknologi informasi tersebut telah menciptakan kemungkinan-kemungkinan baru dalam melakukan kejahatan, khususnya kejahatan penyalahgunaan teknologi informasi, yang sering disebut *cyber crime* yaitu kejahatan yang dilakukan melalui jaringan internet.

Menurut Heru (dalam Sugiaryo, 2011:158) Secara umum, *Cyber Crime* dapat dikategorikan menjadi dua kelompok yaitu kejahatan biasa yang menggunakan teknologi informasi sebagai alat bantunya dan kejahatan yang muncul setelah adanya internet, dimana sistem komputer sebagai korbannya.[1] *Cyber Crime* merupakan bentuk-bentuk kejahatan yang timbul karena pemanfaatan teknologi internet.[2] Berdasarkan beberapa pendapat diatas, dapat disimpulan bahwa *Cyber Crime* adalah sebuah tindakan yang memanfaatkan komputer atau internet sebagai alat bantu ataupun sebagai sasaran kejahatan.

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.[3]

Perkembangan hacking di Indonesia bukanlah ilusi akan tetapi merupakan sebuah fakta sosial yang semakin meningkat dari tahun ke tahun bahkan ada yang menyatakan bahwa perkembangan hacking di Indonesia telah meningkat secara signifikan sejak tahun 1998 seiring dengan meningkatnya jumlah pengguna internet di Indonesia, sehingga diperlukan perlindungan hukum yang kuat bagi korban-korban pelaku kejahatan hacking tersebut.[1]

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*.[4]

Hacker berarti seorang *programmer* yang pintar / cerdik dalam bidang pemrograman yang tidak ada kaitannya dengan bidang keamanan komputer. *Hacker* dapat juga berarti sebagai penghargaan kepada orang-orang yang memiliki kemampuan dan pengetahuan yang lebih dari rata-rata orang biasa di berbagai bidang komputer. Seorang *hacker* yang baik, jika menemukan hal-hal seperti itu akan memberitahu sistem *administrator*, bahwa sistem komputer yang dimasukinya telah terdapat kelemahan yang mungkin berbahaya bagi sistem komputer tersebut. Jika hasil dari *hacking* ini dimanfaatkan oleh orang yang tidak baik, maka tindakan tersebut digolongkan ke dalam *Cyber Crime*.[4]

METODE

Jenis penelitian ini adalah penelitian kepustakaan (*library research*). Penelitian kepustakaan adalah penelitian yang dilaksanakan dengan menggunakan literature (kepustakaan), baik berupa buku, catatan, maupun laporan hasil penelitian terdahulu. Penelitian ini termasuk penelitian kepustakaan karena didasarkan pada literature baik berupa buku, catatan, maupun laporan hasil penelitian terdahulu. Sehubungan dengan jenis penelitian yang digunakan yaitu penelitian hukum normatif, maka pendekatan yang digunakan adalah Pendekatan PerundangUndangan (Statute Approach).

Sumber data yang digunakan penelitian ini adalah data sekunder. Data sekunder adalah data yang diperoleh atau dikumpulkan oleh orang yang melakukan penelitian dari sumber-sumber yang telah ada melalui bahan-bahan kepustakaan (*library*). Teknik pengumpulan data yang digunakan adalah Studi Kepustakaan. Dalam studi kepustakaan penulis menggunakan teknik pengumpulan data dengan cara membaca, mencatat dan mempelajari bahan hukum tersebut diatas yang berkaitan dengan pengaturan *hacking* dan penanggulangnya.

HASIL DAN PEMBAHASAN

Faktor – Faktor Penyebab Terjadinya *Hacking*

1. Faktor internal
   a. Niat pelaku

      Niat merupakan awal dari suatu perbuatan, dalam melakukan tindak pidana pencurian niat dari pelaku penting dalam faktor terjadinya pencurian. Pelaku sebelum melakukan pencurian biasanya sudah berniat dan merencanakan bagaimana akan melakukan perbuatannya.

   b. Moral dan Pendidikan

      Moral disini berarti tingkat kesadaran akan norma-norma yang berlaku di dalam masyarakat. Kesadaran hukum seseorang merupakan salah satu faktor internal yang dapat menentukan apakah pelaku dapat melakukan perbuatan yang melanggar notmanorma di masyarakat. Tingkat pendidikan seseorang juga menentukan seseorang dapat melakukan tindk pidana pencurian. Karena kebanyakan dri pelaku pencurian memiliki tingkat pendidikan yang rendah.

