

BAB I

PENDAHULUAN

1.1 Latar Belakang Permasalahan

Kemajuan teknologi dimasa sekarang ini memberikan banyak manfaat dan kemudahan bagi umat manusia, namun kemajuan teknologi ini tidak sekedar membawa nilai positif saja, tetapi juga membawa nilai negatif yang sama banyak dengan manfaatnya, dari sinilah dapat kita lihat bahwa semakin berkembangnya teknologi informasi dan juga komunikasi akan berbanding lurus dengan semakin berkembangnya kejahatan.

adanya internet memberikan kemudahan bagi kita untuk melakukan komunikasi sosial yang biasa kita sebut '*social networking*' adapun beberapa contoh website seperti Facebook, Twitter, Whats App, dan masih banyak lagi.

Adanya kemudahan dalam pertukaran dan keterbukaan informasi memberikan jalan pada siapa saja untuk dapat mengakses informasi dengan bebas, bahkan karena kebebasan tersebut oleh para pihak yang tidak bertanggungjawab sering disalahgunakan untuk berbuat suatu tindakan kriminal, seperti pengatas namaan untuk disalahgunakan, plagiasi, dan juga penyebaran informasi yang salah atau tidak benar.

Terkait dengan hal tersebut, sekarang sering kita mendengar adanya kata Hacking, atau pun Hack, yang merupakan salah satu bentuk kejahatan

berupa pembobolan informasi, diketahui bahwa kejahatan ini tidak mengenal batas wilayah (*borderless*) dan waktu kejadian karena korban dan pelaku sering berada di negara yang berbeda. Indonesia merupakan salah satu negara yang menyadari akan bahaya tersebut, sehingga disepakati bahwa kejahatan IT/*Cybercrime* memiliki karakter yang berbeda dengan tindak pidana umum baik dari segi korban, pelaku, modus operandi dan tempat kejadian perkara sehingga butuh penanganan serta pengaturan khusus diluar KUHP (Kitab Undang-undang Hukum Pidana). Para penjahat *cyber* memanfaatkan jaringan pertemanan melalui jejaring sosial, karena sebagian besar pengguna jejaring sosial percaya begitu saja atas *link* atau konten yang mereka terima dari sesama teman tanpa melakukan konfirmasi atau pengecekan lebih lanjut, pengguna jejaring sosial tersebut melakukan akses langsung ke web atau situs yang mereka terima bahkan tanpa disadari di dalamnya berisi program jahat.¹

Indonesia adalah negara hukum seperti yang tertuang dalam konstitusi, sebagai sebuah negara hukum tentunya negara wajib melindungi setiap warga negaranya dari setiap perbuatan yang dapat merugikan apalagi perbuatan tersebut dapat merusak tatanan kehidupan berbangsa dan bernegara. Seperti halnya kejahatan yang terjadi di dunia maya atau biasa disebut dengan *cybercrime*. Kejahatan yang tidak mengenal ruang dan waktu ini mengalami perkembangan yang pesat akhir-akhir ini, kecanggihan teknologi yang disalah gunakan oleh oknum yang tidak bertanggung jawab demi keuntungan pribadi

¹ Dista amalia arifah, kasus cybercrime di Indonesia, jurnal bisnis dan ekonomi (JBE) september 2011, hal. 185-195

yang menyebabkan negara-negara berkembang kesulitan untuk menindak pelaku kejahatan komputer khususnya pihak kepolisian, disamping dibutuhkan suatu perangkat aturan yang mengatur tentang penyalahgunaan informasi ini juga dibutuhkan sumber daya manusia dan sarana dan prasarana yang mendukung.²

