PERLINDUNGAN HUKUM DAN HAM TERHADAP NASABAH BANK KORBAN *CYBER CRIME* DALAM INTERNET BANKING BERDASARKAN UNDANG-UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK

TESIS

Disusun untuk Memenuhi Sebagian Syarat Memperoleh

Gelar Magister Ilmu Hukum

Oleh :

DICKY ZHAFAR RIYANTO

NIM 21120071

MAGISTER ILMU HUKUM FAKULTAS HUKUM

UNIVERSITAS DARUL ULUM ISLAMIC CENTRE SUDIRMAN GUPPI

(UNDARIS)

2023

PERLINDUNGAN HUKUM DAN HAM TERHADAP NASABAH BANK KORBAN *CYBER CRIME* DALAM INTERNET BANKING BERDASARKAN UNDANG-UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK

TESIS

Disusun untuk Memenuhi Sebagian Syarat Memperoleh

Gelar Magister Ilmu Hukum

Oleh :

DICKY ZHAFAR RIYANTO, S.Ak.

21120071

MAGISTER ILMU HUKUM FAKULTAS HUKUM

UNIVERSITAS DARUL ULUM ISLAMIC CENTRE SUDIRMAN GUPPI

(UNDARIS)

2023

HALAMAN PERSETUJUAN PEMBIMBING

Judul Tesis	:	PERLINDUNGAN HUKUM DAN HAM TERHADAP NASABAH BANK KORBAN *CYBER CRIME* DALAM INTERNET BANKING BERDASARKAN UNDANG-UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK
Nama Mahasiswa	:	DICKY ZHAFAR RIYANTO, S.Ak.
NIM	:	21120071
Program Studi	:	Magister Ilmu Hukum

Tesis ini telah disetujui oleh Dosen Pembimbing dan dinyatakan memenuhi syarat ilmiah untuk dipertahankan dalam Sidang Ujian Tesis yang diselenggarakan oleh Program Studi Magister Ilmu Hukum Undaris.

Persetujuan Dosen Pembimbing diberikan pada hari Sabtu, tanggal 8 April 2023.

Tim Dosen Pembimbing

Pembimbing I	Pembimbing II
Dr. Drs. Lamijan, S.H., M.Si.	Dr. Mohamad Tohari, S.H., M.H.

Mengetahui

Ketua Program Studi Magister Ilmu Hukum

Dr. Drs. Lamijan, SH, M. Si

HALAMAN PENGESAHAN UJIAN TESIS

Judul Tesis	:	PERLINDUNGAN HUKUM DAN HAM TERHADAP NASABAH BANK KORBAN *CYBER CRIME* DALAM INTERNET BANKING BERDASARKAN UNDANG-UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK
Nama Mahasiswa	:	DICKY ZHAFAR RIYANTO, S.Ak.
NIM	:	21120071
Program Studi	:	Magister Ilmu Hukum

Tesis ini telah dipertahankan di hadapan Dewan Penguji dalam Sidang Ujian Tesis dan dinyatakan sah menemuhi syarat serta lulus pada hari hari Kamis, tanggal 4 Mei 2023.

Dewan Penguji Ujian Tesis

Ketua Penguji.

Dr. Drs. Lamijan, S.H., M.Si.

Anggota Penguji,

Dr. Mohamad Tohari, S.H., M.H.

Anggota Penguji,

Dr. Hj. Endang Kusuma A., S.H., M.Hum.

Mengetahui

Ketua Program Studi Magister Ilmu Hukum

Dr. Drs. Lamijan, S.H., M.Si.

SURAT PERNYATAAN KEASLIAN TESIS

Yang bertanda tangan di bawah ini, saya:

Nama Lengkap : DICKY ZHAFAR RIYANTO, S.Ak.

Tempat, Tanggal Lahir : 20 Februari 1998

NIM : 21120071

Program Studi : Magister Ilmu Hukum

Menyatakan dengan ini sesungguhnya bahwa naskah tesis saya yang berjudul:

PERLINDUNGAN HUKUM DAN HAM TERHADAP NASABAH BANK KORBAN *CYBER CRIME* DALAM INTERNET BANKING BERDASARKAN UNDANG-UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK

Adalah benar-benar merupakan karya asli saya sendiri. Hal-hal yang bukan karya saya sendiri dalam naskah tesis tersebut telah diberi tanda sitasi dan ditunjukkan dalam daftar pustaka.

Apabila di kemudian hari terbukti pernyataan daya tersebut tidak benar, maka saya bersedia menerima sanksi akademik, berupa pencabutan tesis dan gelar akademik yang saya peroleh dari tesis tersebut.

Demikian pernyataan ini saya buat dengan sebenar-benarnya untuk dapat dipergunakan sebagaimana mestinya.

Ungaran, April 2023

Yang Membuat Pernyataan,

DICKY ZHAFAR RIYANTO, S.Ak.

PRAKATA

Puji syukur kami panjatkan atas kehadirat Allah SWT, berkat karunia-Nya Tesis ini dapat penulis selesaikan. Tesis ini disusun sebagai salah satu syarat dalam menyelesaikan Program Magister Hukum (S2) pada Program Pascasarjana Universitas Darul Ulum Islamic Center Sudirman Guppi Ungaran dengan judul **"PERLINDUNGAN HUKUM DAN HAM TERHADAP NASABAH BANK KORBAN *CYBER CRIME* DALAM INTERNET BANKING BERDASARKAN UNDANG-UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK"**

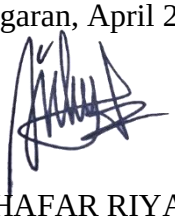
Penulis menyadari bahwa Tesis ini melibatkan banyak pihak yang telah berkontribusi baik berupa motivasi, tenaga dan pemikiran yang tak ternilai harganya. Maka perkenankanlah penulis mengucapkan terima kasih yang tak terhingga dan tulus kepada;

1. Dr. Drs. H. Hono Sejati, S.H., M.Hum., selaku Rektor Universitas Darul Ulum Islamic Center Sudirman Guppi Ungaran yang telah memberikan kesempatan kepada kami untuk mengikuti pendidikan Program Magister Hukum Universitas Darul Ulum Islamic Center Sudirman Guppi Ungaran.
2. Dr. Drs. Lamijan, SH, M. Si., selaku ketua program studi magister ilmu hukum Universitas Darul Ulum Islamic Center Sudirman Guppi Ungaran dan selaku pembimbing I tesis atas kesempatan yang diberikan untuk mengikuti pendidikan Program Magister Hukum Universitas Darul Ulum Islamic Center Sudirman Guppi Ungaran serta telah menyediakan waktu, tenaga dan pikiran untuk bimbingan penyusunan hasil penelitian tesis ini

3. Dr. Mohamad Tohari, S.H., M.H., selaku pembimbing II tesis yang telah menyediakan waktu, tenaga dan pikiran untuk bimbingan penyusunan hasil penelitian tesis ini.
4. Bapak dan Ibu Staf pengajar dan Sekretariat Program Magister Hukum Universitas Darul Ulum Islamic Center Sudirman Guppi Ungaran.
5. Keluargaku terkasih, terima atas doa dan bantuan untuk penyelesian hasil penelitian tesis ini.

Penulis menyadari bahwa Tesis ini masih terdapat sejumlah kekurangan yang merupakan kelemahan penulis dalam membuat. Dengan segala hormat, segala bentuk kekurangan penulis mohon dapat dikoreksi oleh penguji pada ujian seminar hasil penelitian ini.

Ungaran, April 2023



DICKY ZHAFAR RIYANTO, S.Ak.

ABSTRAK

Penelitian ini bertujuan untuk 1) Menganalisis dan mendeskripsikan apa faktor-faktor penyebab timbulnya nasabah bank menjadi korban *cyber crime* dalam internet banking. 2) Menganalisis dan mendeskripsikan bagaimana perlindungan hukum dan ham terhadap nasabah bank korban *cyber crime* dalam internet banking berdasarkan undang-undang nomor 11 tahun 2008 tentang informasi dan transaksi elektronik. 3) Menganalisis dan mendeskripsikan apa saja hambatan yang dihadapi dalam perlindungan hukum dan ham terhadap nasabah bank korban *cyber crime* dalam internet banking berdasarkan undang-undang nomor 11 tahun 2008 tentang informasi dan transaksi elektronik.

Metode Penelitian dilakukan dengan normatif/doctrinal karena menggunakan konsep hukum yaitu norma-norma di dalam sistem perundang-undangan hukum nasional. Sedangkan pendekatan penelitian menggunakan *field reasearch* dengan jenis penelitian deskriptif dengan teknik pengumpulan data melalui wawancara dan studi pustaka kemudian data yang diperoleh dari hasil penelitian tersebut akan dianalisa dengan menggunakan metode analisis deskriptif.

Berdasarkan hasil penelitian dan pembahasan diperoleh hasil kesimpulan bahwa : 1) Perlindungan terhadap nasabah dapat dilakukan secara eksplisit yaitu perlindungan yang diperoleh melalui pembentukan lembaga yang menjamin simpanan masyarakat, dan perlindungan secara implisit yaitu perlindungan yang dihasilkan oleh pengawasan dan pembinaan bank secara efektif. 2) Perlindungan hukum dan HAM terhadap korban *cyber crime* diatur dalam Pasal 3 Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, dan Pasal 4 Undang-Undang Nomor 11 Tahun 2008. 3) Kendala yang dihadapi yaitu tingkat pemahaman para penegak hukum terhadap kegiatan/operasional perbankan yang berbeda-beda dan belum merata serta lemahnya koordinasi dalam penanganan kasus perbankan, belum efektifnya tindak lanjut penanganan kasus yang telah diserahkan, terdapat beberapa kasus yang sulit diungkapkan modus operandinya, perangkat hukum yang belum memadai, kurangnya pemahaman terhadap hacking komputer terhadap kasus-kasus itu.

Kata Kunci : *Cyber Crime*, Perlindungan Hukum, Transaksi Elektronik

ABSTRACT

This study aims to 1) analyze and describe what are the factors that cause bank customers to become victims of cyber crime in internet banking. 2) Analyze and describe how legal protection and human rights are for bank customers who are victims of cyber crime in internet banking based on law number 11 of 2008 concerning information and electronic transactions. 3) Analyze and describe what are the obstacles faced in legal and human rights protection for bank customers who are victims of cyber crime in internet banking based on law number 11 of 2008 concerning information and electronic transactions.

The research method is carried out in a normative/doctrinal way because it uses legal concepts, namely the norms in the national legal system. While the research approach uses field research with descriptive research types with data collection techniques through interviews and literature study then the data obtained from the research results will be analyzed using descriptive analysis methods.

Based on the results of the research and discussion, it can be concluded that: 1) Protection of customers can be carried out explicitly, namely protection obtained through the establishment of an institution that guarantees public deposits, and implicit protection, namely protection produced by effective bank supervision and development. 2) Legal protection and human rights for victims of cyber crime are regulated in Article 3 of Law Number 11 of 2008 concerning Information and Electronic Transactions, and Article 4 of Law Number 11 of 2008. 3) The obstacle faced is the level of understanding of law enforcers towards diverse and uneven banking activities/operations as well as weak coordination in handling banking cases, ineffective follow-up on cases that have been submitted, there are several cases where the modus operandi is difficult to disclose, inadequate legal instruments, lack of understanding of computer hacking against those cases.

Keywords : Cyber Crime, Legal Protection, Electronic Transactions

DAFTAR ISI

BAB I

PENDAHULUAN

A. Latar Belakang

Cyber crime merupakan kejahatan di dunia maya. Salah satu jenis kejahatan yang meningkat di dunia modern yang serba online karena kemajuan teknologi. Berbagai macam jenis modus kejahatan *cyber crime*. Mulai dari meminta-minta sumbangan atas nama kemanusiaan, pencurian data, sampai pembobolan rekening. *Cyber crime* termasuk perilaku ilegal yang dilakukan pelaku kejahatan dengan cara penggunaan teknologi komputer dan jaringan internet guna menyerang sistem informasi korban. Seperti melakukan *hack* media sosial, masuk dengan paksa pada perangkat teknologi dan data-data korban. Selanjutnya, merampas habis saldo rekening atau kartu kredit korban.[1]

Teknologi informasi dan komunikasi telah melahirkan inovasi perbankan serta memberikan dampak efisien dan ektivitas yang luar biasa.[2] Salah satu inovasinya yaitu bank menciptakan produk dan jasa. Produk dan jasa yang dilakukan oleh bank harus sesuai dengan ketentuan yang ada berdasarkan jenis banknya sebagaimana yang diatur dalam Undang-Undang Nomor 7 tahun 1992 tentang perbankan sebagaimana telah diubah dengan Undang-Undang Nomor 10 Tahun 1998.

[1] Barda Nawawi Arief, Strategi Penanggulangan Kejahatan Telematika, Semarang, Universitas Atma Jaya Yogyakarta, 2010
[2] Ronny Prasetya, *Pembobolan ATM, Tinjauan Hukum Perlindungan Nasabah Korban Kejahatan Perbankan*, Jakarta: PT. Prestasi Pustaka, 2010, hlm. 27

Di balik kemudahan yang diperoleh dari penggunaan internet, ada juga resiko yang diperoleh ketika menggunakan layanan ini, diantaranya banyak terjadi pelanggaran hukum menyangkut data-data pribadi melalui internet dan juga mengenai resiko finansial yang diderita oleh penggunaan internet, terutama dalam hal ini adalah *internet banking*[3]. Sementara ini, keamanan dan kenyamanan kurang diprioritaskan oleh banyak bank yang masuk ke internet di Indonesia.[4] Banyak nasabah bank yang tidak mau menggunakan fasilitas internet banking karena merasa tidak aman dan nyaman ketika melakukan transaksi.

Mayoritas nasabah merasa tidak aman jika web internet banking yang di akses adalah bukan web resmi melainkan manipulasi dari paracracker (seam page) dan juga takut ketika melakukan transaksi uang mereka tidak sampai ke tujuan yang disebabkan karena ulah para cracker. Bukan hanya itu, tetapi nasabah juga takut kalau PIN dan UserID mereka dapat diketahui oleh pihak yang tidak berwenang. Masalah tersebutlah yang membuat banyak nasabah tidak ingin menggunakan fasilitas internet banking, padahal fasilitas ini sangat efesien dan efektif. Hal ini juga dapat dikategorikan sebagai kebocoran data pribadi dari perusahaan perbankan. [5]

Pada dasarnya perlindungan hukum kepada nasabah merupakan hal yang sangat essensial melihat adanya fungsi bank sebagai *agent of trust*. Bank sebagai

---

[3] Menurut Bank Indonesia, Internet banking merupakan salah satu layanan jasa Bank yang memungkinkan nasabah untuk memperoleh informasi, melakukan komunikasi dan melakukan transaksi perbankan melalui jaringan internet. Jenis kegiatan internet banking dibedakan menjadi tiga.

[4] Gazali, Djoni S., and Rachmadi Usman. "Banking Law." Cet: III, Jakarta: Sinar Grafika, 2016

[5] Indonesia, Ikatan Bankir. Mengelola Bank Komersial. Gramedia Pustaka Utama, 2014

agen of trust dengan dasar utama kegiatan perbankan adalah trust atau kepercayaan, baik dalam menyalurkan dana maupun dalam menghimpun dana. Besarnya kepercayaan nasabah terhadap sistem elektronik berkaitan dengan besarnya kepercayaan mereka terhadap online banking.

Untuk mengatur adanya penggunaan teknologi informasi dalam dunia perbankan yang salah satunya internet banking, OJK membuat Peraturan Otoritas Jasa Keuangan No. 38/POJK.03/2016 tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum (POJK Manajemen Resiko TI). Adanya pengaturan baik berupa undang-undang maupun peraturan Otoritas Jasa Keuangan diharapkan dapat mengakomodir semua kebutuhan perlindungan hukum bagi nasabah yang akan melakukan transaksi internet banking.