2. Faktor eksternal
   a. Lingkungan tempat tinggal

      Lingkungan tempat tinggal pelaku kejahatan biasanya merupakan lingkungan atau daerahdaerah yang pergaulan sosialnya rendah, rendahnya moral penduduk dan seringnya norma-norma sosial dilanggar dan tidak ditaati lagi.

   b. Keadaan ekonomi

      Keadaan ekonomi dari pelaku tindak pidana pencurian kerap kali menjadi faktor yang melatarbelakangi seseorang melakukan tindak pidana pencurian. Karena desakan ekonomi yang menghimpit, yaitu harus memenuhi kebutuhan keluarga, membeli sandang maupun papan, atau ada keluarga yang sedang sakit, maka seseorang dapat berbuat nekat dengan melakukan tindak pidana pencurian.

   c. Perkembangan global

      Perkembangan global memiliki dampak positif bagi kemajuan suatu negara, sedangkan bagi individu perkembangan global merupakan suatu sarana untuk menunjukkan bahwa dia adalah seseorang yang mampu memenuhi kebutuhan hidupnya dalam masa perkembangan global tersebut. Selain itu seseorang yang memiliki harta yang lebih dipandang sebagai orang

yang sukses, hal ini tentunya membuat setiap orang dalam masyarkat bersaing satu sama lainnya untuk menunjukkan bahwa dirinyaah yang paling unggul.[5]

Cara Kerja *Hacking*

1. *Foot printing* merupakan Proses mencari informasi tentang korban sebanyak-banyaknya. Dilakukan dengan data-data di internet, koran dan lain-lain.
2. *Scanning* merupakan Proses lanjutan dengan menganalisa service yang dijalankan di internet. Biasanya dilakukan dengan ping, nmap dan lain-lain.
3. *Enumeration* merupakan Proses lajutan dengan mencoba koneksi ke mesin target.
4. *Gaining Access* merupakan Percobaan pengambil alihan ke target berdasarkan informasi yang telah didapatkan.
5. *Escalating Privilege* merupakan Meningkatkan hak akses jika telah berhasil masuk ke dalam sistem.
6. *Covering Tracks* merupakan Proses menutupi jejak dengan menghapus segala macam *log* agar tidak terlacak.
7. *Denial of Service* merupakan Setelah segala macam cara gagal dilakukan, biasanya dilakukan serangan terakhir yaitu membanjiri target dengan data sehingga mesian tidak dapat berfungsi. Cara ini biasanya setelah hacker putus asa dalam usaha pengambil alihan mesin.[6]

Cara Mencegah Terjadinya Kejahatan *Hacking*

1. Memasang Proteksi

   Dalam menjaga privasi informasi, memasang proteksi merupakan hal utama. Proteksi ini dapat berupa antivirus maupun *firewall*. Antivirus digunakan untuk mendeteksi program-program yang dapat merusak sistem-sistem dan data yang ada di dalam komputer, seperti Virus.
2. Memantau serangan Seringkali serangan dari penyusup (*hacker*) dilakukan tanpa sepengetahuan dari *administrator* (*network security*), maka perlu digunakan sistem pemantau terhadap serangan tersebut. Sistem ini dinamakan *Intruder Detection System* (IDS). secara langsung sistem ini memberikan tanda peringatan kepada administrator berupa alarm, sinyal bahkan pesan e-mail jika adanya serangan. Salah satu contoh IDS yaitu tcpdump untuk menganalisis paket apa saja yang lewat.
3. Mengatur keamanan program Saat membuat sistem keamanan jaringan komputer seringkali *administrator* (*network security*) tidak memperhatikan hal-hal kecil yang dapat dimanfaatkan oleh penyusup (*hacker*), nantinya akan menjadi masalah besar. Oleh karena itu, diperlukan keteliltian dalam membuat suatu program, misalnya pemilihan karakter-karakter khusus yang digunakan untuk pemrograman serta ketelitian perhitungan algoritma dalam pembuatam program.
4. Menutup service yang tidak diperlukan Pada umumnya suatu Operation System (OS) terdapat layanan (service) yang diikutsertakan dan dijalankan secara umum (default). Contohnya seperti Telnet, memlaui Telnet ini seseorang dapat berhubungan dengan sedemikian banyak komputer di tempat lain di internet dan secara interaktif dapat mencari berbagai data, file, software dan informasi lainnya. Namun dibalik kegunaannya tersebut tanpa disadari layanan ini dapat dimanfaaatkan oleh penyusup (hacker) untuk melakukan hacking terhadap suatu web, misalnya merubah tampilan halaman situs. Oleh karena itu, jika tidak diperlukan sebaiknya layanan tersebut ditutup.
5. Menggunakan *Publick-Key Cryptogrphy* (Kunci Umum Pengacakan) Selain sistem, data-data penting yang ada di dalam komputer perlu dijamin keamanannya dengan menggunakan *Publick-Key Cryptogrphy* (Kunci Umum Pengacakan). Dengan bantuan program ini otomstis informasi yang