Kejahatan di dunia maya sangat memprihatinkan dan harus mendapatkan perhatian yang serius dari pemerintah, hal ini dapat kita lihat bahwa pada tahun 2004 Negara Indonesia menduduki peringkat pertama dalam kasus *cybercrime* bahkan dinilai lebih berat dibandingkan negara lain, termasuk Amerika Serikat. Meski Indonesia menduduki peringkat pertama dalam *cybercrime* pada tahun tersebut, akan tetapi jumlah kasus yang diputus oleh pengadilan tidaklah banyak. Dalam hal ini angka *dark number* cukup besar dan data yang dihimpun oleh Polri juga bukan data yang berasal dari investigasi Polri, sebagian besar data tersebut berupa laporan dari para korban. Selanjutnya Polda Metro Jaya mencatat total kerugian masyarakat akibat kejahatan cyber berdasarkan laporan polisi yang masuk ke Polda Metro Jaya tahun 2011 kerugian masyarakat mencapai 4 milyar dan pada tahun 2012 meningkat mencapai 5 milyar rupiah. Pada tahun 2012 berdasarkan hasil survei yang diselenggarakan oleh Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) mengungkapkan bahwa jumlah pengguna internet mencapai 63 juta orang atau 24,23 persen dari populasi negeri ini, dalam hal jumlah pengguna internet Indonesia menempati urutan

² Dheny Wahyudi, perlindungan hukum terhadap korban kejahatan ciber crime di indonesia, jurnal ilmu hukum

kedelapan di seluruh dunia. Oleh karena jumlah pengguna teknologi yang begitu banyak tentunya hal ini rentan untuk terjadinya suatu tindak pidana khususnya kejahatan di dunia maya.³

Biasanya *hacker* menggunakan *tool-tool* yang sudah ada di internet. *Tool* tersebut kemudian dijalankan untuk menyerang sistem computer. *Hacker* berpengalaman membuat *script* atau program sendiri untuk melakukan *hacking*, yang menjadi incaran sasaran yaitu:

1. Database kartu kredit
2. Database account bank
3. Database informasi pelanggan
4. Pembelian barang dengan kartu kredit palsu atau kartu kredit orang lain yang bukan merupakan hak kita (*carding*)
5. Mengacaukan sistem

Hacker tersebut dapat menjalankan aksinya melalui Internet Relay Chat (IRC), Voice over IP (VoIP), ICQ, Online forums, dan Encryption. Dalam menjalankan aksinya hacker menggunakan tahapan sebagai berikut:

a. *Footprinting*

Suatu tahap mencari informasi secara umum terhadap target

b. *Enumeration*

Telaah intensif terhadap sistem, mencari *user account* yang absah, resource jaringan dan aplikasi yang sedang berjalan pada sistem.

c. *Gaining Access*

³*Ibid.*

Mendapatkan data lebih banyak lagi untuk mulai mencoba mengakses sasaran. Meliputi mengintip dan merampas password, menebak password, serta melakukan *buffer overflow*.

d. *Escalating Privilege*

Dalam tahap ini diusahakan mendapat *privilege* admin jaringan dengan *password cracking* atau melakukan eksploitasi.

e. *Pilfering*

Proses pengumpulan informasi dimulai lagi untuk mengidentifikasi mekanisme untuk mendapatkan akses ke trusted system. Mencakup *evaluasi trust* dan pencarian clear text password di registry, config file, dan user data.

f. *Covering Tracks*

Ketika kontrol penuh terhadap sistem diperoleh, maka menutup jejak menjadi prioritas. Meliputi membersihkan *network log* dan penggunaan *hide tool* seperti macam-macam *rootkit* dan *filestreaming*. Pintu belakang diciptakan pada berbagai bagian dari sistem untuk memudahkan masuk kembali ke sistem ini dengan cara membentuk *user account* palsu, menjadwalkan *batch job*, mengubah *startupfile*, menanamkan servis pengendali jarak jauh serta *monitoring system*.

g. *Denial of Service*

Bila semua usaha di atas gagal, penyerang dapat melumpuhkan sasaran sebagai usaha terakhir. Dengan membanjiri system target meliputi

SYNflood, teknik-teknik ICMP, Supernuke, land/latierra, teardrop, bonk, newtear, trino, smurf, dan lain-lain.