Namun ternyata peraturan ini masih terdapat tindakan yang melanggar hak-hak dan perlindungan terhadap nasabah. Salah satu kasus terkait permasalahan internet banking adalah hilangnya uang nasabah pengguna internet banking. Perlindungan yang diberikan oleh bank sangat penting untuk menimbulkan kepercayaan dan kenyaman nasabah. Karena resiko yang ditimbulkan dalam layanan ini sangat tinggi, ada kemungkinan nasabah menderita kerugian karena disadap oleh hacker/crackeryang mampu menembus firewall atau memasuki website yang memiliki nama domain yang hampir sama.[6]

Sangat terlihat jelas sekali dengana adanya kemajuan zaman dan teknologi yang semakin berkembang juga semakin mendukung tumbuh kembang kejahatan dunia maya (*cyber crime*) yang semakin bermacam-macam atau bisa disebut *cyber*

[6] Marzuki, Petter Mahmud, 2015, Penemuan Hukum, Jakarta: Prenamedia Group.

crime yang berevolusi dan modus operadi yang berkaitan dengan tindakan kejahatan dunia maya. *Cyber crime* yang dulunya hanya dikenal dengan *"Hacking, Carding, Cracking"* hingga saat ini muncul berbagai macam bentuk kejahatan seperti "Danial of Service, Root Copromize (account compromixe dengan previlege bagi si penyusup), Account Copromize (penggunakaan akun secara ilegal), Probe (usaha untuk memperoleh akses ke dalam suatu sistem), Scan (Probe dalam jumlah besar), dan lain sebagainya.[7]

Yang justru menjadi persoalan bahwa adopsi teknologi terbaru, termasuk internet banking tidak bisa lepas dari proses edukasi kepada karyawan dan nasabah karena keduanya merupakan faktor yang berpengaruh terhadap transaksi. Realitas pembobolan rekening bank harus secepatnya dituntaskan demi menjaga reputasi internet banking. Perlindungan hukum berkaitan erat dengan rasa kepercayaan dan keamanan nasabah terhadap sistem tersebut, oleh karena itu diperlukan suatu perlindungan hukum yang memadai.[8]

Jenis modus operadi berbasis teknologi yang semakin bervariasi dan berkembang dengan pesat ini mempunyai karakteristik tertentu yang membedakannya dengan kejahatan yang lain, diantaranya:

1. Kejahatannya berkaitan dengan teknologi yang bekerja secara elektronik dan sistem digital dibarengi dengan pendukungnya seperti data, program dan sistem.

---

[7] Barda Nawawi Arief, *Strategi Penanggulanagn Kejahatan Telematika*, Semarang, Uiniversitas Atma Jaya Yogyakarta, 2010, hlm. 56

[8] Anggara, Bayu, and I. Nyoman Darmadha. "Penegakan Hukum Kejahatan Dunia Maya (Cybercrime) Yang Dilakukan Anak Di Bawah Umur." Kertha Wicara: Journal Ilmu Hukum

2. Teknologi pada kejahatan ini mampu berposisi menjadi alat, sarana, objek, atau sasaran kejahatan , bahkan mungkin saja sebagai subjek kejahatan.
3. Perlakuan atau kegiatan itu dilakukan dengan ilegal, tanpa maksud tidak etis atau tanpa hak.
4. Perbuatan itu dilakukan dengan cara memanipulasi atau memperdaya teknologi hingga sebagaimana yang seharusnya (sesuai dengan kemauan pelaku).
5. Sifat kejahatan mengikuti sifat teknologi yang bersifat intangible, virtual, dan borderless.
6. Kerugian yang ditimbulkan tidak selalu bersifat material namun juga bersifat immaterial seperti privasi, keamanan, jasa, waktu, pelayanan).
7. Pelaku kejahatan via teknologi dilakukan oleh orang yang profesional dalam artian mempunyai pengetahuan dan keterampilan yang lebih di bidang pengembangan dan pemanfaatan teknologi.
8. Pelakunya susah untuk dicari sebab pada teknologi informasi, identitas seseorang dapat disamarkan secara sempurna.
9. Sebagaimana pelaku dunia Information Technology (IT) lainnya pelaku kejahatan via teknologi informasi juga mempunya jiwa yang menyukai tantangan. Semakin terdorong untuk mencari celahnya atau kelemahannya dari sistem teknologi kemudian menyalahgunaan untuk motif-motif penyimpangan.

10. Korban kejahatan via IT ini umumnya tidak melaporkan kejahatan yang dialaminya, dengan beralasan tidak mengetahui kalau dirinya menjadi korban ketidakpercayan pada aparatur penegak hukum atau takut terkena imbas yang lebih parah lagi.

Hukum berguna untuk menjadi payung hukum yang melindungi kepentingan masyarakat. Artinya hukum ada karena untuk melindung segala bentuk kepentingan masyarakat di dalamnya agar terciptanya kadaan yang tenteram, aman dan damai.[9] Terdapat beberapa persoalan secara yuridis yang saling berkaitan dalam menjerat pelaku kejahatan *cyber crime* yakni, (1) siapa yang berhak mengatur atau membuat regulasi yang berhubungan dengan kejahatan di dunia maya jika melihat bahwasannya kejahatan ini melintasi batas teritorial atau bahkan bisa dilakukan diluar batas teritorial, yang berujung pada peradilan mana yang berhak mengadili kasus kejahatan ini. Tetapi dalam kajian ini lebih memfokuskan pada tindak kejahatan *cyber crime* teritorial nasional yang diatur oada Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Selanjutnya, (2) berkaitan dengan asas legalitas yang sangat mendasar dalam hukum pidana, apakah *cyber crime* mampu diikat dengan hukum pidana melalui cara interprestasi, mengingat tindakan jahat tersebut adalah suatu yang sama sekali baru. Sementara biasanya hukum pidana hanya menerima penafsiran otentik saja. Disamping berbagai persoalan lain yang kaitannya dengan seperti alat bukti elektronik dan sebagainya sebagai kelanjutan. Persoalan tersebut sebenarnya

[9] Astrini, Dwi Ayu. "Perlindungan Hukum Terhadap Nasabah Bank Pengguna Internet Banking Dari Ancaman Cybercrime." Lex Privatum 3, no. 1 (2015).

berkaitan dengan kebijakan hukum pidana. Marc Ancel mendefinisikan kebijakan hukum pidana sebagai suatu ilmu sekaligus seni yang bertujuan untuk memungkinkan peraturan hukum positif dirumuskan secara lebih baik.[10]

Sementara itu upaya perumusan hukum pidana secara lebih baik, mencakup di dalamnya kebijakan merubah atau membuat aturan khusus (hukum pidana) yang berkaitan dengan kejahatan *cyber crime*.[11] Artinya walaupun secara essensial dapat di analogikan dengan kejahatan atau tindak pidana yang dapat diatur dalam Kitab Undang-Undang Hukum Pidana (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.

---

[10] Al' Adl. *Perlindungan Hukum Terhadap Nasabah Bank yang menjadi Korbsn krjahatan dibidang Perbankan. 2013* Volume V Nomor 9 hlm. 34

[11] Disemadi, Hari Sutra, and Paramita Prananingtyas. "Perlindungan Hukum Terhadap Nasabah Perbankan Pengguna CRM (Cash Recycling Machine)." Jurnal Magister Hukum Udayana (Udayana Master Law Journal) 8, no. 3 (2019)

Kebijakan hukum pidana (penal policy) dengan membuat peraturan hukum pidana yang baik melalui pembaharuan hukum pidana materiel/ substantif, merupakan upaya yang dapat memberikan perlindungan terhadap korban kejahatan *cyber crime* di bidang Informasi dan Transaksi Elektronik. Oleh karena itu, pembaharuan hukum pidana materiel atau substantif khususnya KUHP dalam rangka pembangunan/pembaharuan (sistem) hukum nasional merupakan kebutuhan penting dalam upaya memberikan perlindungan terhadap masyarakat. [12]

Dalam Konsep KUHP saat ini yang mempertegas pelaku kejahatan bukan hanya orang (naturalijk person), tetapi juga badan hukum (recht person) merupakan perkembangan yang sangat luar biasa, karena melalui pembaharuan KUHP terbuka kesempatan untuk memperluas jenis kejahatan yang juga dapat dilakukan oleh korporasi, yakni dengan memastikan atas perbuatan pidana siapa sajakah suatu korporasi harus bertanggung jawab secara pidana, serta menentukan jenis-jenis pidana yang paling tepat bagi korporasi agar dapat memberikan rasa adil bagi korban serta menimbulkan deterrent effect. Seiring perkembangannya, ternyata badan usaha atau korporasi tidak hanya bisa menjadi pelaku kejahatan *cyber crime* tetapi juga menjadi sasaran pelaku kejahatan dunia maya yang lain.[13]

Sehubung dengan hal-hal di atas, perlindungan hukum amat sangat diperlukan bagi para nasabah pengguna *internet banking* yang bertujuan untuk melindungi hak-hak nasabah selaku konsumen dalam jasa perbankan, mengingat

---

[12] Nugraha, Ferry Satya, and Rinitami Njatrijani Budiharto. "Perlindungan Hukum Terhadap Nasabah Bank Dalam Pembobolan Internet Banking Melalui Metode Malware." Diponegoro Law Journal 5, no. 3 (2016)

[13] Sjahdeini, Sutan Remy, *Kejahatan dan Tindak Pidana Komputer*, Jakarta: Puataka utama Grafiti, 2009, hlm. 82

jasa hukum itu memandu dan melayani masyarakat. Kejahatan dunia maya ini di Indonesia telah diatur sebagaimana pada UU No. 11/2008 tentang Informasi dan Transaksi Elektronik. Lalu konsep perlindungan seperti apa yang tertuang dalam peraturan tersebut sehingga mampu melindungi nasabah, mengingat juga hukum itu memadu dan melayani masyarakat.

B. Rumusan Masalah

1. Apa faktor-faktor penyebab timbulnya nasabah bank menjadi korban *cyber crime* dalam internet banking?
2. Bagaimana perlindungan hukum dan ham terhadap nasabah bank korban *cyber crime* dalam internet banking berdasarkan undangundang nomor 11 tahun 2008 tentang informasi dan transaksi elektronik?
3. Apa saja hambatan yang dihadapi dalam perlindungan hukum dan ham terhadap nasabah bank korban *cyber crime* dalam internet banking berdasarkan undang-undang nomor 11 tahun 2008 tentang informasi dan transaksi elektronik?

C. Tujuan Penelitian

1. Tujuan Umum

Untuk menggunakan pemahaman teori yang telah didapatkan.

2. Tujuan Khusus

a. Untuk menganalisis dan mendeskripsikan apa faktor-faktor penyebab timbulnya nasabah bank menjadi korban *cyber crime* dalam internet banking.

b. Untuk menganalisis dan mendeskripsikan bagaimana perlindungan hukum dan ham terhadap nasabah bank korban *cyber crime* dalam internet banking berdasarkan undangundang nomor 11 tahun 2008 tentang informasi dan transaksi elektronik.

a. Untuk menganalisis dan mendeskripsikan apa saja hambatan yang dihadapi dalam perlindungan hukum dan ham terhadap nasabah bank korban *cyber crime* dalam internet banking berdasarkan undang-undang nomor 11 tahun 2008 tentang informasi dan transaksi elektronik.

D. Manfaat Penelitian

1. Manfaat Teoritis

Penelitian ini dilaksanakan dalam rangka menganalisis teori yang telah ada dan kemudian mengembangkan teori yang ada menuju kearah yang lebih progresif.

2. Manfaat Praktis

Memperluas pengetahuan tentang perlindungan hukum terhadap nasabah bank korban *cyber crime* dalam internet banking berdasarkan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

E. Sistematika Penelitian

Bab I Pendahuluan berisi tentang latar belakang masalah, keterbaruan penelitian, rumusan masalah, tujuan penelitian, manfaat penelitian dan sistematika tesis.

Bab II Tinjuan Pustaka berisi tentang landasan konseptual, landasan teori, orisinalitas penelitian, kerangka pemikiran.

Bab III Metode Penelitian berisi tentang jenis penelitian, metode pendekatan, sumber data, teknik pengumpulan data dan teknik analisis data.

Bab IV Hasil Penelitian dan Pembahasan meliputi perlindungan hukum dan ham terhadap nasabah bank korban *cyber crime* dalam internet banking berdasarkan Undang-Undang Nomor 11 tahun 2008 tentang informasi dan transaksi elektronik, hambatan yang dihadapi dalam perlindungan hukum dan ham terhadap nasabah bank korban *cyber crime* dalam internet banking berdasarkan Undang-Undang Nomor 11 tahun 2008 tentang informasi dan transaksi elektronik, serta upaya mengatasi kendala perlindungan hukum dan ham terhadap nasabah bank korban *cyber crime* dalam internet banking berdasarkan Undang-Undang Nomor 11 tahun 2008 tentang informasi dan transaksi elektronik.

Bab V Penutup, bab ini merupakan bab penutup yang berisikan tentang kesimpulan dan saran dari penulis yang mungkin berguna sebagai salah satu upaya dalam menjawab permasalahan yang ada.

BAB II

TINJAUAN PUSTAKA

A. Landasan Konseptual

1. Hak asasi manusia

   Hak asasi manusia secara harfiah dapat dipahami, sebagai suatu pemberian dari Tuhan Yang Maha Esa dan melekat secara kodrati kepada manusia yang tanpanya manusia tidak akan mampu untuk menjalani kehidupan sebagai seorang manusia yang bertanggungjawab[14].

2. Nasabah bank

   Nasabah adalah orang atau badan usaha yang mempunyai rekening simpanan atau pinjaman pada bank.

3. Informasi dan transaksi elektronik

   Informasi dan transaksi elektronik adalah kegiatan informatif dan transaksi yang dijalankan dengan menggunakan suatu sistem elektronik.

B. Landasan Teoritis

1. *Cyber crime*

Memasuki pembahasan terkait pengertian *cyber crime* maka akan menyinggung tentang keamanan suatu jaringan komputer atau informasi teknologi telekomunikasi. Terutama pada era globalisasi saat ini, yang membawa kemajuan teknologi sangat pesat maka hal tersebut tidak terlepas adanya resiko dari penyalahgunaan dari pemanfaatan teknologi sebagai

[14] Serlika Aprita dan Yonani Hasyim, *Hukum dan Hak Asasi Manusia*, (Bogor: Mitra Wacana Media, 2020), hal. 6.

kebutuhan informasi. “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.” Kemajuan teknologi sangat berdampak besar bagi masyarakat yang membawa dampak positif dan dampak negatif terhadap perkembangan manusia dan peradabannya. Dampak negatif yang dimaksud adalah yang berkaitan dengan dunia kejahatan. J. E Sahetapy telah menyatakan, bahwa kejahatan erat kaitanya dan bahkan menjadi sebagian dari hasil budaya itu sendiri. Maka demikian artinya semakin tinggi tingkat budaya dan semakin modern suatu bangsa, maka semakin modern pula kejahatan itu dalam bentuk, sifat dan cara pelaksanaanya.

Perkembangan teknologi komputer, teknologi informasi, dan teknologi komunikasi juga menyebabkan munculnya tindak pidana baru yang memiliki karakteristik yang berbeda dengan tindak pidana konvensional. Penyalahgunaan komputer sebagai salah satu dampak dari ketiga perkembangan teknologi tersebut itu tidak terlepas dari sifatnya yang memiliki ciri-ciri tersendiri sehingga membawa persoalan yang rumit dipecahkan berkenaan dengan masalah penanggulangannya mulai dari penyelidikan, penyidikan hingga dengan penuntutan. Sehingga berdasarkan beberapa pendapat tersebut maka dapat dikatakan bahwa adanya kemajuan

teknologi dan informasi selain dapat dipergunakan manusia sebagai komoditi informasi, juga dapat membawa dampak negatif yakni penyalahgunaan teknologi yang membawa hal tersebut pada suatu tindak pidana yang disebut dengan *cyber crime*.

Cybercrime merupakan kejahatan yang berbeda dengan kejaharan konvensional (street crime). *Cyber crime* muncul bersamaan dengan lahirnya revolusi teknologi informasi. Sebagimana dikemukakan oleh Ronni R. Nitibaskara bahwa: "Interaksi sosial yang meminimalisir kehadiran secara fisik, merupakan ciri lain revolusi teknologi informasi. Penyimpangan social menyesuasikan bentuk dn karakter baru dalam kejahatan.13 Merujuk pada pendapat tersebut maka *cyber crime* dapat dimaknai secara luas dan sempit. Dalam arti sempit, *cyber crime* dapat dimaknai sebagai perbuatan yang melanggar hukum dengan memanfaatkan teknologi komputer. Sedangkan dalam arti luas, *cyber crime* merupakan keseluruhan bentuk kejahatan yang ditujukan pada komputer baik dari jaringan maupun penggunanya serta kejahatan konvensional yang menggunakan teknologi komputer.

Berdasarkan beberapa literatur dan prakteknya, *cyber crime* memiliki beberapa karakter yang khas dibandingkan kejahatan konvensional, yaitu antara lain :

a. Perbuatan yang dilakukan secara illegal, tanpa hak tersebut terjadi di ruang/wilayah maya (cyber space),sehingga sulit dipastikan yurisdiksi hukum negara mana yang berlaku terhadapnya;

b. Perbuatan tersebut dilakukan dengan menggunakan peralatan apapun yang bisa terhubung dengan internet;
c. Perbuatan tersebut mengakibatkan kerugian materiil maupun immateriil (waktu, nilai, jasa, uang, barang, harga diri, martabat, kerahasiaan informasi) yang cenderung lebih besar dibandingkan kejahatan konvensional;
d. Pelakunya adalah orang yang menguasai penggunaan internet beserta aplikasinya;
e. Perbuatan tersebut sering kali dilakukan secara transnasional/ melintasi batas negara.

2. Perlindungan Nasabah

Perlindungan terhadap konsumen pada umumnya dan perlindungan pada nasabah bank pada khususnya merupakan topik yang sangat menarik untuk didiskusikan. Konsumen atau nasabah bank seringkali menjadi pihak yang dirugikan. Hubungan antara bank dengan nasabah sebagai konsumen merupakan hubungan yang timpang karena di satu sisi bank mempunyai bargaining power yang lebih kuat sehingga nasabah berada pada posisi menerima (take it or leave it) saja. Dengan adanya hubungan yang tidak seimbang ini, perlindungan terhadap nasabah sebagai konsumen bank adalah menjadi sangat penting. Perlindungan terhadap nasabah bank atau konsumen dilakukan melalui undang-undang yang pada akhirnya dapat mengikat para pihak.