di kirimkan maupun diterima akan diacak (*encrypt*)dan jika ingin membukannya (*decrypt*) diperlukan kata sandi (*password*) yang sebelumnya telah disepakati bersama. kunci umum pengackan ini dilakukan dengan menggunakan *Publick Key Insfrastructures* yang dimiliki oleh lembaga penyelenggaranyauntuk mendukung *Digital Signature* (tanda tangan elektronik).

6. Melakukan *Backup* Mengingat perkembangan kejahatan *hacking* yang semakin kompleks dan informasi sebagai sasaran utamanya maka dengan melakukan *backup* secara berkala merupakan suatu alternatif yang sangat diperlukan karena jika penyusup (*hacker*) telah menaklukkan sistem pengamanannya maka selanjutnya yang menjadi sasaran adalah data-data di dalam komputer korban, jika sudah disalin maka ada kemungkinan data-data asli yang ada di dalam komputer korban tersebut akan dirusak atau dimanipulasi sehingga tidak dapat digunakan hal itu dimaksudkan untuk meghilangkan jejak. [3]

Sistem Hukum yang berlaku di Indonesia mengenai Kejahatan *Hacking*

Terdapat sebagian hukum positif yang legal biasa serta bisa dikenakan untuk para pelaksana *cyber crime* paling utama buat kasuskasus yang memakai komputer selaku prasarana, antara lain:

1. Kitab Undang Undang Hukum Pidana Dalam usaha menanggulangi kasus- kasus yang terjalin para pemeriksa melaksanakan kemiripan ataupun ibarat serta persamaaan kepada Pasal- Pasal yang terdapat dalam KUHP. Pasal-Pasal didalam KUHP umumnya dipakai lebih dari satu Artikel sebab mengaitkan sebagian aksi sekalian Pasal- Pasal yang bisa dikenakan dalam KUHP pada *cyber crime* antara lain :
2. Pasal 362 KUHP yang dikenakan buat permasalahan *hacking* dimana pelakon mencuri no kartu angsuran kepunyaan orang lain meski tidak dengan cara raga sebab nomor kartunya saja yang didapat dengan memakai aplikasi card generator di Internet buat melaksanakan bisnis di *e-commerce*.
3. Pasal 378 KUHP bisa dikenakan buat pembohongan dengan seakan olah menawarkan serta menjual sesuatu produk ataupun benda dengan memasang promosi di salah satu web alhasil orang terpikat buat membelinya kemudian mengirimkan duit pada pemasang promosi. Namun, pada faktanya, benda itu tidak terdapat. Perihal itu dikenal sehabis duit dikirimkan serta benda yang dipesankan tidak tiba alhasil konsumen itu jadi terkecoh.
4. Pasal 335 KUHP bisa dikenakan buat permasalahan penggertakan serta eksploitasi yang dicoba lewat e-mail yang dikirimkan oleh pelakon buat memforsir korban melaksanakan suatu cocok dengan apa yang di idamkan oleh pelakon serta bila tidak dilaksanakan hendak bawa akibat yang mematikan. Perihal ini umumnya dicoba sebab pelakon umumnya mengenali rahasia korban.
5. Pasal 311 KUHP bisa dikenakan buat permasalahan kontaminasi julukan bagus dengan memakai alat Internet. Modusnya merupakan pelakon mengedarkan e-mail pada sahabat korban mengenai sesuatu narasi yang tidak betul ataupun mengirimkan e-mail ke sesuatu mailing list alhasil banyak orang mengenali narasi itu.
6. Artikel 303 KUHP bisa dikenakan buat memerangkap game gambling yang dicoba dengan cara online di Internet dengan eksekutor dari Indonesia.
7. Pasal 282 KUHP bisa dikenakan buat penyebaran pornografi ataupun web porno yang banyak tersebar serta gampang diakses di Internet. Meski berbicara Indonesia, amat susah sekali buat menangani pelakunya sebab mereka melaksanakan registrasi daerah itu diluar negara dimana pornografi yang menunjukkan orang berusia bukan ialah perihal yang bawah tangan.
8. Pasal 282 serta 311 KUHP bisa dikenakan buat permasalahan penyebaran gambar ataupun film individu seorang yang cabul di internet, misalnya permasalahan Sukma Ayu- Bjah.