Dengan metodologi seperti ini, *hacker* melakukan penyerangan dengan berbagai tehnik seperti *exploit* (eksploitasi langsung ke sistem), *spoofing* (penyamaran), *sniffing* (penangkapan data/capture data), dan *social engineering* (rekayasa sosial).⁴

Hukum yang salah satu fungsinya menjamin kelancaran proses pembangunan nasional sekaligus mengamankan hasil-hasil yang telah dicapai harus dapat melindungi hak para pemakai jasa internet sekaligus menindak tegas para pelaku *Cybercrime*. Pemberantasan tindak kejahatan *Cybercrime* diperlukan langkah-langkah yang kompleks, terintegrasi serta berkesinambungan dari banyak pihak, tidak hanya tugas penegak hukum semata.⁵ Keutuhan Negara Kesatuan Republik Indonesia, dengan berasaskan pada Undang Undang Dasar Republik Indonesia 1945, akhirnya melahirkan Undang Undang nomor.11 Tahun 2008, dan saat ini telah dirubah menjadi Undang Undang nomor.19 Tahun 2016.

1.2 Rumusan Permasalahan

Rumusan permasalahan hukum yang dapat disusun berdasarkan latar belakang yang telah diuraikan adalah sebagai berikut:

⁴ Dista Amalia Arifah, "*Kasus Ciber Crime Di Indonesia*", (jurnal bisnis dan ekonomi, 2011), Vol.18 No. 2

⁵Dista amalia arifah, kasus cybercrime di Indonesia, jurnal bisnis dan ekonomi (JBE) september 2011, hal. 185-195

1. Apakah peraturan perundang-undangan yang berlaku saat ini telah cukup memberikan perlindungan kepada pengguna internet dari tindak pencurian data pribadi?
2. Bagaimana bentuk perlindungan yang diberikan hukum kepada pengguna internet dari tindak pencurian data pribadi?

1.3 Tujuan

Dari beberapa permasalahan di atas, maka tujuan daripadanya adalah sebagai berikut:

1. Mengetahui perlindungan yang diberikan oleh peraturan perundang-undangan kepada pengguna internet dari tindak pencurian data pribadi,
2. Mengetahui bentuk perlindungan yang diberikan kepada pengguna internet dari tindak pencurian data pribadi.

1.4 Kegunaan

Dari penelitian ini diharapkan dapat memberikan 2 (dua) kegunaan yaitu kegunaan dari segi teoritis dan kegunaan dari segi praktis.

1. Kegunaan teoritis, diharapkan hasil dari penelitian ini dapat membantu para akademisi dalam upaya pengkajian dan pengembangan ilmu hukum pidana
 - a. Memberikan masukan dan sumbangan pemikiran untuk pengembangan kebijakan penanggulangan tindak pidana pencurian data pribadi dengan internet, baik kebijakan legislatif maupun kebijakan aplikatif

- b. Melengkapi khasanah kajian yang berkaitan dengan “pidana dan pembedaan” terutama yang berkaitan dengan kebijakan legislatif dalam bidang yang berkaitan dengan pendidikan

2. Tujuan praktis

Penelitian ini diharapkan dapat:

- a. Memberi masukan kepada para pembuat kebijakan atau pembentuk Undang-Undang dalam rancangan kitab undang-undang hukum pidana (KUHP) maupun diluar KUHP yang sampai saat ini dirasa kurang dalam penanganan tindak kejahatan yang terkait dengan internet
- b. Memberikan wawasan kepada aparat penegak hukum dalam membantu tugasnya untuk menangani maupun menyelesaikan perkara pidana yang terkait dengan internet
- c. Memberikan masukan bagi pengguna internet dalam mengantisipasi adanya tindak kejahatan yang berkaitan dengan internet yang dapat berdampak pada diri sendiri maupun pada masyarakat luas.