Pada prinsipnya setiap undang-undang melindungi kepentingan masyarakat, atau nasabah bank pada khususnya. Misalnya pada UU Perlindungan Konsumen,perlindungan terhadap nasabah bank terutama bisa dilihat dari pasal 18 tentang pencantuman klausula baku. Pelaku usaha, dalam hal ini bank, dalam setiap perjanjian kredit atau surat-surat yang berkenaan dengan bank biasanya selalu mencantumkan klausula baku. Pencantuman klausula baku ini membuat nasabah tidak bisa berkutik atau protes. Apabila nasabah tidak setuju dengan klausula yang diajukan oleh bank, maka nasabah boleh saja untuk tidak mengikatkan diri dengan bank, tetapi hal tersebut akan merugikan nasabah itu sendiri.

Oleh karena itu UU Perlindungan Konsumen berupaya untuk melindungi nasabah bank dengan cara membuat batasan-batasan terhadap klausula baku yang tidak dapat dihindari di dalam dunia bisnis ini. Contoh yang lain dari upaya Undang-undang untuk melakukan perlindungan kepada masyarakat dengan adanya KUH Perdata, misalnya pada pasal 1367 disebutkan bahwa:

"Tiap perbuatan melanggar hukum, yang membawa kerugian kepada seorang lain, mewajibkan orang yang karena salahnya menerbitkan kerugian itu, untuk mengganti kerugian tersebut".

Pasal mengenai perbuatan melanggar hukum ini juga bertujuan untuk melindungi kepentingan masyarakat, pada khususnya nasabah bank. Selain itu juga yang jelas secara tegas melindungi kepentingan nasabah bank adalah UU Perbankan, UU Bank Indonesia, KUHP, UU PT, dan lain sebagainya. Apabila berbicara mengenai perlindungan terhadap nasabah bank, maka kita harus membedakan nasabah sebagai kreditur terhadap bank dan nasabah sebagai debitur terhadap bank. Dalam konteks UU Perbankan, nasabah dibagi menjadi 2 (dua) yaitu nasabah penyimpan dan nasabah debitur. Nasabah Penyimpan adalah nasabah yang menempatkan dananya di bank dalam bentuk simpanan berdasarkan perjanjian bank dengan nasabah yang bersangkutan. Sedangkan yang dimaksud dengan nasabah debitur adalah nasabah yang memperoleh fasilitas kredit atau pembiayaan berdasarkan prinsip syariah atau yang dipersamakan dengan itu berdasarkan perjanjian bank dengan nasabah yang bersangkutan.

Sedangkan dalam praktek perbankan yang ada di Indonesia, nasabah bank dibedakan menjadi 3 (tiga) yaitu: Pertama, nasabah deposan, yaitu nasabah yang menyimpan dananya pada suatu bank, misalnya dalam bentuk giro, tabungan dan deposito. Kedua, nasabah yang memanfaatkan fasilitas kredit atau pembiayaan, misalnya kredit kepemilikan rumah, pembiayaan murabahah, dan sebagainya. Ketiga, nasabah yang melakukan transaksi dengan pihak lain melalui bank (walk in customer), misalnya nasabah yang melakukan transfer tetapi tidak memiliki rekening di bank tersebut.

1. Perlindungan Terhadap Nasabah Penyimpan Dana Sebagai Kreditur

   Nasabah berkedudukan sebagai Kreditur terhadap bank manakala ia menyalurkan dananya kepada bank dalam bentuk antara lain tabungan, deposito, rekening koran, dan lain-lain. Dari sudut hukum, maka dana ini sudah beralih kepemilikannya kepada bank pada saat dana tersebut diserahkan.

2. Perlindungan Terhadap Nasabah Penyimpan Dana Sebagai Debitur

   Apabila berbicara tentang perlindungan nasabah sebagai Debitur, maka kita tidak bisa melepaskan diri dari pembahasan isi suatu perjanjian kredit. Telah dibahas di awal bahwa hubungan bank dan nasabah antara lain berdasarkan asas kebebasan berkontrak, namun asas kebebasan berkontrak tidaklah bekerja secara tak terbatas. Pembatasan-pembatasan dilakukan dibuat untuk mengingat adanya kepentingan pihak yang lemah bertentangan dengan peraturan-peraturan yang ada.

3. Tindak Pidana

Tindak pidana atau delik berasal dari bahasa Latin *delicta* atau *delictum* yang dikenal dengan istilah *strafbaar feit* dan dalam KUHP (Kitab Undang-Undang hukum Pidana) dengan perbuatan pidana dan peristiwa pidana. Kata *Srafbaar feit* inilah yang melahirkan berbagai istilah yang berbeda-bada dari kalangan ahli hukum sesuai dengan sudut pandang yang berbeda pula[15]. Menurut K. *wantjik* Saleh, ada enam iatilah yang tercipta dalam behasa Indonesia untuk menerjemahkan istilah *"starfbaar feit"* atau "delik" itu yaitu:

1. Perbuatan yang boleh di hukum
2. Peristiwa pidana
3. Pelanggaran pidana
4. Perbuatan pidana
5. Tindak pidana

Tindak pidana merupakan perbuatan yang dilakukan oleh seseorang dangan melakukan suatu kejahatan atau pelanggaran pidana yang merugikan kepentingan orang lain atau merugikan kepentingan umum. Menurut Vos, tindak pidana adalah suatu kelakuan pada umumnya dilarang dengan ancaman pidana. Menurut Moeljatno, perbuatan pidana adalah perbutan yang dilarang oleh suatu aturan hukum, larangan mana disertai ancaman (sanksi) yang berupa pidana tertentu, bagi barang siapa yang melanggar lapangan tersebut[16].

---

[15] Tri Andrisman, Hukum Pidana, Asas-asas dan Dasar Aturan Umum Hukum Pidana Indonesia, Universitas Lampung 2005, hlm, 53

[16] Ibid.

Menurut Pompe, tindak pidana secara teoritis dapat dirumuskan sebagai "suatu pelanggaran norma (gangguan terhadap tertib hukum) yang dengan sengaja atau tidak sengaja telah dilakukan oleh seorang pelaku, dimana penjatuhan hukuman terhadap pelaku tersebut adalah perlu demi terpeliharanya tertib hukum dan terjaminnya kepentingan umum". Selanjutnya dikatakan oleh Pompe bahwa menurut hukum positif kita, suatu tindak pidana itu sebenarnya adalah tidak lain daripada suatu tindakan yang menurut suatu rumusan undang-undang telah dinyatakan sebagai suatu tindakan yang dapat dihukum.

Simons merumuskan tindak pidana adalah suatu tindakan yang melanggar hukum yang dilakukan dengan sengaja atau tidak dengan sengaja oleh seseorang yang dapat dipertanggungjawabkan atas tindakannya dan yang oleh undang-undang telah dinyatakan sebagai suatu tindakan yang dapat dihukum. Menurut Simons tindak pidana itu dirumuskan seperti diatas adalah karena:

1. Untuk adanya suatu tindak pidana disyaratkan bahwa harus terdapat suatu tindakan yang dilarang ataupun diwajibkan oleh undang-undang, dimana pelanggaran terhadap larangan atau kewajiban semacam itu telah dinyatakan sebagai suatu tindakan yang dapat dihukum
2. Agar suatu tindakan itu dapat dihukum, maka tindakan itu harus memenuhi semua unsur dari delik seperti yang dirumuskan di dalam undang-undang
3. Setiap tindak pidana sebagai pelanggaran terhadap larangan atau kewajiban menurut undang-undang itu, pada hakikatnya merupakan suatu tindakan melawan hukum

Moeljatno, yang berpendapat bahwa pengertian tindak pidana menurut istilah beliau yakni perbuatan pidana adalah:

"Perbuatan yang dilarang oleh suatu aturan hukum larangan mana disertai ancaman (sanksi) yang berupa pidana tertentu, bagi barang siapa melanggar larangan tersebut".

Pendapat tersebut di atas pengertian dari tindak pidana yang dimaksud adalah bahwa perbuatan pidana atau tindak pidana senantiasa merupakan suatu perbuatan yang tidak sesuai atau melanggar suatu aturan hukum atau perbuatan yang dilarang oleh aturan hukum yang disertai dengan sanksi pidana yang mana aturan tersebut ditujukan kepada perbuatan sedangkan ancamannya atau sanksi pidananya ditujukan kepada orang yang melakukan atau orang yang menimbulkan kejadian tersebut[17].

Sehubungan dengan hal pengertian tindak pidana ini Bambang Poernomo, berpendapat bahwa perumusan mengenai perbuatan pidana akan lebih lengkap apabila tersusun sebagai berikut:[18]

"Bahwa perbuatan pidana adalah suatu perbuatan yang oleh suatu aturan hukum pidana dilarang dan diancam dengan pidana bagi barang siapa yang melanggar larangan tersebut."

Jika kita berusaha untuk menjabarkan suatu rumusan delik kedalam unsur-unsurnya, maka mula-mula yang dapat kita jumpai adalah disebutkannya suatu tindakan manusia, dengan tindakan itu seorang telah melakukan suatu tindakan

[17] Moeljatno, Asas-asas Hukum Pidana, Bina Aksara, Jakarta, 1987, hlm 54
[18] Bambang Poernomo,. Asas-asas Hukum Pidana, Ghalia Indonesia, Jakarta, 1992, hlm 130

yang terlarang oleh undang-undang. Setiap tindak pidana yang terdapat didalam kitab undang-undang hukum pidana (KUHP) pada umumnya dapat kita jabarkan kedalam unsur-unsur yang pada dasarnya dapat kita bagi menjadi dua macam unsur, yakni unsur subyektif dan unsur objektif[19].

Dari beberapa pengertian tindak pidana tersebut, melihat adanya sesuatu yang dilarang oleh hukum pidana dan ada orang yang melakukan perbuatan tersebut. Maka, pengertian tindak pidana ini dapat dilihat dari dua segi, yaitu[20]:

1. Segi Perbuatannya Perbuatan adalah perbuatan yang melawan hukum, dalam arti formil (suatu perbuatan yang dilarang dan diancam dengan hukuman oleh undang-undang; merupakan unsur tertulis dalam suatu delik pidana) dalam arti materiil (tidak secara tegas dilarang dan diancam dengan undang-undang; merupakan unsur tidak tertulis yang didasarkan pada ketentuan-ketentuan yang tidak tertulis yang hidup dimasyarakat, seperti asas-asas umum yang berlaku).
2. Segi Orangnya

   Orang harus mempunyai kesalahan dan dapat dipertanggung jawabkan. Semua Tindak pidana mempunyai persamaan sifat. Istilah Tindak dari tindak pidana adalah merupakan singkatan dari Tindakan atau Petindak, artinya ada orang yang melakukan suatu tindakan, sedangkan orang yang melakukan itu dinamakan Petindak. Sesuatu tindakan dapat dilakukan oleh siapa saja tetapi dalam banyak hal sesuatu tindakan tertentu hanya mungkin dilakukan oleh

[19] Lamintang, Dasar-dasar Hukum Pidana Indonesia, PT Citra Aditya Bhakti, Bandung, 1997 hlm 193

[20] Abdoel Djamail, R, Pengantar Hukum Indonesia, Edisi Revisi, Raja Grafindo persada, Jakarta, 2006, hlm 175

seseorang dari yang bekerja pada negara atau pemerintah, atau orang yang mempunyai suatu keahlian tertentu. Sesuatu tindakan yang dilakukan itu haruslah bersifat melawan hukum, dan tidak terdapat dasar-dasar atau alasan-alasan yang meniadakan sifat melawan hukum dari tindakan tersebut. Setiap tindakan yang bertentangan dengan hukum atau tidak sesuai dengan hukum, tidak disenangi oleh orang atau masyarakat, yang baik langsung maupun yang tidak langsung terkena tindakan tersebut.

Tindak pidana adalah pelanggaran norma-norma dalam tiga bidang hukum lain, yaitu Hukum Perdata, Hukum Ketatanegaraan, dan Hukum Tata Usaha Pemerintah, yang oleh pembentuk undang-undang ditanggapi dengan suatu hukum pidana, maka sifat-sifat yang ada dalam suatu tindak pidana adalah sifat melanggar hukum, karena tidak ada suatu tindak pidana tanpa sifat melanggar hukum[21]. Adapun unsur-unsur tindak pidana adalah sebagai berikut:

1. Objektif, yaitu suatu tindakan (perbuatan) yang bertentangan dengan hukum dan mengindahkan akibat yang oleh hukum dilarang dengan ancaman hukum. Yang dijadikan titik utama dari pengertian objektif disini adalah tindakaknya.

2. Subjektif, yaitu perbuatan seseorang yang berakibat tidak dikehendaki oleh undang-undang, Sifat unsur ini mengutamakan adanya pelaku (seseorang atau beberapa orang)

Pada umumnya untuk menyelesaikan setiap tindakan yang sudah dipandang merugikan kepentingan umum di samping kepentingan

[21] Wirjono Prodjodikro, Asas-asas Hukum pidana, Ghalia Indonesia Jakarta 2002 hlm 45

perseorangan, dikehendaki turunnya penguasa, dan jika penguasa tidak turun tangan maka tindakan-tindakan tersebut akan menjadi sumber kekacauan yang tidak akan habis-habisnya. Suatu Tindak Pidana yang dilakukan oleh seseorang yang menurut kehendaknya dan merugikan kepentingan umum atau masyarakat termasuk kepentingan perseorangan, lebih lengkapnya harus ternyata bahwa tindakan tersebut terjadi pada suatu tempat, waktu dan keadaan yang ditentukan. Artinya, dipandang dari sudut tempat, tindakan itu harus terjadi pada suatu tempat dimana ketentuan pidana Indonesia berlaku, dipandang dari sudut waktu, tindakan itu masih dirasakan sebagai suatu tindakan yang yang perlu diancam dengan pidana, dan dari sudut keadaan, tindakan itu harus terjadi pada suatu keadaan dimana tindakan itu dipandang sebagai tercela[22].

Penerapan unsur-unsur tindak pidana seperti yang telah dituliskan di atas maka unsur- unsur tindak pidana atau delik sangatlah membantu dalam kebutuhan praktek, perumusan seperti itu sangatlah memudahkan pekerjaan penegak hukum, baik sebagai peserta-pemain (medespleger) maupun sebagai peninjau (toeschouwer). Apakah suatu peristiwa telah memenuhi unsur-unsur delik yang dirumuskan dalam pasal undang-undang, maka diadakanlah penyesuaian atau pencocokan (bagian-bagian/kejadian-kejadian) dari peristiwa tersebut kepada unsur-unsur dan delik yang didakwakan, dalam hal ini unsur-unsur dari delik tersebut disusun terlebih dahulu seperti tersebut di atas. Dengan demikian sering didengar bahwa penggunaan istilah perbuatan pidana dengan

[22] Lili Rasjidi Ira Thania Rasjidi. Dasar-Dasar Filsafat dan Teori Hukum Citra Aditya Bakti, Bandung, 2007. hlm 66-67

pengertiannya sebagai aliran/teori dualisme, sedangkan penggunaan istilah tindak pidana dengan pengertiannya sebagai aliran/teorimonisme.

4. Hak Asasi Manusia

Pembahasan tentang hak asasi manusia, secara komprehensif merupakan bagian yang konstitusional dalam konteks sistem pemerintahan dan kenegaraan Indonesia. Sebagaimana yang dijelaskan oleh Prof. Jimly Asshiddiqie, bahwa Indonesia harus memiliki konstitusi yang demokratis dan melakukan supremasi hak asasi manusia maupun hak asasi warga negara sebagai konsekuensi atas diberlakukannya sistem negara hukum yang demokratis dan negara demokrasi yang berlandaskan atas supremasi hukum[23]. Dalam pandangan yang lebih komprehensif, Padmo Wahjono menegaskan bahwa negara hukum Pancasila yang berasaskan kekeluargaan menegasikan bahwa penghargaan atas hakikat dan martabat rakyat banyak merupakan suatu keharusan yang penting untuk diberlakukan[24]. Hak asasi manusia secara harfiah dapat dipahami, sebagai suatu pemberian dari Tuhan Yang Maha Esa dan melekat secara kodrati kepada manusia yang tanpanya manusia tidak akan mampu untuk menjalani kehidupan sebagai seorang manusia yang bertanggungjawab[25]. Dalam Pasal 1 ayat (1) Undang-Undang Nomor 39 Tahun 1999 Tentang Hak Asasi Manusia, dijelaskan bahwa yang dimaksud dengan hak asasi manusia adalah seperangkat hak yang melekat

[23] Jimly Asshiddiqie, *Hukum Tata Negara dan Pilar-Pilar Demokrasi,* (Jakarta: Konstitusi Press, 2005), hal. XIV.