9. Pasal serta 262 KUHP bisa dikenakan pada permasalahan *hacking*, sebab pelakon melaksanakan pembohongan seakan mau membeli sesuatu benda serta melunasi dengan kartu kreditnya yang no kartu kreditnya ialah jarahan.
10. Pasal 406 KUHP bisa dikenakan pada permasalahan deface ataupun hacking yang membuat sistem kepunyaan orang lain, semacam web ataupun program jadi tidak berperan ataupun bisa dipakai begitu juga mestinya.
11. Undang-Undang No. 19 tahun 2016 tentang Informasi dan Transaksi Elektronik. UU ITE dipersepsikan selaku cyberlaw di Indonesia, yang diharapkan dapat menata seluruh hal bumi Internet (siber), tercantum didalamnya berikan punishment kepada pelaksana *Cyber Crime*. *Cyber Crime* dideteksi dari 2 ujung penglihatan:
    a. Kesalahan yang Memakai Teknologi Data Selaku Sarana: Pemalsuan, Pornografi, Manipulasi atau Perampokan Kartu Angsuran, Pembohongan Melalui Email (Fraud), Email Spam, Pertaruhan Online, Perampokan Account Internet, Terorisme, Rumor Sara, Web Yang Menyesatkan, dsb.
    b. Kesalahan yang Menghasilkan Sistem Teknologi Data Selaku Target: Perampokan Informasi Individu, Pembuatan atau Penyebaran Virus Pc, Pembobolan atau Pembajakan Situs, C*yberwar*, *Denial of Service (DOS)*, Kesalahan Berkaitan Dengan Julukan Daerah, dsb.[6]

SIMPULAN

Berdasarkan pembahasan di atas dapat disimpulkan bahwa Semakin meningkatnya Teknologi Informasi semakin banyak juga dampak positif dan negatifnya. Dampak positif yaitu menambah trend perkembangan teknologi dunia dengan segala bentuk kreatifitas manusia. Selain itu dampak negatifnya dapat menyebabkan munculnya kejahatan yang disebut dengan *Cyber Crime* atau kejahatan melalui jaringan Internet. *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*. Oleh karena itu, dalam penanggulangannya dibutuhkan pengaturan hukum yang berkaitan dengan pemanfaatan teknologi tersebut, selain itu juga diperlukan adanya kerja sama dengan lembaga khusus untuk memberikan informasi tentang *Cyber Crime*, melakukan sosialisasi secara intensif kepada masyarakat, serta melakukan riset-riset khusus dalam penanggulangan *Cyber Crime*.

DAFTAR PUSTAKA

Sugiaryo, "Penegakan Hukum Kejahatan Hacking Dalam Prespesktif Kebijakan Hukum Pidana Di Indonesia," *Jurnal Ilmu Hukum REFLEKSI HUKUM*. pp. 171–172, 2011.

D. Z. Abidin, "Kejahatan dalam Teknologi Informasi dan Komunikasi," *J. Ilm. Media Process.*, vol. 10, no. 2, pp. 1–8, 2015, [Online]. Available: http://ejournal.stikom-db.ac.id/index.php/processor/article/view/107/105

D. Rofifah, "Kejahatan Hacking Melalui Jaringan Internet Di Indonesia," *Pap. Knowl. . Towar. a Media Hist. Doc.*, pp. 12–26, 2020.

H. Murti, "Cybercrime," vol. X, no. 1, pp. 37–40, 2005, [Online]. Available: https://www.unisbank.ac.id/ojs/index.php/fti1/article/view/2214?PageSpeed=noscript

R. P. Saputra, "PERKEMBANGAN TINDAK PIDANA PENCURIAN DI INDONESIA," vol. 2, pp. 5–10, 2019.

H. S. Arnold Bagas Kurniawan, "Perlindungan Hukum Kepada Pengguna Elektronik Banking Atas Kejahatan Carding Ditinjau Dari Undang-Undang Informasi dan Transaksi Elektronik," vol. 5, no. 01, pp. 65–87, 1945.