BAB I

PENDAHULUAN

A. Latar Belakang Masalah

Perkembangan kejahatan yang berkaitan dengan teknologi ini sering dikatakan sebagai bentuk kejahatan *cybercrime* (kejahatan dunia maya). Bentuk klasik dari kejahatan ini adalah seperti: *Joycomputing* (memakai komputer tanpa ijin), *hacking* (memasuki sistem jaringan komputer secara tidak sah), *The Trojan horse* (memanipulasi program komputer), *Data Leakage* (pembocoran data), *Data Diddling* (manipulasi data komputer) dan Perusakan Data Komputer. Kejahatan tersebut dapat disebut sebagai *´cost´* atau harga mahal dari suatu perubahan masyarakat global yang tingkat perkembangannya melebihi eksistensi hukum. Kejahatan *cybercrime* yang populer disebut juga kejahatan cyber space merupakan cerminan dari kondisi masyarakat yang selalu berkejaran antara keinginan dengan tarikan pengaruh global yang tidak sedikit memproduk dan menawarkan perubahan yang bersifat kerugian. Misalnya menjadikan teknologi sebagai alat memenuhi perkembangan dan dasar pengembangan sistem transaksi pada perbankan, tetapi masih seringkali kita gagal menolak dampak destruktifnya.

Berdasarkan perkembangan zaman dan semakin canggihnya teknologi pula yang semakin memacu kejahatan *cybercrime* untuk berevolusi menjadi berbagai macam jenis kejahatan baru dan modus operandi yang berkaitan dengan tindak kejahatan cybercrime.

Hukum berfungsi sebagai perlindungan kepentingan manusia. Agar kepentingan manusia terlindungi, hukum harus dilaksanakan[1]. Jadi perlindungan hukum merupakan perlindungan yang diberikan oleh hukum maupun undang-undang untuk melindungi kepentingan manusia agar kehidupan manusia dapat berlangsung normal, tentram dan damai.

Permasalahan secara yuridis untuk menjerat pelaku kejahatan ini biasanya dikaitkan dengan berbagai persoalan yang berhubungan dengan beberapa karakteristik kejahatan *cybercrime* yaitu, *pertama*, siapa yang berwenang mengatur atau membuat regulasi yang berkaitan dengan kejahatan di internet mengingat kejahatan ini melintasi batas teritorial atau borderless territory, atau bahkan bisa dikatakan di luar teritorial negara (*out of the state territory*), yang pada akhirnya berkaitan dengan yurisdiksi mana yang berhak melakukan proses peradilan. Tetapi dalam kajian ini, lebih memfokuskan pada tindak kejahatan *cybercrime* di wilayah teritorial nasional.

Kedua, berkaitan dengan asas legalitas yang sangat fundamental dalam hukum pidana, apakah kejahatan dalam dunia maya dapat di jerat dengan hukum pidana melalui cara penafsiran, mengingat kejahatan tersebut merupakan sesuatu yang sama sekali baru. Sementara umumnya hukum pidana hanya menerima penafsiran otentik saja. Disamping berbagai persoalan lain yang berkaitan seperti alat bukti elektronik dan sebagainya sebagai kelajutan.

---

[1] Sudino Mertokusumo dan A. Pitlo, *Bab- bab Tentang Penemuan Hukum*, Cet I, PT. Citra Aditya Bakti, 1993, h. 1.

Persoalan tersebut diatas sesungguhnya berkaitan dengan kebijakan hukum pidana (*penal policy*). Marc Ancel mendefinisikan kebijakan hukum pidana (*penal policy*) sebagai suatu ilmu sekaligus seni yang bertujuan untuk memungkinkan peraturan hukum positif (dalam hal inihukum pidana) di rumuskan secara lebih baik.

Sementara itu upaya perumusan hukum pidana secara lebih baik, mencakup di dalamnya kebijakan merubah atau membuat aturan khusus (hukum pidana) yang berkaitan dengan kejahatan *cybercrime*. Artinya walaupun secara essensial dapat di analogikan dengan kejahatan atau tindak pidana yang dapat diatur dalam KUHP, namun menurut pendapat para ahli, hukum pidana tidak menerima analogi. Disamping itu, juga karena karakteristik kejahatan tersebut yang berbeda maka dimungkinkan dijadikan tindak pidana tersendiri dengan aturan tersendiri pula dalam rangka mewujudkan rumusan hukum pidana yang lebih baik.

Kriminalisasi terhadap perbuatan-perbuatan yang dalam Bab VII sebagai perbuatan ada dua Undang- undang utama yang mengatur tentang informasi dan transaksi elektronik di Indonesia. Undang-undang yang pertama adalah Undang-undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Undang- undang yang ke dua adalah undang- undang yang telah dikeluaran sebelum dikeluarkannya Undang- undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Undang- undang tersebut adalah Undang- undang No. 36 Tahun 1999 tentang Telekomunikasi.