[24] Rosmery Elsye, *op.cit*, hal. 13.

[25] Serlika Aprita dan Yonani Hasyim, *Hukum dan Hak Asasi Manusia*, (Bogor: Mitra Wacana Media, 2020), hal. 6.

pada hakikat dan keberadaan manusia sebagai mahkluk Tuhan Yang Maha Esa dan merupakan anugerah-Nya yang wajib dihormati, dijunjung tinggi dan dilindungi oleh negara, hukum, Pemerintah, dan setiap orang demi kehormatan serta perlindungan harkat dan martabat manusia.

Sehingga secara sederhana, hak asasi manusia (HAM) adalah paradigm yang memandang manusia sebagai mahkluk Tuhan dengan derajat kehormatan yang sama tingginya[26]. Dalam pemahaman yang lebih komprehensif, maka kebebasan dan hak atau privasi merupakan dua substansi yang menyusun hak asasi manusia[27]. Terkait aspek kebebasan, John Locke membagi kebebasan dalam dua perspektif berikut:[28]

a. Kebebasan alamiah (*natural liberty*) adalah kebebasan dari berbagai aturan yang ada, yang artinya tidak tunduk pada hukum manampun dan hanya tunduk kepada hukum kodrat (alam) sebagai norma utama dalam hidupnya.
b. Kebebasan masyarakat (*civil liberty*) adalah kebebasan atas kekuasaan manapun dan hanya akan tunduk kepada kekuasaan yang berdasarkan atas persetujuan diri sendiri.

C. Originalitas Penelitian

1. Meslik Anin. Perlindungan Hukum Terhadap Nasabah Bank Korban *Cyber crime* Dalam Internet Banking Berdasarkan Undang-Undang Nomor 11

[26] Marcheyla Sumera, "Perbuatan Kekerasan / Pelecehan Seksual Terhadap Perempuan", *Lex et Socieatis Vol. 1 No. 2* (2013) : 44.

[27] Nico Syukur Dister, *Filsafat Kebebasan*, (Yogyakarta: Kanisius, 1991), hal. 183.

[28] Sunarso, *Pendidikan Hak Asasi Manusia (Buku Pegangan Kuliah),* (Surakarta: CV. Indotama Solo, 2020), hal. 16.

Tahun 2008 Tentang Informasi dan Transaksi Elektronik. *Jurnal Iustitia Omnibus Vol. 1 No. 2* (2020). Internet selain memberi manfaat juga menimbulkan ekses negatif dengan terbukanya peluang penyalahgunaan teknologi tersebut. Hal itu terjadi pula untuk data dan informasi yang dikerjakan secara elektronik. Dalam jaringan komputer seperti internet, masalah kriminalitas menjadi semakin kompleks karena ruang lingkupnya yang luas. Kriminalitas di internet atau *cyber crime* pada dasarnya merupakan suatu tindak pidana yang berkaitan dengan cyber space, baik yang menyerang fasilitas umum di dalam cyber space ataupun kepemilikan pribadi. Secara garis besar kejahatan-kejahatan yang terjadi terhadap suatu sistem atau jaringan komputer dan yang menggunakan komputer sebagai instrumen delicti, juga dapat terjadi di dunia perbankan. Sehubungan dengan hal tersebut di atas ada beberapa permasalahan yang menarik untuk dikaji antara lain bagaimanakah perlindungan hukum terhadap nasabah bank yang mengalami *cyber crime* dalam internet banking serta bagaimanakah pembuktian dalam *cyber crime* di bidang perbankan dihubungkan dengan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik ? Pendekatan pembahasan tesis ini penulis menggunakan metode penelitian yuridis normatif yang bertujuan untuk mencari asas-asas dan dasar-dasar falsafah hukum positif, serta menemukan hukum secara in-concreto. Spesifikasi penelitian ini deskriptif analitis, yaitu tidak hanya menggambarkan permasalahan saja, melainkan juga menganalisis melalui peraturan yang berlaku dalam hukum pidana.

Teknik pengumpulan data dilakukan melalui studi kepustakaan serta penelitian lapangan untuk mengumpulkan data primer dan sekunder. Hasil penelitian menyimpulkan Perlindungan hukum bagi nasabah pengguna layanan internet banking mutlak diperlukan seperti halnya perlindungan yang diberikan kepada nasabah penyimpan dana lainnya. Perlindungan hukum bagi nasabah ada yang berdasarkan ketentuan administratif dan berdasarkan jaminan asuransi deposito. Jaminan perlindungan bagi nasabah sangat diperlukan untuk memberikan kepastian hukum bagi nasabah dikemudian hari bilamana bank mengalami kegagalan dalam sistem keamanan. Kemudian Informasi elektronik dan Dokumen Elektronik dapat dijadikan sebagai alat bukti yang sah menurut undang-undang tentang Teknologi Informasi dan Transaksi Elektronik, walaupun sulit untuk diklasifikasikan termasuk alat bukti yang sah sebagaimana dimaksud Pasal 184 ayat (1) KUHAP. Informasi Elektronik dan/atau Dokumen Elektronik dinyatakan sah apabila menggunakan Sistem Elektronik12 sesuai ketentuan yang diatur dalam UU ITE.

2. Khairil Aswan Harahap. Perlindungan Hukum Nasabah Bank dalam *Cyber crime* Terhadap Internet Banking Dikaitkan dengan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Tesis 2009. Teknologi Informasi dan Komunikasi (TIK) telah memberikan peluang untuk terjadinya kejahatan-kejahatan baru (*cyber crime*). "Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Lembaran Negara Republik Indonesia Tahun 2008

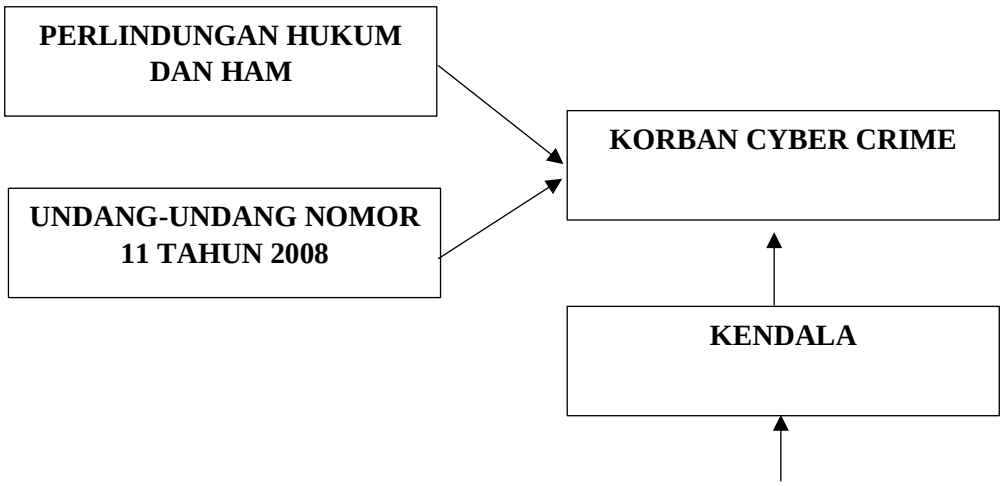
Nomor 58, dan Tambahan Lembaran Negara Republik Indonesia Nomor 4843", ("Selanjutnya disebut dengan UU ITE") adalah wujud dari tanggung jawab yang harus diemban oleh negara yang memberikan perlindungan maksimal pada seluruh aktivitas pemanfaatan TIK dalam kehidupan berbangsa dan bernegara. Kepastian hukum yang kuat akan membuat seluruh aktivitas pemanfaatan TIK di dalam negeri terlindungi dengan baik dari potensi kejahatan dan penyalahgunaan teknologi. Sebagai "rezim hukum baru" dalam khazanah peraturan perundang-undangan RI, UU ITE yang terdiri dari 13 Bab dan 54 Pasal menganut "asas yurisdiksi ekstra territorial", asas kebebasan memilih teknologi atau netral teknologi, dengan cakupan materi antara lain: pengakuan informasi dan/ atau dokumen elektronik sebagai alat bukti hukum yang sah, pengakuan atas tanda tangan elektronik, penyelenggaraan sertifikasi elektronik dan sistem elektronik; nama domain, hak kekayaan intelektual dan perlindungan hak pribadi; perbuatan yang dilarang serta ketentuan pidananya. Adapun permasalahan yang akan dibahas dalam tesis ini adalah: bagaimanakah pengaturan internet banking di Indonesia, bagaimanakah bentuk *cyber crime* di bidang perbankan, bagaimanakah perlindungan hukum nasabah bank dalam *cyber crime* terhadap internet banking dikaitkan dengan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Metode yang digunakan dalam penelitian ini adalah yuridis normatif. Metode penelitian normatif disebut juga sebagai penelitian doktrinal (doctrinal research) yaitu suatu penelitian yang menganalisis hukum baik yang tertulis di dalam buku

(law as it is written in the book), maupun hukum yang diputuskan oleh hakim melalui proses pengadilan (law it is decided by the judge through judicial process). Dalam rangka aplikasi dan perdagangan secara elektronik, UU ITE yang kini telah menjadi landasan hukumnya, serta diharapkan berjalan ke arah pemanfaatan yang bertanggung jawab dan melahirkan manfaat yang sebesar- besarnya bagi pencapaian kesejahteraan bersama. Perlu segera diupayakan sosialisasi cyber law di Indonesia yang akan sangat menunjang pemanfaatan teknologi informasi di berbagai bidang secara bertanggung jawab dan Perlu adanya perubahan terhadap hukum pembuktian yang ada agar dapat menjangkau dan menjawab persoalan atau masalah yang terjadi di dunia maya.

3. I Made Adi Medhaya Putra dan Anak Agung Ngurah Wirasila. Perlindungan Hukum Atas Hak Nasabah Bank Sebagai Konsumen Layanan Internet Banking Dari Ancaman Cybercrime. Jurnal Kertha Wicara Vol. 9 No. 4 (2020). Tujuan penulisan jurnal ini untuk mengkaji pengaturan tentang perlindungan hukum pengguna aplikasi internet banking di Indonesia berdasarkan hukum positif dan tanggung jawab bank dalam memberikan perlindungan hukum bagi pengguna aplikasi Internet Banking dari ancaman cybercrime. Penulisan jurnal ini menggunakan metode penelitian hukum normatif yang berdasarkan atas asas-asas hukum serta penelitian hukum empiris digunakan dengan tujuan untuk mempelajari saja tidak bersifat non-doktrinal. Pasal 28G ayat (1) UUD 1945 dapat dijadikan sebagai aturan dasar untuk menjamin perlindungan data pribadi nasabah

bank pengguna aplikasi internet banking. Pasal 28D Ayat (1) UUD 1945 dapat diajdikan acuan atas jaminan perlindungan hukum dan kepastian hukum apabila nasabah bank pengguna aplikasi internet banking didapati ancaman cybercrime. Selain itu, peraturan perundang-undangan lain yang juga dapat dijadikan sebagai payung hukum yaitu Undang-undang Negara Republik Indonesia Nomor 10 Tahun 1998 tentang Perubahan Undang-undang Nomor 7 Tahun 1992 tentang Perbankan, Undang-undang Negara Republik Indonesia Nomor 8 Tahun 1999 tentang Perlindungan Konsumen, dan Undang-undang Negara Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Dan sebaiknya, pihak perbankan bersama-sama dengan pemerintah harus terus megusahakan mengembangkan teknologi serta pengaturan hukum sehingga penggunaan layanan aplikasi internet banking khususnya dapat lebih terjamin kemananan, kenyamanan serta keselamatannya.

D. Kerangka Berpikir



SOLUSI MENGATASI KENDALA

Gambar 4.1
Kerangka Pemikiran

Informasi, Teknologi dan Komunikasi adalah tiga bidang yang mengalami perkembangan cukup signifikan dalam beberapa tahun terakhir. Perkembangan yang terjadi dalam ketiga bidang tersebut, terjadi sebagai suatu konsekuensi atas berlangsungnya revolusi industri 4.0 yang menekankan kecepatan dalam penggunaannya. Sehingga perkembangan yang terjadi dalam ketiga bidang ini, adalah perkembangan yang mengarah pada digitalisasi. Digiitalisasi sendiri, telah menjadi bagian yang tidak terpisahkan dalam kehidupan umat manusia. Hal ini semakin menguat, ketika dunia mengalami pandemi covid-19.

Pandemi covid-19 secara faktual telah berhassil mendigitalisasi banyak aspek dalam kehidupan umat manusia. Meskipun membantu manusia dalam banyak aspek, namun pada faktanya digitalisasi juga memiliki dampak negatif yang tidak kalah besar. Salah satu dampak negatif dari digitalisasi yang terjadi, adalah munculnya tindak *cyber crime* dalam tindak internet banking. Hal inilah yang kemudian menjadi suatu perhatian khusus dari Pemerintah, dalam aspek perlindungan hukum dan hak asasi manusia (HAM) terhadap nasabah bank. Perlindungan hukum dan hak asasi manusia (HAM) terhadap nasabah bank menjadi urgensi yang penting, sebagai realisasi atas asas demokrasi hukum Indonesia.

BAB III

METODE PENELITIAN

A. Jenis Penelitian

Penelitian ini merupakan penelitian *field reasearch* dengan jenis penelitian deskriptif, penelitian yang berusaha mendeskripsikan suatu gejala, peristiwa, kejadian yang terjadi saat sekarang. Penelitian deskriptif memusatkan perhatian kepada masalah-masalah actual sebagaimana adanya pada saat penelitian berlangsung yaitu penelitian yang menggambarkan atau menjelaskan serta memberi data sedetail mungkin mengenai permasalahan yang terjadi mengenai perlindungan hukum terhadap nasabah bank korban *cyber crime* dalam internet banking berdasarkan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik [29]

B. Metode Pendekatan

Peneitian ini menggunakan pendekatan hukum normatif/doctrinal karena menggunakan konsep hukum yaitu norma – norma di dalam sistem perundang – undangan hukum nasional.

C. Lokasi Penelitian

Penelitian ini dilaksanakan dalam wilayah hukum Kepolisian Resor Kota Besar Semarang (Polrestabes) Semarang.

[29] Soerjono Soekanto, *Pengantar Penelitian Hukum*, Universitas Indonesia - Press, Jakarta hlm 74

D. Sumber dan Jenis Data

1. Data Primer

   Keterangan yang secara langsung dari narasumber atau subyek penelitian.

2. Data Sekunder

   Keterangan-keterangan yang diperoleh dari bahan-bahan kepustakaan, dalam hal ini mengacu pada literature, perundang-undangan, dengan penyusunan penelitian ini yang kemudian dibedakan menjadi:

   1) Bahan hukum Primer

      Bahan hukum primer adalah bahan-bahan hukum yang diperoleh dari perundang-undangan.

   2) Bahan Hukum Sekunder

      Bahan hukum sekunder adalah bahan-bahan yang memberikan penjelasan mengenai bahan hukum primer.

   3) Bahan Hukum Tersier

      Bahan hukum tersier adalah bahan yang memberikan petunjuk maupun penjelasan bahan hukum primer dan sekunder. Seperti, kamus hukum dan ensikopledia.

E. Subyek Penelitian

Subjek penelitian atau responden adalah pihak-pihak yang dijadikan sebagai sampel dalam sebuah penelitian. Subjek penelitian juga membahas karakteristik subjek yang digunakan dalam penelitian, termasuk penjelasan mengenai populasi, sampel dan teknik sampling yang digunakan.

F. Teknik Pengumpulan Data

1. Wawancara yaitu suatu acara memperoleh informasi langsung dari nara sumber. Wawancara adalah kegiatan tanya-jawab secara lisan untuk memperoleh informasi. Bentuk informasi yang diperoleh dinyatakan dalam tulisan, atau direkam secara audio, visual, atau audio visual. Wawancara merupakan kegiatan utama dalam kajian pengamatan. Pelaksanaan wawancara dapat bersifat langsung maupun tidak langsung.
2. Studi pustaka juga berarti teknik pengumpulan data dengan melakukan penelaahan terhadap buku, literatur, catatan, serta berbagai laporan yang berkaitan dengan masalah yang ingin dipecahkan.

G. Metode Analisis Data

Data yang diperoleh dari hasil penelitian akan dianalisa dengan menggunakan metode analisis deskriptif yang memaparkan secara jelas. Analisis data merupakan upaya mencari dan menata secara sistematis catatan hasil observasi, wawancara dan lainnya. Analisa ini perlu dilakukan untuk mencari makna. Dalam penelitian kualitatif analisis data dalam praktenya tidak dapat dipisahkan dengan proses pengumpulan data, dan dilanjutkan setelah pengumpulan data selesai. Dengan demkian secara teoritik, analisis dan pengumpulan data dilaksanakan secara berulang-ulang untuk memecahkan masalah.

