JURNAL HUKUM CARAKA JUSTITIA | Vol. 2 No. 1 | Mei 2022 | p. 54 - 74

PERLINDUNGAN HUKUM BAGI NASABAH DAN BANK TERHADAP TINDAK KEJAHATAN BERBASIS TEKNOLOGI INFORMASI *(CYBER CRIME)*

Benedictus Renny See
Fakultas Hukum, Universitas Proklamasi 45
benedictus.renny@up45.ac.id

Abstract

Banks as intermediary institutions and trust institutions as the driving force of a country's economy, in their activities, cannot be separated from the use of information technology to support their operations. The use of information technology by banks in addition to having a positive impact also has a negative impact that will threaten and harm the bank and its customers, if not managed properly. Banking crimes that use information technology, especially against bank products and services that use computers and internet networks (cybercrime) will cause losses to customers and the bank itself.

This research is normative juridical research that is descriptive-analytical with a case approach to identify and analyze forms of crime in the banking world and the efforts made by the government CQ. financial authorities in providing legal protection for customers and banks from criminals who use information technology.

The results of this study indicate that cybercrime is a crime using information technology that can be carried out without recognizing territorial boundaries and no direct interaction between perpetrators and victims of crime is required; so that the public (customers) and banking institutions need protection with preventive and repressive measures, namely by applying existing laws and regulations and coordinating with law enforcement officials in preventing the occurrence of cybercrime and providing severe penalties for the perpetrators of these crimes.

Keywords*: Legal protection, customers and banks.*

Abstrak

Bank sebagai lembaga intermediasi dan lembaga kepercayaan sebagai penggerak roda ekonomi suatu negara, dalam aktivitasnya tidak lepas dari penggunaan teknologi informasi dalam mendukung operasionalnya. Penggunaan teknologi informasi oleh bank selain membawa dampak positif juga membawa dampak negatif yang akan mengancam dan merugikan bank maupun nasabah, apabila tidak dikelola secara baik. Kejahatan perbankan yang menggunakan teknologi informasi khususnya terhadap produk maupun jasa bank yang menggunakan komputer dan jaringan internet *(cyber crime)* akan menimbulkan kerugian bagi nasabah maupun bank itu sendiri.

Penelitian ini merupakan penelitian yuridis normatif yang bersifat deskriptif analitis dengan pendekatan kasus *(case approach)* untuk mengetahui dan menganalisis bentuk-bentuk kejahatan dalam dunia perbankan dan upaya-upaya yang telah dilakukan oleh pemerintah cq. otoritas keuangan dalam memberikan perlindungan hukum bagi nasabah dan bank dari para pelaku kejahatan yang menggunakan teknologi informasi.

Hasil Penelitian ini menunjukkan bahwa c*yber crime* adalah kejahatan dengan menggunakan teknologi informasi yang dapat dilakukan tanpa mengenal batas teritorial dan tidak diperlukan

interaksi langsung antara pelaku dan korban kejahatan; sehingga masyarakat (nasabah) dan lembaga perbankan membutuhkan perlindungan dengan tindakan preventif maupun represif, yaitu dengan menerapkan peraturan perundang-undangan yang ada serta melakukan koordinasi dengan aparat penegak hukum dalam mencegah terjadinya *cyber crime* serta memberikan hukuman yang berat bagi para pelaku kejahatan tersebut.

Kata kunci: Perlindungan hukum, nasabah dan bank.

A. Pendahuluan

Keberadaan lembaga perbankan memiliki peran yang strategis dalam menggerakkan roda perekonomian suatu negara. Fungsi "intermediasi" bank sebagai lembaga keuangan yang menghimpun dana pihak ketiga (masyarakat) dan menyalurkannya kembali kepada masyarakat dalam bentuk pembiayaan atau kredit, memacu setiap bank berlomba-lomba dalam pengembangan produk, jasa dan pelayanan guna menarik dan meningkatkan jumlah nasabahnya antara lain dengan memanfaatkan kemajuan Teknologi Informasi dan Komunikasi (TIK).

Proses globalisasi dan perkembangan sektor keuangan yang pesat didukung dengan semakin berkembangnya teknologi informasi, telah menciptakan sistem keuangan yang sangat kompleks, dinamis, dan saling terkait antara satu sub sektor keuangan dengan yang lain. Bank yang tidak menerapkan teknologi informasi dalam produk dan jasanya akan semakin ditinggalkan oleh para nasabahnya, akibatnya adalah setiap bank akan berupaya semaksimal mungkin melengkapi semua produk dan jasa bank dengan berbasiskan teknologi informasi[1].

Di samping dampak positif teknologi informasi dan komunikasi (TIK) dibidang perbankan juga disadari bahwa perkembangan Teknologi Informasi dan Komunikasi memberi peluang terjadinya tindak pidana kejahatan baru (*cyber crime*). Oleh karena itu TIK telah menjadi "pedang bermata dua" di mana selain memberikan kontribusi positif bagi bank dalam meningkatkan kinerjanya, sekaligus menjadi sarana efektif bagi timbulnya kejahatan dan perbuatan melawan hukum yang akan merugikan pihak nasabah maupun bank itu sendiri[2].