Peran teknologi dalam dunia perbankan sangatlah mutlak, dimana kemajuan suatu sistem perbankan sudah barang tentu ditopang oleh peran teknologi informasi[2]. Semakin berkembang dan kompleks fasilitas yang diterapkan perbankan untuk memudahkan pelayanan, itu berarti semakin beragam dan kompleks adopsi teknologi yang dimiliki oleh suatu bank. Tidak dapat dipungkiri, dalam setiap bidang termasuk perbankan penerapan teknologi bertujuan selain untuk memudahkan operasional intern perusahaan, juga bertujuan untuk semakin memudahkan pelayanan terhadap kostomer atau nasabah bank. Apabila untuk saat ini, khususnya dalam dunia perbankan hampir semua produk yang ditawarkan kepada nasabah (costomer) serupa, sehingga persaingan yang terjadi dalam dunia perbankan adalah bagaimana memberikan produk yang serba mudah dan serba cepat. Namun tampaknya dibalik perkembangan ini terdapat berbagai permasalahan hukum yang berkaitan dengan kejahatan informasi dan transaksi elektronik di bidang perbankan yang kemudian merugikan bank, masyarakat dan/ nasabah jika tidak diantisipasi dengan baik.

Seiring dengan semakin maraknya tindak kejahatan *cybercrime* di bidang perbankan yaitu kasus pembobolan terhadap sistem keamanan dan pembobolan rekening (*hacking*) atau sistem elektronik nasabah dalam sistem perbankan nasional dengan menggunakan sarana, prasarana dan identitas orang lain guna memalsukan kartu kredit dalam kejahatan yang disebut *Carding*. Sehingga dalam penegakan hukum pidana, korporasi khususnya

[2] Ronny Presetya, *Pembobolan ATM, tinjauan hukum perlindungan nasabah korban kejahatan perbankan*, Jakarta, PT. Pustaka, 2010, h. 27.

lembaga perbankan tidak hanya menjadi korban pembobolan rekening nasabah tetapi juga masih bertanggung jawab atas kerugian yang dialami oleh nasabah.

Modus operandi carding yaitu terdapat berbagai program carding dan bagaimana mendapatkan kartu- kartu kredit, bagaimana membuat nomor-nomor kartu kredit yang palsu, bagaimana menggandakan kartu- kartu kredit yang sah, dan bagaimana menggunakan kartu kredit yang palsu itu. Memperoleh data yang terkait dengan suatu rekening itu dapat dilakukan dengan berbagai cara. Hal itu biasanya dilakukan tanpa sepengetahuan pemegang kartu kredit (*credit card holder*), merchant, atau bank penerbit kartu kredit setidak- tidaknya sampai akhirnya rekening tersebut digunakan untuk melakukan kejahatan.

Sehingga dengan munculnya modus operandi dari kejahatan carding ini, menjadi pemicu munculnya dampak yang ditimbulkan. Dampak atas kejahatan carding tersebut antara lain yaitu terjadinya viktimisasi secara langsung dan tidak langsung kepada masyarakat, Kerugian secara material dan non material kepada sistem perbankan secara khusus dan sistem perekonomian secara umum, hukum di negara kita harus segera diremajakan. Maka semakin berkembangnya dunia komunikasi melalui jasa internet dan semakin bergantungnya transaksi bisnis menggunakan jasa perbankan lewat Internet, maka pengaturan *cybercrime* di Indonesia sudah sangat mendesak dibutuhkan.

Seiring dengan pesatnya perkembangan teknologi informasi telah merubah pola kehidupan, *virtual life* dan *reality life*. Perubahan paradikma ini

sebagai akibat dari kehadiran *cyber space*, yang merupakan imbas dari jaringan computer global.

Terutama berkaitan mengenai unsur-unsur perbuatan, mendistribusikan, menstransmisikan, membuat dapat diakses. Sedangkan yang berkaitan dengan unsur perbuatan yang memiliki muatan "Pemerasan" dan "Pengancaman" masih sangat kurang spesifik dalam aturan penjelasannya.

Berkaitan dengan unsur yang memiliki muatan "Pengancaman" penafsirannya masih sangatlah luas. Sebagai contohnya yaitu apabila seseorang mengakses suatu jaringan atau sistem komputer milik perusahaan atau perbankan tertentu, sudah dapat dikatakan sebagai perbuatan pengancaman.

Sehubungan dengan hal- hal yang memiliki muatan pengancaman di atas belum terdapat aturan penjelasannya dalam UU ITE, maka para hakim melakukan penafsiran yang bersifat legal positifistik dengan menggunakan ketentuan perbuatan yang dilarang dalam KUHP yaitu : pencurian, penggelapan, dan penipuan. Apabila hakim menerapkan ketentuan tersebut, maka hanya akan ditujukan kepada para pelaku kejahatan ITE saja dan hak-hak korban terutama hak- hak para nasabah bank belum terpenuhi. Sehingga dalam permasalahan ini UU ITE masih belum memberikan perlindungan atas hak- hak nasabah bank sebagai korban kejahatan ITE di bidang perbankan. Maka perlu dilakukan upaya hukum perdata, sebagai upaya atas pemenuhan hak- hak nasabah bank sebagai korban kejahatan ITE di bidang perbankan.