Dalam penelitian ini peneliti menggunakan analisis deskriptif dengan menerangkan proses berfikir induktif yaitu berangkat dari faktor- faktor khusus, peristiwa-peristiwa yang konkrit kemudian dari faktor-faktor atau

peristiwa yang khusus dan konkrit kemudian itu ditarik generalisasi yang bersifat umum. Adapun teknik analisis data yang akan dilakukan peneliti yaitu:

1. Reduksi data

   Data yang diperoleh di lapangan sebelum dilakukan laporan lengkap dan terperinci disortir dulu, yaitu yang memenuhi fokus penelitian. Dalam mereduksi data, semua data lapangan ditulis sekaligus dianalisis, direduksi, dirangkum, dipilih hal-hal yang pokok, difokuskan pada hal-hal yang penting, dicari tema dan polanya, sehingga disusun secara sistematis dan lebih mudah dikendalikan.

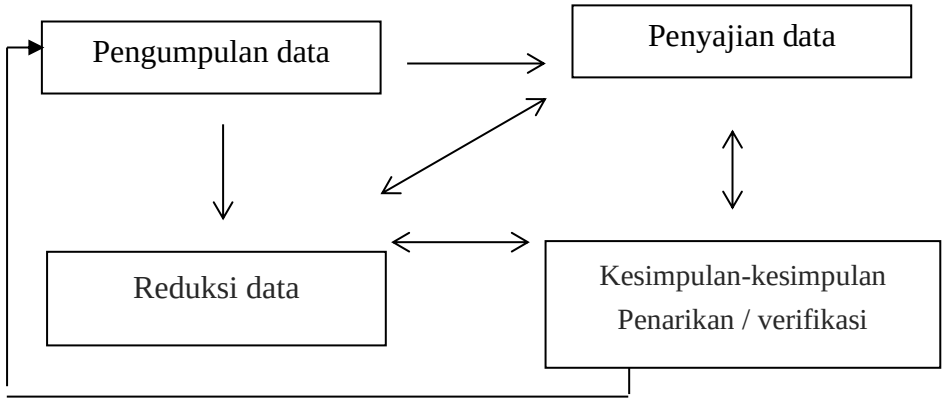
2. Penyajian data

   Dalam penelitian ini peneliti akan menyajikan data dalam bentuk laporan berupa uraian yang lengkap dan terperinci. Ini dilakukan peneliti agar data yang diperoleh dapat dikuasai dengan dipilah secara fisik dan dipilah kemudian dibuat dalam kertas dan bagan.

3. Menarik kesimpulan

   Dalam penelitian ini, setelah dilakukan verifikasi maka akan ditarik kesimpulan yang merupakan hasil dari penelitian ini. Yaitu dengan cara mencari makna fokus penelitian. Peneliti melakukan verifikasi dan menarik kesimpulan guna mencari makna yang terkandung di dalamnya. Pada awalnya kesimpulan yang dibuat bersifat tentatif, kabur, dan penuh keraguan, tetapi dengan bertambahnya data dan pembuatan kesimpulan

demi kesimpulan akan ditemukan data yang dibutuhkan. Berikut adalah "model interaktif" seperti yang dikutip oleh Ibrahim:[30]



Gambar: 3.1

Teknik Analisis Data

[30] *Miles dan Huberman. 1992*. Analisis data Kualitatif. (diterjemahkan oleh: Tjetjep Rohedi Rosidi). Jakarta: Universitas Indonesia

BAB IV

HASIL PENELITIAN DAN PEMBAHASAN

A. Faktor Penyebab Timbulnya Nasabah Bank Menjadi Korban *Cyber crime* Dalam Internet Banking

Internet Banking merupakan layanan yang melalui saluran distribusi Bank untuk melihat rekening nasabah peroragan maupun perusahaan melalui jaringan Internet dan memakai perangkat lunak browser pada komputer maupun perangkat lunak lainnya. Berikut ini merupakan beberapa karakteristik layanan yang dimiliki oleh Internet Banking yaitu:

1. Produk BSM Net Banking (BNB) merupakan suatu layanan transaksi perbankan yang melalui jaringan Internet Banking kemudian masuk ke alamat http://bsmnet.syariahmandiri.co.id/cms/ yang dapat diakses oleh nasabah untuk kepetingan pengecekan informasi, pembayaran tagihan, transfer ke bank lain, pembayaran dan lain-lain.
2. Cara pendaftaran bisa dilakukan di Cash Oulet BSM terdekat/Brach Office/Area
3. Limit standar nasabah perorangan sampai dengan Rp250 juta
4. Limit standar nasabah perusahaan maksimal sampai dengan Rp1 miliar

Kejahatan di dalam e-banking yaitu kejahatan kartu ATM. Kejahatan kartu ATM yang sering terjadi adalah pemalsuan kartu ATM. Pelaku kejahatan membuat kartu ATM palsu lengkap dengan magnetic stripe yang sudah berisi rekaman data dari kartu yang dipalsukan. Selain memalsukan

kartu, pelaku kejahatan juga mengetahui nomor PIN dari kartu yang digandakan/dipalsukan. Pemalsuan atau penggandaan kartu ATM dapat dilakukan karena peralatan yang diperlukan untuk melakukan hal tersebut dapat diperoleh dengan mudah dipasaran. Modus lainnya dari kejahatan kartu ATM adalah membuat kartu ATM fiktif untuk nomor-nomor rekening nasabah yang tidak menginginkan kartu ATM. Pelaku biasanya menggunakan rekening-rekening nasabah yang saldonya besar namun sudah lama tidak ada aktivitas transaksi. Dengan kartu ATM tersebut maka pelaku dengan leluasa menguras isi rekening nasabah yang tidak aktif tersebut. Modus kejahatan ATM lainnya adalah terjadi karena kelalaian pemilik kartu ATM. Seorang pemilik kartu ATM menuliskan nomor PIN pada kartu ATM yang bersangkutan hingga suatu saat kartu ATM tersebut hilang atau dicuri dan digunakan oleh orang yang menemukan atau yang mencuri kartu tersebut.

Contoh cybercrime dalam transaksi perbankan yang menggunakan sarana internet sebagai basis transaksi adalah sistem layanan kartu kredit dan layanan perbankan online (online banking). Dalam sistem layanan yang pertama, yang perlu diwaspadai adalah tindak kejahatan yang dikenal dengan istilah carding. Prosesnya adalah, pelaku carding memperoleh data kartu kredit korban secara tidak sah (illegal interception) dan kemudian menggunakan kartu kredit tersebut untuk berbelanja di toko online (forgery). Modus ini dapat terjadi kemungkinan akibat lemahnya sistem autentifikasi yang digunakan dalam memastikan identitas pemesan barang di toko online.

Faktor penyebab munculnya ancaman serangan phising ketika pengguna menggunakan layanan online banking adalah minimnya pengetahuan pengguna, psikologis, dan privasi social networking services pengguna.

Peristiwa *cyber crime* yang timbul akibat penyalahgunaan data pribadi oleh pihak yang tidak berwenang masih sering terjadi. Dapat kita lihat masih banyak telepon, sms atau email dari seseorang yang tidak kita kenal atau menyamar sebagai pihak dari institusi yang berwenang, menawarkan beraneka ragam tawaran yang menarik bagi calon korban, padahal calon korban tersebut tidak pernah memberikan data pribadi kepada siapapun. Nasabah yang tidak memiliki edukasi yang cukup tentunya akan berpikir bahwa penyalahgunaan data pribadi tersebut berasal dari kebocoran data pribadi nasabah pada bank yang bersangkutan.

Kegiatan phising ini sering terjadi pada pengguna perbankan digital karena menggunakan isian data pengguna dan kata sandi. Ketika nasabah memasukkan isian data dan kata sandi miliknya ke dalam website tiruan tersebut, maka data tersebut akan diketahui oleh phiser tersebut.

Kegagalan sistem dapat disebabkan karena adanya kerusakan sistem (misalnya turunnya jaringan atau server down), dan dalam skala luas bisa disebabkan karena bencana alam. Sementara itu, *cyber crime* juga yang terjadi pada industri perbankan cenderung meningkat. Seperti kejahatan pertama, pharming bisa disebut juga sebagai penipu atau hacker melakukan pengalihan dari situs yang sah ke situs yang palsu tanpa diketahui dan disadari oleh korban, kemudian mengambil data yang dimasukkan oleh

korban sehingga masuk ke dalam area yang menjadi permainan penipu tersebut. Kedua, spoofing kejahatan yang menggunakan perangkat lunak untuk menutupi identitas dengan menampilkan alamat e-mail/ nama/ nomor palsu di komputer agar menyembunyikan identitas. Ketiga, keylogger tersebut menggunakan sofware yang dapat menghafal tombol keyboard yang digunakan tanpa diketahui oleh pengguna. Keempat, phising adalah tindakan memperoleh informasi pribadi seperti User ID, PIN, nomor rekening bank atau nomor kartu redit secara tidak sah. Kelima, sniffing pekerjaan menyadap paket data yang lalu-lalang pada jaringan. Kejahatan-kejahatan tersebut yang sering terjadi pada nasabah yang menggunakan internet banking.

Penggunaan layanan internet banking dapat menyebabkan beberapa faktor yang dapat merugikan pihak nasabah. Faktor utama yang menjadi kelemahan nasabah adalah tingkat kesadaran masyarakat akan haknya masih rendah.Di balik kemudahannya yang didapat dari pengguna internet banking, ada juga resiko yang didapat dalam penggunaan layanan ini yang membuat nasabah berada di posisi lemah, seperti yang sering terjadi saat ini pada kalangan masyarakat yang mengeluh baik dari sisi sistem maupun daripihak bank, seperti rekening pihak nasabah yang berkurang tanpa sepengetahuan mereka, data rahasia pihak nasabah tersebut telah dibajak oleh pihak yang tidak bertanggungjawab, serta pengiriman uang yang telah ditransfer melalui internet banking tidak masuk kepada rekening tujuan.

Ada beberapa kelalaian yang di sengaja dalam bidang perbankan yang dilakukan dengan modus-modus sebagai berikut

a. Membuat atau menyebabkan adanya pencatatan palsu dalam pembukuan atau dalam proses laporan, maupun dalam dokumen atau laporan kegiatan usaha, laporan transaksi atau rekening suatu bank;
b. Menghilangkan atau tidak memasukkan atau menyebabkan tidak dilakukannya pencatatan dalam pembukuan atau dalam laporan, maupun dalam dokumen atau laporan kegiatan usaha, laporan transaksi atau rekening suatu bank;
c. Mengubah, mengaburkan, menyembunyikan, menghapus, atau menghilangkan adanya suatu pencatatan dalam pembukuan atau dalam laporan, maupun dalam dokumen atau laporan kegiatan usaha, laporan transaksi atau rekening suatu bank, atau dengan sengaja mengubah, mengaburkan, menghilangkan, menyembunyikan atau merusak catatan pembukuan tersebut, diancam dengan pidana penjara sekurang-kurangnya 5 (lima) tahun dan paling lama 15 (lima belas) tahun serta denda sekurang- kurangnya Rp. 10.000.000.000,00 (sepuluh miliar rupiah) dan paling banyak Rp. 200.000.000.000,00 (dua ratus miliar rupiah).

Selain itu juga perlindungan hukum yang diberikan oleh Undang- undang ITE dalam hal perlindungan data pribadi, berhubungan dengan hak pribadi nasabah (privasi), menurut Pasal 26 menyatakan bahwa kecuali ditentukan lain oleh Peraturan Perundang-undangan, penggunaan setiap informasi melalui

media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan.

B. Perlindungan Hukum dan Hak Asasi Manusia Terhadap Nasabah Bank Korban *Cyber Crime* dalam Internet Banking

Aturan Yang Melindungi Nasabah Bank Pengguna Internet Banking Dari Acaman Kejahatan Cyber Perkembangan pelayanan jasa-jasa perbankan yang dilakukan melalui internet semakin berkembang seiring dengan pertumbuhan teknologi informasi yang semakin cepat. Masalah keamanan tidak hanya untuk kepentingan nasabah tetapi juga untuk kepentingan bank penyelenggara internet banking itu sendiri maupun industri perbankan secara keseluruhan. Tetapi, masalah keamanan bertransaksi serta perlindungan nasabah menjadi perhatian tersendiri untuk pengembangan internet banking ke depan, terutama karena tidak adanya kepastian hukum bagi nasabah dimana belum terdapat suatu bentuk pengaturan atas kegiatan internet di Indonesia.

Di dalam peraturan hukum Indonesia, belum ada pengaturan perundang-undangan khusus mengatur tentang internet banking di Indonesia, tetapi dapat menemukan peraturan yang berkaitan dengan perlindungan nasabah internet banking dengan cara mengartikan peraturan-peraturan tersebut ke dalam pemahaman tentang internet banking atau mengaitkan peraturan yang satu dengan peraturan yang lainnya. Berikut ini penjelasan mengenai peraturan-peraturan yang terkait dengan pelindungan nasabah pengguna internet banking:

1. Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik Salah satu bentuk implementasi dari yuridiksi untuk menetapkan hukum (yuridiction to enforce) terhadap tindak pidana siber berdasarkan hukum pidana Indonesia adalah pembentukan Undang-Undang ITE (Informasi dan Transaksi Elektronik). Undang-Undang ITE adalah undang-undang yang dibentuk secara khusus untuk mengatur berbagai aktivitas manusia dalam bidang teknologi informasi dan komunikasi termasuk beberapa tindak pidana yang dikategorikan tindak pidana siber. Namun dengan demikian berdasarkan luas lingkup dan kategorisasi tindak pidana siber, disamping UU ITE peraturan perundang-undangan lainnya juga secara eksplisit atau implisit mengatur tentang tindak pidana siber. Kriminalisasi tindak pidana siber dalam peraturan perundang-undangan di Indonesia tersebut memiliki implikasi terhadap upaya pemberantasan tindak pidana siber di Indonesia khususnya dan dunia pada umumnya. Setiap penyelenggara sistem elektronik wajib untuk menyediakan sistem elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya sistem elektronik tersebut sebagaimana mestinya. “Andal” artinya adalah sistem elektronik memiliki kemampuan yang sesuai dengan kebutuhan penggunanya. “Aman” artinya adalah sistem elektronik terlindungi secara fisik maupun non-fisik dalam artian tidak dapat disabotase atau dibobol atau diakses tanpa izin pihak terkait. “Beroperasi sebagaimana mestinya” artinya adalah sistem elektronik memiliki kemampuan sesuai spesifikasinya.

Bertanggung jawab artinya adalah ada subjek hukum yang bertanggung jawab secara hukum terhadap penyelenggaraan sistem elektronik tersebut. Tetapi ketentuan tersebut tidak dapat berlaku dalam hal dapat pembuktian terjadinya keadaan memaksa, kesalahan, dan/atau kelalaian pihak pengguna sistem elektronik. Undang-undang ITE juga mengatur bahwa sepanjang tidak ditentukan lain oleh Undang-undang tersendiri, setiap penyelenggara sistem elektronik wajib mengoperasikan sistem elektronik yang memenuhi persyaratan minimum sebagai berikut, yaitu:

2. Dapat menampilkan kembali informasi elektronik dan/atau dokumen elektronik secara utuh sesuai dengan masa retensi yang ditetapkan dengan peraturan perundang-undangan.
3. Dapat melindungi ketersediaan, keutuhan, keotentikan, kerahasiaan dan keteraksesan informasi elektronik dalam penyelenggaran sistem elektronik tersebut.
4. Dapat beroperasi sesuai dengan prosedur atau petunjuk dalam penyelenggaraan sistem elektronik
5. Dilengkapi dengan prosedur atau petunjuk yang diumumkan dengan bahasa, informasi atau simbol yang dapat dipahami oleh pihak yang bersangkutan dengan penyelenggaraan sistem elektronik.

Memiliki mekanisme yang berkelanjutan untuk menjaga kebaruan, kejelasan dan kebertanggungjawaban prosedur atau produk. Selain itu juga perlindungan hukum yang diberikan oleh Undang- undang ITE dalam hal

perlindungan data pribadi, berhubungan dengan hak pribadi nasabah (privasi), menurut Pasal 26 menyatakan bahwa kecuali ditentukan lain oleh Peraturan Perundang-undangan, penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan.

Upaya perlindungan hukum terhadap pemberi jasa atau pengguna internet telah melahirkan suatu produk hukum dalam bentuk UU ITE, namun dengan lahirnya UU ITE belum semua permasalahan menyangkut masalah ITE dapat tertangani. Dengan lahirnya UU ITE tidak semata-mata undang-undang ini bisa diketahui oleh masyarakat pengguna teknologi informasi dan praktisi hukum. Kemudian berbagai bentuk perkembangan teknologi yang menimbulkan penyelenggaraan dan jasa baru harus dapat diidentifikasikan dalam rangka antisipasi terhadap pemecahan berbagai persoalan teknis yang dianggap baru sehingga dapat dijadikan bahan untuk penyusunan berbagai Peraturan Pelaksanaan. Pengayaan akan bidang-bidang hukum yang sifatnya sektoral (rejim hukum baru) akan makin menambah semarak dinamika hukum yang akan menjadi bagian sistem hukum nasional.