1.5 Keaslian

Dalam penelitian Perlindungan Hukum Terhadap Tindak Pencurian Data Pribadi Melalui Internet Di Indonesia ini terdapat kesamaan tema dengan penelitian yang dilakukan oleh Hurriyatul Fikriyah konsentrasi kepidanaan islam fakultas syariah dan hukum di Uin Syarif hidayatullah jakarta pada tahun 2011 yang berjudul Tindak Pidana Pemalsuan Data Dalam Undang-undang No. 11 Tahun 2008 Tentang ITE dan Kajian Hukum islam. Tetapi berbeda pada

pokok bahasan dimana Penelitian Perlindungan Hukum Terhadap Tindak Pencurian Data Pribadi Melalui Internet Di Indonesia membahas tentang perlindungan hukum dari korban tindak pidana pencurian data pribadi di internet serta penegakan hukum yang dilakukan pemerintah dalam KUHP serta Undang-undang No 11 Tahun 2008 tentang ITE sedang penelitian Tindak pidana pemalsuan data dalam Undang-undang No 11 tahun 2011 tentang ITE dan kajian hukum islam lebih membahas tentang pelaku diantaranya sanksi hukum pidana serta sanksi yang diberikan hukum islam kepada pelaku pemalsuan data.

1.6 Metode Penelitian

1.6.1. Jenis penelitian

Jenis penelitian yang digunakan dalam penyusunan tugas akhir ini menggunakan metode penelitian hukum normatif. Metode penelitian hukum normatif atau metode penelitian hukum kepustakaan adalah metode atau cara yang dipergunakan di dalam penelitian hukum yang dilakukan dengan cara meneliti bahan pustaka yang ada.⁶ Tahapan pertama penelitian hukum normatif adalah penelitian yang yang ditujukan untuk mendapatkan hukum obyektif (norma hukum), yaitu dengan mengadakan penelitian terhadap masalah hukum. Tahapan

⁶Soerjono Soekanto dan Sri Mamudji, *Penelitian Hukum Normatif Suatu Tinjauan Singkat*, Cetakan ke-11. Jakarta, PT Raja Grafindo Persada, 2009, hal. 13-14.

kedua penelitian hukum normatif adalah penelitian yang ditujukan untuk mendapatkan hukum subjektif (hak dan kewajiban).⁷

1.6.2. Metode Pendekatan

Metode pendekatan yang digunakan adalah *Statuta Approach* (pendekatan Undang-Undang), dilakukan dengan menelaah semua undang-undang dan regulasi yang bersangkut paut dengan isu hukum yang sedang ditangani.⁸

1.6.3. Teknik Pengumpulan Data

Penelitian ini menggunakan metode penelitian hukum normatif dengan menggunakan pendekatan *statute approach* (pendekatan undang-undang). Jenis data yang dikumpulkan adalah data primer dimana bahan hukum primer merupakan bahan hukum yang bersifat autoritatif artinya yang mempunyai otoritas. Bahan hukum primer terdiri dari perundang-undangan, catatan-catatan resmi atau risalah dalam pembuatan perundang-undangan dan putusan-putusan hakim.⁹

Mengenai teknik pengumpulan data, menurut Ronny Hanitijo Sumitro, teknik pengumpulan data terdiri dari tiga (3) macam yaitu studi kepustakaan, pengamatan (observasi), wawancara (interview), dan menggunakan daftar pertanyaan (kuisisioner). Teknik pengumpulan data yang digunakan dalam skripsi ini adalah study pustaka (Literatur Study) dan studi dokumen.

⁷ Hardijan Rusli, “Metode Penelitian Hukum Normatif: Bagaimana?”, Law Review Fakultas Hukum Universitas Pelita Harapan, Volume V No. 3 Tahun 2006, hal. 50.

⁸ Peter mahmud marzuki, *Penelitian Hukum*, pt kharisma Putra Utama, 2005. Hal. 133

⁹ Peter mahmud marzuki, *Penelitian Hukum*, pt kharisma Putra Utama, 2005. Hal. 181

1.6.4. Metode Analisa

Dalam penelitian ini penulis menggunakan metode kualitatif dan diuraikan secara deskriptif analisis, analisis kualitatif ini dilakukan secara deskriptif karena penelitian ini tidak hanya bermaksud mengungkapkan atau menggambarkan data kebijakan hukum pidana sebagaimana adanya, tetapi juga bermaksud menggambarkan tentang kebijakan hukum pidana yang diharapkan dalam undang-undang yang akan datang.