Sebetulnya UU ITE sudah mengatur mengenai sanksi hukum terhadap pelaku kejahatan, yaitu tertuang dalam Pasal 30 ayat (1) jo Pasal 46 ayat (1) UU ITE, namun ketentuan tersebut masih jarang digunakan karena masih bersifat umum. Sedangkan apabila kita fokus kepada upaya hukum perdata yang dilakukan oleh pihak bank dan nasabah bank yang menjadi korban kejahan ITE di bidang perbankan, maka hak- hak nasabah bank yang menjadi korban belum juga terealisasi. Karena berdasarkan unsur perbuatannya, pelaku kejahatan ITE membobol suatu sistem milik perusahaan perbankan dan melakukan upaya mengakses, mendistribusikan, memanipulasi, menyalin data dan membobol data atau rekening nasabah bank. Sehingga berdasarkan realita yang ada, lembaga perbankan tidak menjamin atas ganti kerugian material atas pencurian rekening nasabah bank yang dilakukan oleh pelaku kejahatan ITE apabila tidak diatur secara terperinsi dalam draf kesepakatan perjanjian penjaminan keamanan rekening antara pihak bank dengan nasabah bank.

Karena dalam ketentuan UU Saksi dan Korban diuraikan berkaitan dengan pemenuhan hak-hak korban atas kerugian yang di timbulkan oleh pelaku kejahatan. Sehingga diperlukan ketentuan khusus dalam UU Perbankan yang mengatur hak-hak nasabah bank yang menjadi korban kejahatan ITE di bidang perbankan. Selain nasabah bank yang menjadi korban kejahatan yang di lakukan oleh pelaku kejahatan ITE. Perusahaan perbankan juga menjadi korban atas kerugian yang ditimbulkan oleh pelaku kejahatan ITE di bidang perbankan.

Bank yang menjadi korban atas pelaku kejahatan ITE juga berhak mendapatkan hak-hak atas kerugian yang dialami. Baik berkenaan dengan sistem/jaringan komputer bank yang dirusak atau dibobol oleh pelaku kejahatan, juga ganti kerugian atas rekening nasabah yang telah di curi atau dibobol para pelaku kejahan ITE. Selain itu perusahaan perbankan juga berkewajiban memenuhi hak-hak nasabah bank yang menjadi korban kejahatan pelaku pembobol rekening bank tersebut (apabila ada perjanjian yang mengatur).

B. Rumusan Masalah

Berdasarkan latar belakang masalah yang telah diuraikan di atas dan sesuai dengan judulnya, maka permasalahan yang akan dibahas dalam penelitian ini adalah sebagai berikut :

1. Bagaimanakah perlindungan hukum terhadap nasabah yang menjadi korban kejahatan ITE di bidang perbankan dalam Undang-Undang terkait?
2. Bagaimanakah tanggung jawab bank terhadap nasabah yang menjadi korban tindak pidana ITE dalam bidang perbankan?

C. Tujuan Penelitian

Tujuan utama yang ingin dicapai dalam penelitian ini adalah sebagai berikut :

1. Untuk mengetahui perlindungan hukum terhadap nasabah yang menjadi korban kejahatan ITE di bidang perbankan dalam Undang-Undang terkait.

2. Untuk mengetahui tanggung jawab bank terhadap nasabah yang menjadi korban tindak pidana ITE dalam bidang perbankan

D. Manfaat Penelitian

Adapun manfaat penelitian ini adalah sebagai berikut :

1. Manfaat Teoritis

   Secara Teoritis, penelitian ini diharapkan dapat memberikan sumbangsih ilmiah bagi ilmu pengetahuan hukum dalam pengembangan hukum pidana, khususnya pemahaman teoritis tentang perlindungan hukum terhadap nasabah yang menjadi korban kejahatan ITE di bidang perbankan, dan pengkajian terhadap beberapa peraturan hukum pidana yang berlaku saat ini berkaitan dengan upaya perlindungan hukum terhadap nasabah yang menjadi korban kejahatan ITE di bidang perbankan.

2. Manfaat Praktis

   Secara praktis, hasil penelitian yang berfokus pada perlindungan hukum terhadap nasabah yang menjadi korban kejahatan ITE di bidang perbankan ini diharapkan bisa menjadi bahan pertimbangan dan sumbangan pemikiran serta dapat memberikan kontribusi dan solusi kongkrit bagi para legislator dalam upaya memberikan perlindungan hukum terhadap nasabah yang menjadi korban kejahatan ITE di bidang perbankan di Indonesia. Dengan pendekatan kebijakan hukum pidana yang tetap memperhatikan pendekatan aspek lainnya dalam kesatuan pendekatan sistemik/integral, diharapkan dapat menghasilkan suatu

kebijakan yang benar-benar dapat memberikan perlindungan hukum terhadap nasabah yang menjadi korban kejahatan ITE di bidang perbankan ini, khususnya dalam rangka pembaharuan hukum pidana di Indonesia di masa yang akan datang.