Jaminan perlindungan bagi nasabah sangat diperlukan untuk memberikan kepastian hukum bagi nasabah dikemudian hari bilamana bank mengalami kegagalan dalam sistem keamanan sehingga menyebabkan uang nasabah yang disimpan dalam bank tersebut dicuri oleh para pelaku *cyber crime*. Satu langkah yang dianggap penting untuk menanggulangi keamanan sistem informasi adalah telah diwujudkannya rambu-rambu hukum yang

tertuang dalam UU ITE. Hal yang mendasar dari UU ITE ini sesungguhnya merupakan upaya mengakselerasikan manfaat dan fungsi hukum (peraturan) dalam kerangka kepastian hukum. Penegakan hukum pidana dalam *cyber crime* dapat dilakukan oleh penyidik yang terdiri dari Kepolisian Republik Indonesia dan Penyidik Pegawai Negeri Sipil. Penyidikan dilakukan berdasarkan KUHP dan UU ITE.

Kewenangan Penyidik Pegawai Negeri Sipil dalam rangka memberikan perlindungan hukum terhadap nasabah bank yang mengalami *cyber crime* dalam internet banking tercantum dalam Pasal 43 UU ITE. Perlindungan hukum terhadap nasabah bank yang mengalami *cyber crime* dalam internet banking dihubungkan dengan UU ITE terdapat dalam Pasal 45, Pasal 46, Pasal 47, Pasal 48, Pasal 49, Pasal 50, Pasal 51 UU ITE. Namun menurut hemat penulis, ketentuanketentuan yang terdapat di dalam UU ITE masih memerlukan penjabaran yang relevan, misalnya ketentuan yang diatur dalam Bab VII Pasal 27 sampai dengan Pasal 37 UU ITE mengenai perbuatan yang dilarang, semua pasal tersebut menggunakan kalimat setiap orang. Padahal perbuatan yang dilarang, seperti spam, penipuan, cracking, virus, dan flooding sebagian besar akan dilakukan oleh mesin oleh program bukan langsung oleh manusia.

Menurut sistem perbankan Indonesia, perlindungan terhadap nasabah dapat dilakukan melalui dua metode, yaitu perlindungan secara eksplisit (explicit deposit protection) yaitu perlindungan yang diperoleh melalui pembentukan lembaga yang menjamin simpanan masyarakat, sebagaimana

diatur dalam Keputusan Presiden No. 26 Tahun 1998 tentang Jaminan terhadap Kewajiban Bank Umum. Sehingga apabila bank mengalami kegagalan, maka lembaga tersebut akan mengganti dan masyarakat yang disimpan dalam bank yang gagal tersebut.

Hal ini diatur dalam Keputusan Presiden No. 26 Tahun 1998 tentang Jaminan terhadap Kewajiban Bank Umum, sebelum diberlakukannya asuransi deposito. Perlindungan secara implisit (implicit deposit protection) yaitu perlindungan yang dihasilkan oleh pengawasan dan pembinaan bank secara efektif. Maksudnya agar dapat menghindari terjadinya kebangkrutan bank yang diawasi. Perlindungan semacam ini dapat diperoleh melalui peraturan perundang-undangan di bidang ITE dan perbankan. Perlindungan yang dihasilkan oleh pengawasan dan pembinaan yang efektif, yang dilakukan oleh Bank Indonesia.

Berdasarkan Pasal 3 UndangUndang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik menyatakan bahwa:

> *"Pemanfaatan Teknologi Informasi dan Transaksi Elektronik dilaksanakan berdasarkan asas kepastian hukum, manfaat, kehatihatian, itikad baik, dan kebebasan memilih teknologi atau netral teknologi."*

Sedangkan berdasarkan Pasal 4 Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, Pemanfaatan Teknologi Informasi dan Transaksi Elektronik dilaksanakan dengan tujuan untuk:

1. Mencerdaskan kehidupan bangsa sebagai bagian dari masyarakat informasi dunia;
2. Mengembangkan perdagangan dan perekonomian nasional dalam rangka meningkatkan kesejahteraan masyarakat;
3. Meningkatkan efektivitas dan efisiensi pelayanan publik;
4. Membuka kesempatan seluas-luasnya kepada setiap orang untuk memajukan pemikiran dan kemampuan di bidang penggunaan dan pemanfaatan Teknologi Informasi seoptimal mungkin dan bertanggung jawab; dan
5. Memberikan rasa aman, keadilan, dan kepastian hukum bagi pengguna dan penyelenggara Teknologi Informasi. ATM, phone banking, electronic fund transfer, internet banking, mobile phone." Selain itu tercantum dalam pasal 1 ayat (7) yang menyatakan bahwa disaster recovery center (DRC) adalah fasilitas pengganti pada saat Pusat Data (data center) mengalami gangguan atau tidak dapat berfungsi antara lain karena tidak adanya aliran listrik ke ruang komputer, kebakaran, ledakan atau kerusakan pada komputer, yang digunakan sementara waktu selama dilakukannya pemulihan pusat data bank untuk menjaga kelangsungan kegiatan usaha (business continuity). Dasar hukum mengenai transaksi electronic banking khususnya bagi kegiatan perbankan belum ada undang-undang secara khusus yang mengaturnya, namun ketentuan-ketentuan berupa peraturan dan Surat Edaran. Undang-undang No. 11 tahun 2008 tentang ITE telah menjadi payung hukum bagi penyelenggaraan kegiatan transaksi elektronik, yang

diselenggarakan oleh bank. Undang-Undang ITE telah mengatur mengenai tanggung jawab yang fair antara penyelenggara sistem elektronik bank dan nasabah. Memenuhi prinsip hubungan keperdataan nasabah dengan bank, maka bank bertanggung jawab terhadap pelaksanaan penyelenggaraan teknologi informasi yang menggunakan jasa pihak penyedia jasa. Demikian pula pihak penyelenggara jasa tersebut akan terikat dengan segala ketentuan sebagai pihak terkait bank.

Menurut Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Teknologi Elektronik pada Pasal 16 huruf b dan d:

1. Sepanjang tidak ditentukan lain oleh undang-undang tersendiri, setiap Penyelenggara Sistem Elektronik wajib mengoperasikan Sistem Elektronik yang memenuhi persyaratan minimum
2. Dapat melindungi ketersediaan, keutuhan, keotentikan, kerahasiaan, dan keteraksesan Informasi Elektronik dalam Penyelenggaraan Sistem Elektronik tersebut
3. Dilengkapi dengan prosedur atau petunjuk yang diumumkan dengan bahasa, informasi, atau symbol yang dapat dipahami oleh pihak yang bersangkutan dengan Penyelenggaraan Sistem Elektronik tersebut. Kerahasian sebuah informasi merupakan bukan hanya diatur dalam sistem perbankan untuk menjaga informasi atas data nasabah tetapi di dalam UU ITE sebagaimana yang diatur untuk melindungi suatu kerahasiaan yang menyangkut data nasabah yang dilakukan oleh penyelenggara elektronik

Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik Salah satu bentuk implementasi dari yuridiksi untuk menetapkan hukum (yuridiction to enforce) terhadap tindak pidana siber berdasarkan hukum pidana Indonesia adalah salah satu pembentukan Undang-undang ITE. Undang-undang ITE merupakan Undang-undang yang dibentuk khusus untuk mengatur berbagai aktivitas manusia dibidang teknologi informasi dan komunikasi termasuk beberapa tindak pidana yang dikategorikan tindak pidana siber. Namun demikian berdasarkan luas lingkup dan kategorisasi tindak pidana siber, disamping UU ITE peraturan perundang-undangan lainnya juga secara eksplisit atau implisit mengatur tindak pidana siber.

Kriminalisasi tindak pidana siber dalam peraturan perundangundangan Indonesia tersebut memiliki implikasi terhadap upaya pemberantas tindak pidana siber di Indonesia khususnya dan dunia pada umumnya. 15 Undang-undang Nomor 11 Tahun 2008 tentang ITE yang disahkan pada tanggal 21 April 2008 dinilai telah cukup mampu mengatur permasalahan-permasalahan hukum dari sistem Internet banking sebagai salah satu layanan perbankan yang merupakan wujud perkembangan teknologi informasi. Kendala seperti aspek teknologi dan aspek hukum bukan lagi menjadi faktor penghambat perkembangan Internet banking di Indonesia, meskipun dalam pasal-pasal Undang-undang ITE tidak ada pasal-pasal yang spesifik mengatur mengenai Internet Banking itu sendiri, akan tetapi terdapat pasal-pasal yang mengatur mengenai transaksi dengan media Internet.

Setiap penyelenggara sistem elektronik diwajibkan untuk menyediakan sistem elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya sistem elektronik sebagaimana mestinya. "Andal" artinya sistem elektronik memiliki kemampuan yang sesuai dengan kebutuhan penggunanya. "Aman" artinya sistem elektronik terlindungi secara fisik maupun nonfisik. "Beroperasi sebagaimanal mestinya" artinya sistem elektronik memiliki kemampuan sesuai dengan spesifikasinya. Selain itu, penyelenggaraan sistem elektroniknya." "Bertanggung jawab" artinya ada subjek hukum yang bertanggung jawab secara hukum terhadap penyelenggaraan. sistem elektronik tersebut.

Namun demikian ketentuan tersebut tidak berlaku dalam hal dapat dibuktikan terjadinya keadaan memaksa, kesalahan, dan/atau kelalaian pihak pengguna sistem elektronik. bahwa sepanjang tidak ditentukan lain oleh Undang-undang tersendiri, setiap penyelenggara sistem elektronik wajib mengoperasikan sistem elektronik yang memenuhi persyaratan minimum sebagai berikut[19], yaitu:

1. Dapat menampilkan kembali informasi elektronik dan/atau dokumen elektronik secara utuh sesuai dengan masa retensi yang ditetapkan dengan peraturan perundang-undangan.
2. Dapat melindungi ketersediaan, keutuhan, keotentikan, kerahasiaan dan keteraksesan informasi elektronik dalam penyelenggaran sistem elektronik tersebut.

3. Dapat beroperasi sesuai dengan prosedur atau petunjuk dalam penyelenggaraan sistem elektronik.
4. Dilengkapi dengan prosedur atau petunjuk yang diumumkan dengan bahasa, informasi atau simbol yang dapat dipahami oleh pihak yang bersangkutan dengan penyelenggaraan sistem elektronik.
5. Memiliki mekanisme yang berkelanjutan untuk menjaga kebaruan, kejelasan dan kebertanggungjawaban prosedur atau produk.

Perkembangan teknologi informasi saat ini memungkinkan bahwa keamanan privasi data pribadi nasabah yang menggunakan layanan perbankan melalui media internet kurang terjamin. Hal ini dikarenakan masih banyak kelemahan dalam mengantisipasi berbagai pelanggaran atau penyalahgunaan dari media internet yang berdampak kerugian berbagai pihak. Ada juga beberapa pengaturan perbuatan yang dilarang dan dikenai sanksi pidana, yaitu sebagai berikut:

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 yang 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 penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp.800.000.000,00 (delapan ratus juta rupiah).
4. Setiap orang yang memenuhi unsur sebagaimana yang dimaksud dalam Pasal 31 Ayat (1) dan Ayat (2) dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp.800.000.000,00 (delapan ratus juta rupiah).

Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik Salah satu bentuk implementasi dari yuridiksi untuk menetapkan hukum (yuridiction to enforce) terhadap tindak pidana siber berdasarkan hukum pidana Indonesia adalah salah satu pembentukan Undang-undang ITE. Undang-undang ITE merupakan Undang-undang yang dibentuk khusus untuk mengatur berbagai aktivitas manusia dibidang teknologi informasi dan komunikasi termasuk beberapa tindak pidana yang dikategorikan tindak pidana siber.

Namun demikian berdasarkan luas lingkup dan kategorisasi tindak pidana siber, disamping UU ITE peraturan perundang-undangan lainnya juga secara eksplisit atau implisit mengatur tindak pidana siber. Kriminalisasi tindak pidana siber dalam peraturan perundangundangan Indonesia tersebut memiliki implikasi terhadap upaya pemberantas tindak pidana siber di Indonesia khususnya dan dunia pada umumnya. 15 Undang-undang Nomor 11 Tahun 2008 tentang ITE yang disahkan pada tanggal 21 April 2008 dinilai telah cukup mampu mengatur permasalahan-permasalahan hukum dari sistem

Internet banking sebagai salah satu layanan perbankan yang merupakan wujud perkembangan teknologi informasi.

Kendala seperti aspek teknologi dan aspek hukum bukan lagi menjadi faktor penghambat perkembangan Internet banking di Indonesia, meskipun dalam pasal-pasal Undang-undang ITE tidak ada pasal-pasal yang spesifik mengatur mengenai Internet Banking itu sendiri, akan tetapi terdapat pasal-pasal yang mengatur mengenai transaksi dengan media Internet. Setiap penyelenggara sistem elektronik diwajibkan untuk menyediakan sistem elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya sistem elektronik sebagaimana mestinya. 16 “Andal” artinya sistem elektronik memiliki kemampuan yang sesuai dengan kebutuhan penggunanya. “Aman” artinya sistem elektronik terlindungi secara fisik maupun nonfisik. “Beroperasi sebagaimana mestinya” artinya sistem elektronik memiliki kemampuan sesuai dengan spesifikasinya.

Selain itu, penyelenggaraan sistem elektroniknya. 17 “Bertanggung jawab” artinya ada subjek hukum yang bertanggung jawab secara hukum terhadap penyelenggaraan sistem elektronik tersebut. Namun demikian ketentuan tersebut tidak berlaku dalam hal dapat dibuktikan terjadinya keadaan memaksa, kesalahan, dan/atau kelalaian pihak pengguna sistem elektronik. 18 Undang-undang ITE juga mengatur bahwa sepanjang tidak ditentukan lain oleh Undang-undang tersendiri, setiap penyelenggara sistem elektronik wajib mengoperasikan sistem elektronik yang memenuhi persyaratan minimum sebagai berikut 19 , yaitu :

1. Dapat menampilkan kembali informasi elektronik dan/atau dokumen elektronik secara utuh sesuai dengan masa retensi yang ditetapkan dengan peraturan perundang-undangan.
2. Dapat melindungi ketersediaan, keutuhan, keotentikan, kerahasiaan dan keteraksesan informasi elektronik dalam penyelenggaran sistem elektronik tersebut.
3. Dapat beroperasi sesuai dengan prosedur atau petunjuk dalam penyelenggaraan sistem elektronik.
4. Dilengkapi dengan prosedur atau petunjuk yang diumumkan dengan bahasa, informasi atau simbol yang dapat dipahami oleh pihak yang bersangkutan dengan penyelenggaraan sistem elektronik.
5. Memiliki mekanisme yang berkelanjutan untuk menjaga kebaruan, kejelasan dan kebertanggungjawaban prosedur atau produk. Selain itu juga perlindungan hukum yang diberikan oleh Undang-undang ITE dalam hal perlindungan data pribadi, berhubungan dengan hak pribadi nasabah (privasi), menurut Pasal 26 menyatakan bahwa kecuali ditentukan lain oleh Peraturan Perundang-undangan, penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan. Perkembangan teknologi informasi saat ini memungkinkan bahwa keamanan privasi data pribadi nasabah yang menggunakan layanan perbankan melalui media internet kurang terjamin. Hal ini dikarenakan masih banyak kelemahan dalam

mengantisipasi berbagai pelanggaran atau penyalahgunaan dari media internet yang berdampak kerugian berbagai pihak.

Mekanisme perlindungan dan Tanggungjawab yang diberikan oleh pihak bank terhadap nasabah yang mengalami masalah dalam penggunaan Internet Banking Perkembangan teknologi informasi kian pesat, terjadi disegala bidang, termasuk di bidang perbankan. Kegiatan perbankan dapat dilakukan melalui media elektronik, seperti melalui internet. Maka munculah istilah Internet Banking yang saluran jaringannya digunakan untuk memberikan layanan perbankan seperti membuka rekening, transfer dan pembayaran online. Dalam menjalankan kegiatan electronic banking (e-banking) wajib menerapkan manajemen risiko pada aktivitas 26 layanannya secara efektif.

Perlindungan yang diberikan oleh bank sangat penting untuk menimbulkan kepercayaan dan kenyaman nasabah. Karena resiko yang ditimbulkan dalam layanan ini sangat tinggi, ada kemungkinan nasabah menderita kerugian karena disadap oleh hacker/cracker yang mampu 27 menembus firewall atau memasuki website yang memiliki nama domain yang hampir sama. Untuk itu beberapa hal penting yang sudah diterapkan oleh bank dalam rangka melakukan perlindungan kepada nasabahnya 28 , di antara yaitu: Perlindungan hukum terhadap nasabah pengguna layanan internet banking yang diberikan oleh pihak bank dari segi keamanan teknologi sudah maksimal dan juga memenuhi aspek-aspek confidentially, integrity, authentication, availability, access control, dan nonrepudiation 29 karena sekarang rata-rata bank semuanya dalam transaksi yang dilakukan lewat internet banking juga

lebih dilindungi berkat Token PIN. Token PIN adalah alat pengaman tambahan untuk melakukan transaksi finansial di Internet Banking. Token Pin ini berfungsi untuk mengeluarkan dinamyc password (PIN Dinamis), yaitu PIN yang selalu berubah dan hanya dapat digunakan satu kali untuk tiap transaksi finansial yang dilakukan. PIN Dinamis tersebut (disebut juga sebagai PIN) digunakan sebagai otentikasi transaksi pada saat nasabah melakukan transaksi melalui Internet Banking.

Dengan fasilitas ini, rekening Anda tidak mungkin disalahgunakan meskipun informasi yang Anda masukkan telah tertangkap oleh keylogger. Sedangkan untuk login ke dalam sistem Internet Banking, nasabah cukup menggunakan USER ID dan PIN Internet Banking (PIN statis) yang dibuat pada saat nasabah mendaftarkan diri sebagai pengguna. 30 Adapun bentuk dari token PIN ini menyerupai kalkulator dengan ukuran sekitar 3 x 5 sentimeter. Pemakaian Token PIN jelas menguntungkan karena PIN selalu berganti setiap bertransaksi sehingga sukar dilacak oleh orang lain. Ditambah lagi token PIN ini unik bagi setiap nomor rekening dan tidak bisa digunakan pada rekening lain. Menariknya, benda kecil ini telah tersedia dalam sebelas macam warna, sehingga para nasabah bisa memilih yang disukainya.

Selain itu juga pihak bank demi menjaga kerahasiaan identitas dan semua informasi keuangan Nasabah Pengguna. Untuk menjaga komitmen jaminan keamanan dan kerahasiaan data pribadi, keuangan dan transaksi Nasabah Pengguna, Internet Banking menggunakan beberapa sistem yang melindungi informasi rekening dan data Nasabah : 1. User ID dan PIN (Personal

Identification Number), merupakan kode rahasia dan kewenangan penggunaan yang diberikan kepada Nasabah, yaitu setiap kali login ke Internet Banking Nasabah harus memasukkan User ID dan PIN, dan untuk transaksi yang bersifat finansial, Nasabah harus memasukkan kembali PIN untuk menghindari penyalahgunaan oleh orang lain saat komputer ditinggalkan dalam keadaan terhubung dengan Internet Banking.

Automatic log out, jika tidak ada tindakan yang dilakukan lebih dari 10 menit, Internet Banking secara otomatis akan mengakhiri dan kembali ke menu utama. 3. SSL 128-bit encryption, seluruh data di Internet Banking Mandiri dikirimkan melalui protocol Secure Socket Layer (SSL), yaitu suatu standar pengiriman data rahasia melalui internet. Protocol SSL ini akan mengacak data yang dikirimkan menjadi kode-kode rahasia dengan menggunakan 128bit encryption, yang artinya terdapat 2 pangkat 128 kombinasi angka kunci, tetapi hanya satu kombinasi yang dapat membuka kode-kode tersebut.

Firewall, untuk membatasi dan menjamin hanya Nasabah yang mempunyai akses untuk dapat masuk ke sistem Internet Banking. Sedangkan perlindungan dari segi hukum yang paling efektif yaitu yang terdapat pada "syarat dan Ketentuan internet banking", karena di dalam syarat dan ketentuan 31 tersebut mengandung unsur hak dan kewajiban para pihak, khususnya pihak bank dan pihak nasabah. Akan tetapi Syarat dan Ketentuan tersebut merupakan perjaniian standar yang dibuat sepihak oleh pelaku usaha/pihak bank, sehingga lebih banyak mengutamakan kewajiban-kewajiban nasabah dan hakhak bank daripada hak-hak nasabah dan kewajiban- kewajiban bank itu sendiri.

Biasanya syarat dan ketentuan ini terdapat dalam halaman website bank ataupun buku panduan yang diberikan oleh bank dalam penggunaan layanan internet banking. Perlindungan dalam kebijakan privasi terkait dengan semua transaksi perbankan dan informasi rekening lainya disimpan secara rahasia sesuai dengan ketentuan hukum yang berlaku di Indonesia. hanya orang tertentu yang berhak untuk mengakses informasi tersebut untuk digunakan sebagaimana mestinya (dalam hal ini pihak bank akan selalu mengingatkan karyawan akan pentingnya menjaga kerahasian data Nasabah).

Bank tidak akan memperlihatkan/menjual data tersebut kepada pihak ke tiga. Sedangkan dari segi tanggungjawab pihak bank sebagai pihak penyelenggara layanan internet banking membebankan kepada nasabah agar lebih meningkatkan kewaspadaan dan ketelitian dalam menggunakan layanan internet banking. Bila terjadi hal-hal yang mencurigakan atau dianggap akan menimbulkan bahaya dalam hal ini ancaman cybercrime dalam penggunaan internet banking, maka nasabah dapat memberitahukan ke bank bersangkutan melalui call center (layanan 24 jam) yang tersedia ataupun bisa langsung mengajukan atau menyampaikan penggaduansecara tertulis ke CSO bank yang bersangkutan.

Adapun kompensasi yang diberikan oleh bank kepada nasabah internet banking adalah pemberian ganti rugi materiil sesuai kerugian yang dialami nasabah apabila telah tercapai kesepakatan antara nasabah dan pihak bank. Karena sebelum pihak bank memberi ganti rugi terhadap nasabah, mereka akan mengecek terlebih dahulu setiap instruksi transaksi dari nasabah yang

tersimpan pada pusat data dalam bentuk apapun, termasuk namun tidak terbatas pada catatan, tape/cartridge, printout komputer/perangkat, komunikasi yang dikirimkan secara elektronik antara bank dan nasabah, merupakan alat bukti yang sah, kecuali nasabah dapat membuktikan sebaliknya

C. Kendala yang Dihadapi dalam Perlindungan Hukum dan Hak Asasi Manusia Terhadap Nasabah Bank Korban *Cyber crime* dalam Internet Banking

Kejahatan atau tindak pidana perbankan memiliki karakteristik yang khas, yang membedakan dengan tindak pidana lain, sehingga harus dicegah dan ditanggulangi dengan cara-cara yang khas pula. Oleh karena keadaan yang seperti itu, maka kendala selalu muncul dalam upaya mencegah dan menanggulangi kejahatan perbankan. Adapun terdapat beberapa kendala dalam penanganan tindak pidana perbankan, yaitu:

1. Belum adanya kesamaan pandang tentang penggunaan dokumen fotokopi sebagai barang bukti dan dalam menetapkan undang-undang atau ketentuan yang dilanggar dalam tindak pidana bank;
2. Tingkat pemahaman para penegak hukum terhadap kegiatan/operasional perbankan yang berbeda-beda dan belum merata serta lemahnya koordinasi dalam penanganan kasus perbankan;
3. Belum efektifnya tindak lanjut penanganan kasus yang telah diserahkan oleh Bank Indonesia kepada penyidik;
4. Terdapat beberapa kasus yang sulit diungkapkan modus operandinya yang antara lain disebabkan oleh pesatnya teknologi dan informasi

Hambatan dalam Penanganan *Cyber crime* Meskipun sudah ada beberapa pasal yang bisa menjerat pelaku cybercrime ke penjara, tetapi masih dijumpai adanya hambatan-hambatan dalam pelaksanaan di lapangan yang antara lain sebagai berikut:

1. Perangkat hukum yang belum memadai Para penyidik (khususnya Polri) melakukan analogi atau perumpamaan dan persamaan terhadap pasal-pasal yang ada dalam KUHP sependapat bahwa perlu dibuat undang-undang yang khusus mengatur cybercrime.
2. Kemampuan penyidik Secara umum penyidik Polri masih sangat minim dalam penguasaan operasional komputer dan pemahaman terhadap hacking komputer terhadap kasus-kasus itu. Beberapa faktor yang sangat berpengaruh (determinan) adalah:
    a. Kurangnya pengetahuan tentang komputer.
    b. Pengetahuan teknis dan pengalaman para penyidik dalam menangani kasus-kasus cybercrime masih terbatas.
    c. Faktor sistem pembuktian yang menyulitkan para penyidik.
3. Alat Bukti Persoalan alat bukti yang dihadapi di dalam penyidikan terhadap cybercrime antara lain berkaitan dengan karakteristik kejahatan cybercrime itu sendiri, yaitu; sasaran atau media cybercrime adalah data dan atau sistem komputer atau sistem internet yang sifatnya mudah diubah, dihapus, atau disembunyikan oleh pelakunya. Cybercrime seringkali dilakukan hampir-hampir tanpa saksi, di sisi lain, saksi korban seringkali berada jauh di luar

negeri sehingga menyulitkan penyidik melakukan pemeriksaan saksi dan pemberkasan hasil penyidikan.

4. Fasilitas komputer forensik Untuk membuktikan jejak-jejak para hacker, dan cracker dalam melakukan aksinya terutama yang berhubungan dengan program- program dan data komputer, sarana Polri belum memadai karena belum ada komputer forensik. Fasilitas ini diperlukan untuk mengungkapn data digital serta merekam dan menyimpan bukti-bukti berupa soft copy (image, program, dsb). Dalam hal ini Polri masih belum mempunyai fasilitas forensic computing yang memadai. Fasilitas forensic computing yang akan didirikan Polri diharapkan akan dapat melayani tiga hal penting yaitu evidence collection, forensic analysis, expert witness.

MEKANISME CHARGEBACK DI BANK X Chargeback adalah suatu mekanisme beban balik akibat transaksi fraud yang tidak dilakukan oleh pemegang kartu kredit yang sah. Mekanisme beban balik telah menjadi mekanisme lazim dalam industri kartu kredit, dimana terdapat dua pihak pelaku beban balik yakni:

1. Pihak bank sebagai issuer
2. Pihak bank sebagai acquirer Pihak issuer akan melakukan pembebanan atas sejumlah nominal transaksi kepada pihak acquirer karena toko mereka telah memfasilitasi dan atau membuka peluang bagi terjadinya transaksi fraud. Dengan beban balik ini pihak issuer akan mendapatkan

dananya kembali yang kemudian dapat digunakan untuk menghapus transaksi dari pemegang kartu kredit bank tersebut. Eksekusi chargeback dijalankan secara elektronik dengan menggunakan sarana komunikasi elektronik Card Link yang terkoneksi ke jaringan Visa dan atau Master Card. Mekanisme chargeback diatur oleh Visa atau Mastercard dengan contoh regulasi dari pihak principal sebagai berikut: Regulasi No. 3.24.1.2 Periode Waktu bagi Issuer untuk melakukan Chargeback Issuer dapat melakukan beban balik secara layak atas transaksi fraud yang terjadi pada pemegang kartu yang tertera dalam Global Security Bulletin selama periode beban balik itu masih berlaku dalam Global Security Bulletin. Beban balik harus disampaikan tidak lebih dari 120 hari kalender setelah tanggal publikasi pertama Global Security Bulletin yang mencantumkan lokasi merchant atau dalam rentang waktu 120 hari kalender dari tanggal transaksi Central Site Business. Adapun pengajuan teknis chargeback tersebut juga diatur oleh Visa atau Master Card dengan regulasi sebagai berikut: Regulasi No. 3.33.1 Pemakaian Kode Pesan Yang Cocok 4863 Issuer dapat menggunakan kode alasan atau pesan nomor 4863 untuk seluruh transaksi carding (pihak Prinsipal menyebut Carding sebagai Card Not Present Transaction) apabila:

a. Pemegang kartu mengklaim bahwa dia tidak mengenali adanya transaksi yang muncul dalam lembar tagihan ybs.

b. Issuer telah melakukan usaha-usaha yang cukup baik untuk mengidentifikasikan transaksi itu bagi pemegang kartu. (Contoh: Issuer mengkonfirmasi bahwa pemegang kartu berusaha atau telah menghubungi merchant untuk mendapatkan identifikasi transaksi).
c. Issuer harus menginstruksikan pemegang kartunya untuk menghubungi merchant untuk mendapatkan informasi lebih lanjut sebelum mereka melakukan chargeback.

Perlindungan nasabah kasus carding dalam UU ITE No 11 Tahun 2008 Perlindungan hukum bagi nasabah pengguna kartu kredit mutlak diperlukan seperti halnya perlindungan yang diberikan kepada nasabah penyimpan dana lainnya. Menurut sistem perbankan Indonesia, perlindungan terhadap nasabah dapat dilakukan melalui dua metode, yaitu:

1. Perlindungan secara eksplisit *(explicit deposit protection)* Yaitu perlindungan yang diperoleh melalui pembentukan lembaga yang menjamin simpanan masyarakat, sebagaimana diatur dalam Keputusan Presiden No. 26 Tahun 1998 tentang Jaminan terhadap Kewajiban Bank Umum. Sehingga apabila bank mengalami kegagalan, maka lembaga tersebut akan mengganti dana masyarakat yang disimpan dalam bank yang gagal tersebut. Hal ini diatur dalam Keputusan Presiden No. 26 Tahun 1998 tentang Jaminan terhadap Kewajiban Bank Umum, sebelum diberlakukannya asuransi deposito (Marulak Pardede, 2001).
2. Perlindungan secara implisit (implicit deposit protection) Yaitu perlindungan yang dihasilkan oleh pengawasan dan pembinaan bank

secara efektif. Maksudnya agar dapat menghindari terjadinya kebangkrutan bank yang diawasi. Perlindungan semacam ini dapat diperoleh melalui (Marulak Pardede, 2001):

a. Peraturan perundang-undangan di bidang ITE dan perbankan;
b. Perlindungan yang dihasilkan oleh pengawasan dan pembinaan yang efektif, yang dilakukan oleh Bank Indonesia;
c. Upaya menjaga kelangsungan usaha bank sebagai suatu lembaga pada khususnya dan perlindungan terhadap sistem perbankan pada umumnya;

Sementara itu dalam UU ITE No.11 tahun 2008 memang tidak menyebutkan secara eksplisit tindak pidana carding namun Undang-undang ini dalam penjelasannya menyatakan secara eksplisit bahwa kegiatan siber (cyber) tidak lagi sederhana karena kegiatannya tidak lagi dibatasi oleh teritori 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 dana kartu kredit melalui pembelanjaan di Internet.

Oleh karena itu UU ITE No.11 tahun 2008 secara jelas mengatur perlindungan warga negara dari tindak pidana kejahatan yang berhubungan dengan transaksi elektronik baik melalui penegakan hukum perdatan maupun hukum pidana. Untuk kasus carding yang merupakan transaksi elektronik yang dilakukan secara non face to face maka perlindungan nasabahnya diatur oleh Pasal 32 dengan sanksi pidananya berada pada Pasal

48. Kasus carding berhubungan dengan pencurian data dan informasi kartu kredit. Meskipun tidak ada kata “pencurian” dalam UU ITE No.11 tahun 2008 namun pengaturan carding mengacu secara spesifik pada Pasal 32 ayat 1 sebagai berikut:

> Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik Publik.

Dalam kasus-kasus carding dimana nomor kartu kredit tersebar luas dan dapat diakses oleh publik maka pengaturan dalam UU ITE No.11 berada pada Pasal 34 ayat 1 butir b dengan bunyi sebagai berikut: Sandi lewat Komputer, Kode Akses, atau hal yang sejenis dengan itu yang ditujukan agar Sistem Elektronik menjadi dapat diakses dengan tujuan memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33. Masalah yang akan banyak memusingkan pengguna Internet adalah Bab VII mengenai Perbuatan yang dilarang yang terdapat dalam Pasal 27-37 UU ITE, semua pasal ini menggunakan kalimat setiap orang. Padahal perbuatan yang dilarang, seperti spam, penipuan, cracking, virus, penipuan, spam, flooding sebagian besar akan dilakukan oleh mesin dengan algoritma program jahat. Bahkan sering kali penjalaran spam, worm bukan dilakukan oleh programer pada tangan pertama.

Secara sepintas UU ITE dapat memperkecil ruang gerak hacker yang melakukan pengrusakan dan melakukan pencurian nomor kartu kredit melalui Internet atau carding. Memang cakupan atau ruang lingkup UU ITE sangat luas sebagai lex generalis (payung hukum) bagi tindak pidana di bidang elektronika, teknologi informasi dan komunikasi. Namun demikian luasnya cakupan tersebut harus juga dibarengi dengan pengaturan yang spesifik di bidang tindak pidana carding ini. Mengingat RUU TIPITI sudah berada di lembaga legislasi DPR untuk nantinya dirumuskan menjadi UU maka pihak legislator perlu mendapatkan masukan yang memadai dari pelaku industri kartu kredit di Tanah Air.

Penegak hukum di Indonesia saat ini, mengalami kesulitan dalam menghadapi merebaknya cybercrime. Hal ini dilatarbelakangi masih sedikitnya aparat penegak hukum yang memahami seluk beluk teknologi informasi (internet), terbatasnya sarana dan prasarana, serta kurangnya kesadaran hukum masyarakat dalam dalam upaya penanggulangan tindak pidana teknologi informasi. Disamping itu aparat penegak hukum di daerah pun belum siap dalam mengantisipasi maraknya kejahatan ini karena masih banyak aparat penegak hukum yang gagap teknologi (gaptek) hal ini disebabkan oleh masih banyaknya institusi-institusi penegak hukum di daerah yang belum didukung dengan jaringan internet. Keterbatasan alat-alat khusus *cyber crime* yang dimiliki oleh Polisi di daerahdaerah kabupaten sampai dengan tingkat kecamatan untuk menunjang sarana prasarana penyidik dalam mengungkap tindak pidana penipuan transaksi elektronik.

Keterbatasan alat-alat modern di daerah menyebabkan waktu cukup lama dalam mengungkap tindak kejahatan penipuan transaksi elektronik dan alatalat yang dibutuhkan juga memerlukan biaya yang besar.

Upaya untuk mengungkap dan menanggulangi kejahatan penipuan dengan menggunakan transaksi elektronik ini tidaklah mudah, selain karena kurangnya pemahaman atau kewaspadaan masyarakat terhadap tindak pidana penipuan melalui teknologi informasi, masyarakat lebih melihat nominal atau besaran jumlah keuntungan dari suatu barang yang ditawarkan. Ketika terjadi kerugian yang diakibatkan adanya penipuan transaksi elektronik, masyarakatpun dihadapkan dengan tidak mau melaporkan tindak kejahatan yang dialaminya ke aparat penegak hukum, karena:

1. Masyarakat tidak percaya dengan kinerja aparat penegak hukumnya.
2. Kekhawatiran masyarakat jika berurusan dengan aparat penegak hukum masyarakat akan semakin merugi. Ibarat kehilangan ayam, maka masyarakat harus siap kehilangan kambing, artinya sudah kehilangan harta bendanya masyarakat khawatir dipungut biaya oleh aparat penegak hukum.
3. Masyarakat khawatir keselamatan jiwanya terancam jika melaporkan tindak kejahatan yang dialaminya. Pada umumnya suatu masyarakat yang mengalami perubahan sosial akibat kemajuan teknologi, banyak melahirkan masalah-masalah sosial. Hal itu terjadi karena kondisi masyarakat itu sendiri yang belum siap menerima perubahan atau dapat

pula karena nilai-nilai masyarakat yang telah berubah dalam menilai kondisi yang tidak lagi dapat diterima.

Memang tidak bisa diingkari oleh siapapun, bahwa teknologi itu dapat menjadi alat perubahan di tengah masyarakat. Demikian pentingnya fungsi teknologi, hingga sepertinya masyarakat dewasa ini sangat tergantung dengan teknologi, baik untuk hal-hal positif maupun negatif. Pada perkembangannya internet juga membawa sisi negatif, dengan membuka peluang munculnya tindakan-tindakan anti sosial yang selama ini dianggap tidak mungkin terjadi atau tidak akan terpikirkan terjadi. Sebuah teori menyatakan bahwa crime is product of society it self, yang secara sederhana dapat diartikan bahwa semakin tinggi tingkat intelektualitas suatu masyarakat, maka akan semakin canggih dan beraneka-ragam pulalah tingkat kejahatan yang dapat terjadi.

Untuk menangani kasus-kasus cybercrime khususnya tindak pidana penipuan transaksi elektronik, Indonesia sangat membutuhkan aparat penegak hukum yang mumpuni, yang terorganisasi dan terstruktur untuk menyatukan komunitas-komunitas spesialisasi dalam penanganan segala jenis tindak pidana cyber. Tanpa adanya penegakan hukum yang terorganisasi dan terstruktur di bidang teknologi informasi, maka akan sulit menjerat penjahat-penjahat cyber oleh karena kejahatan cyber ini locos delicti-nya bisa lintas negara.

Dalam hal menangani kasus cybercrime khususnya tindak pidana penipuan transaksi elektronik diperlukan spesialisasi aparat penyidik yang

dapat dipertimbangkan sebagai salah satu cara untuk melaksanakan upaya penegakan hukum terhadap cybercrime. Spesialisasi tersebut dimulai dari adanya pendidikan yang diarahkan untuk menguasai teknis serta dasar-dasar pengetahuan di bidang teknologi komputer. Pasal 43 UU ITE, menerangkan selain Penyidik Pejabat Polisi Negara Republik Indonesia, Pejabat Pegawai Negeri Sipil tertentu dilingkungan Pemerintah yang lingkup tugas dan tanggung jawabnya di bidang Teknologi Informasi dan Transaksi Elektronik diberi wewenang khusus sebagai penyidik sebagaimana dimaksud dalam UndangUndang tentang Hukum Acara Pidana untuk melakukan penyidikan tindak pidana di bidang

Teknologi Informasi dan Transaksi Elektronik. Kendala pertanggungjawaban pidana terhadap pelaku pencurian uang di bank melalui internet, antara lain: Terdapat 2 (dua) kendala pokok dalam pertanggungjawaban pidana terhadap pelaku pencurian uang di bank melalui internet. Kendala yang pertama yaitu terletak di penerapan pasal-pasalnya, dan kendala yang kedua terletak di keterbatasan sumber daya manusia (SDM) dalam pembuktian.

Pembuktian dalam kasus cybercrime atau tindak pidana pencurian uang di bank melalui internet dengan modus carding database kesulitan dalam menemukan alat bukti keterangan saksi karena deliknya yang terjadi di dunia maya, sehingga untuk alat bukti yang digunakan banyak bertumpu pada alat bukti keterangan ahli. Alat bukti digital yang digunakan dalam Undang-undang Informasi dan Transaksi Elektronik untuk membuktikan tindak

pidana yang terjadi disimpan di dalam Harddisk, sehingga tidak gampang ditemukan oleh penegak hukum karena data yang disimpan dalam Harddisk ini rawan dimanipulasi dan dihilangkan/dihapus oleh pelaku.

Penangkapan tersangka dan penyitaan alat buktinya mengalami hambatan karena pelaku menggunakan komputer yang bisa menjalankan dari tempat mana saja, sehingga aparat penegak hukum sering kali tidak dapat menentukan secara pasti siapa pelakunya. Penyelidikan merupakan tahap tersulit yang dialami oleh aparat penegak hukum, karena dalam tahap ini aparat penegak hukum tidak hanya harus dapat membuktikan tindak pidana yang terjadi, akan tetapi aparat penegak hukum harus juga menentukan sebabsebab tindak pidana tersebut untuk dapat menetukan bentuk laporan polisi yang akan dibuat.

Dalam hal penindakan untuk memberantas cybercrime, sumber daya manusia seperti aparat penegak hukumnya kurang, karena untuk memberantas tindak pidana ini dibutuhkan keahlian khusus di bidang komputer, sedangkan aparat kepolisian yang mempunyai divisi cybercrime yang bertaraf internasional hanya terletak di Mabes Polri.

Mengingat terbatasnya sumber daya manusia dalam memberantas tindak pidana cybercrime, penegak hukum hendaknya mengirimkan anggotanya untuk mengikuti kursus-kursus atau pelatihan-pelatihan di negara-negara maju agar nantinya ilmu yang diperoleh dapat diterapkan di Indonesia, khususnya ilmu yang berkaitan dengan pemberantatasan tindak pidana kejahatan dunia maya atau cybercrime. Selain di Kepolisian perlunya

dibentuk unit khusus yang menangani kejahatan dunia maya atau cybercrime dalam setiap pemeriksaan, seperti di Kejaksaan, Komisi Pemberantasan Korupsi (KPK), dan pengadilan.

BAB V

PENUTUP

A. Kesimpulan

1. Upaya perlindungan hukum terhadap pemberi jasa atau pengguna internet telah melahirkan suatu produk hukum dalam bentuk UU ITE, namun dengan lahirnya UU ITE belum semua permasalahan menyangkut masalah ITE dapat tertangani. Dengan lahirnya UU ITE tidak semata-mata undang-undang ini bisa diketahui oleh masyarakat pengguna teknologi informasi dan praktisi hukum. Kemudian berbagai bentuk perkembangan teknologi yang menimbulkan penyelenggaraan dan jasa baru harus dapat diidentifikasikan dalam rangka antisipasi terhadap pemecahan berbagai persoalan teknis yang dianggap baru sehingga dapat dijadikan bahan untuk penyusunan berbagai Peraturan Pelaksanaan.
2. Satu langkah yang dianggap penting untuk menanggulangi keamanan sistem informasi adalah telah diwujudkannya rambu-rambu hukum yang tertuang dalam UU ITE. Hal yang mendasar dari UU ITE ini sesungguhnya merupakan upaya mengakselerasikan manfaat dan fungsi hukum (peraturan) dalam kerangka kepastian hukum. Penegakan hukum pidana dalam *cyber crime* dapat dilakukan oleh penyidik yang terdiri dari Kepolisian Republik Indonesia dan Penyidik Pegawai Negeri Sipil. Penyidikan dilakukan berdasarkan KUHP dan UU ITE. Kewenangan Penyidik Pegawai Negeri Sipil dalam rangka memberikan perlindungan hukum terhadap nasabah bank yang mengalami *cyber crime* dalam internet

banking tercantum dalam Pasal 43 UU ITE. Perlindungan hukum terhadap nasabah bank yang mengalami *cyber crime* dalam internet banking dihubungkan dengan UU ITE terdapat dalam Pasal 45, Pasal 46, Pasal 47, Pasal 48, Pasal 49, Pasal 50, Pasal 51 UU ITE.

3. Menurut sistem perbankan Indonesia, perlindungan terhadap nasabah dapat dilakukan melalui dua metode, yaitu perlindungan secara eksplisit (explicit deposit protection) yaitu perlindungan yang diperoleh melalui pembentukan lembaga yang menjamin simpanan masyarakat dan perlindungan secara implisit (implicit deposit protection) yaitu perlindungan yang dihasilkan oleh pengawasan dan pembinaan bank secara efektif. Maksudnya agar dapat menghindari terjadinya kebangkrutan bank yang diawasi.
4. Perlindungan hukum dan HAM terhadap korban *cyber crime* diatur dalam Pasal 3 Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, dan Pasal 4 Undang-Undang Nomor 11 Tahun 2008.
5. Kendala yang dihadapi ketika melakukan program ini yakni belum adanya kesamaan pandang tentang penggunaan dokumen fotokopi sebagai barang bukti dan dalam menetapkan undang-undang atau ketentuan yang dilanggar dalam tindak pidana bank, tingkat pemahaman para penegak hukum terhadap kegiatan/operasional perbankan yang berbeda-beda dan belum merata serta lemahnya koordinasi dalam penanganan kasus perbankan, belum efektifnya tindak lanjut penanganan kasus yang telah diserahkan oleh Bank Indonesia kepada penyidik, terdapat beberapa kasus yang sulit

diungkapkan modus operandinya yang antara lain disebabkan oleh pesatnya teknologi dan informasi, perangkat hukum yang belum memadai Para penyidik (khususnya Polri) melakukan analogi atau perumpamaan dan persamaan terhadap pasal-pasal yang ada dalam KUHP sependapat bahwa perlu dibuat undang-undang yang khusus mengatur *cybercrime*, kemampuan penyidik Secara umum penyidik Polri masih sangat minim dalam penguasaan operasional komputer dan pemahaman terhadap hacking komputer terhadap kasus-kasus itu.

B. Saran

Atas kesimpulan tersebut peneliti dapat memberikan saran diantaranya adalah:

1. Bagi Bank
   a. Penelitian ini memberikan informasi bahwa nasabah masih merasakan kekhawatiran apabila memberikan informasi keuangannya saat melakukan transaksi melalui Internet Banking. Dengan adanya informasi ini diharapkan dapat memberikan masukan pada pihak bank untuk lebih meningkatkan keamanan layanan Internet Banking dan lebih intensif dalam melakukan sosialisasi kemanan dalam penggunaan layanan Internet Banking.
   b. Dan juga diharapkan adanya bentuk perlindungan untuk nasabah yang secara khusus diatur untuk melindungi nasabah dari tindak kejahatan *Cyber crime* yang marak terjadi belakangan ini. Dimana bank mampu untuk membuat semacam aplikasi unit untuk melaporkan setiap

kejahatan kejahatan *Cyber crime* serta membangun pencegahan atau pertahanan anti malware di seluruh server bank.

2. Bagi Nasabah

   Penelitian ini memberikan informasi bahwa nasabah wajib memperhatikan risiko yang dapat ditimbulkan dari adanya Internet Banking ini tidak hanya melihat dari segi kemudahannya saja tetapi juga bisa mengetahui risliko yang sewaktu-waktu dapat terjadi pada nasabah, maka oleh sebab itu diharapkan nasabah pengguna Internet Banking dapat waspada dan hati-hati dalam proses penggunaan Internet Banking itu sendiri.

DAFTAR PUSTAKA

Buku

Al' Adl. *Perlindungan Hukum Terhadap Nasabah Bank yang menjadi Korbsn krjahatan dibidang Perbankan. 2013* Volume V Nomor 9.

Andrisman, Tri, *Hukum Pidana, Asas-asas dan Dasar Aturan Umum Hukum Pidana Indonesia*, Universitas Lampung 2005.

Arief, Barda Nawawi. *Strategi Penanggulanagn Kejahatan Telematika,* Semarang, Uiniversitas Atma Jaya Yogyakarta, 2010.

Gazali, Djoni S., and Rachmadi Usman. "*Banking Law*." Cet: III, Jakarta: Sinar Grafika, 2016

Indonesia, Ikatan Bankir. *Mengelola Bank Komersial*. Gramedia Pustaka Utama, 2014

Lamintang, *Dasar-dasar Hukum Pidana Indonesia*, PT Citra Aditya Bhakti, Bandung, 1997.

Marzuki, Petter Mahmud, 2015, *Penemuan Hukum*, Jakarta: Prenamedia Group

Miles dan Huberman. *1992*. *Analisis data Kualitatif*. (diterjemahkan oleh: Tjetjep Rohedi Rosidi). Jakarta: Universitas Indonesia

Moeljatno, *Asas-asas Hukum Pidana*, Bina Aksara, Jakarta, 1987.

Poernomo, Bambang. *Asas-asas Hukum Pidana*, Ghalia Indonesia, Jakarta, 1992.

Prodjodikro, Wirjono, *Asas-asas Hukum pidana*, Ghalia Indonesia Jakarta 2002.

R, Abdoel Djamail, *Pengantar Hukum Indonesia*, Edisi Revisi, Raja Grafindo persada, Jakarta, 2006.

Rasjidi, Lili Rasjidi Ira Thania. *Dasar-Dasar Filsafat dan Teori Hukum*, Citra Aditya Bakti, Bandung, 2007.

Soekanto, Soerjono, *Pengantar Penelitian Hukum*, Universitas Indonesia - Press, Jakarta.

Jurnal

Anggara, Bayu, and I. Nyoman Darmadha. "Penegakan Hukum Kejahatan Dunia Maya (Cybercrime) Yang Dilakukan Anak Di Bawah Umur." Kertha Wicara: Journal Ilmu Hukum

Astrini, Dwi Ayu. "Perlindungan Hukum Terhadap Nasabah Bank Pengguna Internet Banking Dari Ancaman Cybercrime." Lex Privatum 3, no. 1 (2015).

Disemadi, Hari Sutra, and Paramita Prananingtyas. "Perlindungan Hukum Terhadap Nasabah Perbankan Pengguna CRM (Cash Recycling Machine)." Jurnal Magister Hukum Udayana (Udayana Master Law Journal) 8, no. 3 (2019)

Nugraha, Ferry Satya, and Rinitami Njatrijani Budiharto. "Perlindungan Hukum Terhadap Nasabah Bank Dalam Pembobolan Internet Banking Melalui Metode Malware." Diponegoro Law Journal 5, no. 3 (2016)

Ronny Prasetya, *Pembobolan ATM, Tinjauan Hukum Perlindungan Nasabah Korban Kejahatan Perbankan*, Jakarta: PT. Prestasi Pustaka, 2010.

Sjahdeini, Sutan Remy, *Kejahatan dan Tindak Pidana Komputer*, Jakarta: Puataka utama Grafiti, 2009.

Undang Undang dan Peraturan Pemerintah

Undang-Undang Dasar Negara Republik Indonesia 1945

Undang-undang Nomor 7 Tahun 1992 juncto undang-undang nomor 10 tahun 1998 tentang Perbankan.

1999 Tentang Perlindungan Konsumen.

Undang-undang Negara Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Peraturan Bank Indonesia Nomor 9/15/PBI/2007 Tentang Penerapan Manajemen Risiko Dalam Penggunaan Teknologi Informasi Oleh Bank Umum

Lampiran I

PEDOMAN WAWANCARA

1. Bagaimana tentang fenomena *cyber crime* dalam internet banking?
2. Apakah internet banking banyak memiliki keuntungan atau justru berbahaya?
3. Apa faktor-faktor penyebab timbulnya nasabah bank menjadi korban *cyber crime* dalam internet banking?
4. Bagaimana perlindungan hukum dan ham terhadap nasabah bank korban *cyber crime* dalam internet banking berdasarkan undangundang nomor 11 tahun 2008 tentang informasi dan transaksi elektronik?
5. Apa saja hambatan yang dihadapi dalam perlindungan hukum dan ham terhadap nasabah bank korban *cyber crime* dalam internet banking berdasarkan undang-undang nomor 11 tahun 2008 tentang informasi dan transaksi elektronik?