Menyadari akan hal tersebut Pemerintah telah mengeluarkan beberapa ketentuan hukum guna melindungi nasabah (konsumen) maupun perlindungan bagi bank sendiri, yaitu antara

[1] Philipus M. Hadjon, *Perlindungan hukum bagi rakyat Indonesia* (Surabaya: PT. Bina Ilmu, 1987), 1.
[2] Andi Hamzah, *Hukum Pidana yang Berkaitan Dengan Komputer* (Jakarta: Sinar Grafika, 1993), 3.

lain adanya UU Nomor 8 Tahun 1999 tentang Perlindungan Konsumen serta UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik di mana salah satu pertimbangan lahirnya UU tersebut adalah pemerintah perlu mendukung pengembangan Teknologi Informasi melalui infrastruktur hukum dan pengaturannya sehingga pemanfaatan teknologi informasi dilakukan secara aman untuk mencegah penyalahgunaannya dengan memperhatikan nilai-nilai agama dan sosial budaya masyarakat Indonesia[3].

Beberapa contoh produk dan jasa bank yang berbasis Teknologi Informasi yang saat ini marak digunakan oleh masyarakat dan merupakan produk unggulan bagi sebagian besar bank antara lain ***Mobile Banking, SMS-Banking, phone banking, ATM, CDM, EDC, serta internet Banking*** yang saat ini sangat diminati oleh para nasabah bank yaitu salah satu pelayanan jasa bank yang memungkinkan nasabah untuk memperoleh informasi, melakukan komunikasi dan transaksi perbankan melalui jaringan internet.

Internet Banking sebagai suatu produk perbankan elektronik yang memberikan kemudahan bagi nasabah dalam melakukan transaksi perbankan non tunai melalui komputer dan jaringan internet. Jasa-jasa perbankan yang diberikan melalui *internet banking* adalah jasa-jasa yang juga diberikan melalui perbankan tradisional, seperti pembukaan rekening tabungan, melakukan transfer dana antar rekening, serta tagihan pembayaran elektronis yang memungkinkan nasabah untuk menerima dan melakukan pembayaran melalui *internet banking*. *Internet banking* sangat membantu nasabah dalam berhubungan dengan bank, karena dengan *internet banking* akses perbankan dapat dilakukan di komputer pribadi.

Internet banking banyak memberikan keuntungan bagi nasabah maupun bagi bank sendiri, namun dibalik manfaat yang bisa diperoleh *internet banking* juga bisa membawa dampak negatif. Adapun dampak negatif dari penggunaan *internet banking* adalah terbukanya kemungkinan timbulnya kejahatan di bidang perbankan seperti **pencurian data nasabah dan pencurian nomor kartu kredit, di mana data ataupun nomor yang dicuri tersebut kemudian dimanfaatkan oleh orang yang tidak berhak.**

Cyber crime adalah kejahatan yang dapat dilakukan tanpa mengenal batas teritorial dan tidak diperlukan interaksi langsung antara pelaku dan korban kejahatan. Dengan sifat seperti

[3] Nani Widya Sari, "Kejahatan Cyber Dalam Perkembangan Teknologi Informasi Berbasis Komputer", *Jurnal Surya Kencana Dua: Dinamika Masalah Hukum dan Keadilan* 5, no. 2 (Desember 2018): 579.

itu, semua negara termasuk Indonesia yang melakukan aktivitas internet akan terkena dampak dari perkembangan kejahatan dunia maya. Memudarnya batas-batas geografi dalam abad 21 yang dikenal sebagai abad informasi ini telah mengubah cara pandang terhadap penyelesaian dan praktik kejahatan dari model lama (konvensional) ke model baru (elektronik). Kekuatan jaringan dan komputer pribadi menjadikan setiap komputer sebagai alat yang potensial bagi para pelaku kejahatan. Globalisasi aktivitas kriminal yang memungkinkan para penjahat melintas batas elektronik merupakan masalah nyata dengan potensi mempengaruhi negara, hukum, dan warga negaranya. Fakta ini tak bisa dipungkiri karena internet dapat dijadikan sarana yang efektif melakukan pembobolan terhadap perbankan yang dapat dilakukan tanpa batasan geografis dan teritorial[4].

Mengingat kedudukan dan peranan bank sebagai lembaga kepercayaan yang menunjang pembangunan ekonomi suatu bangsa, maka pengamanan terhadap informasi dan data keuangan nasabah dan data bank adalah menjadi sangat penting. Tugas yang harus diemban lembaga perbankan dalam mengantisipasi dan mengatasi permasalahan kejahatan tindak pidana perbankan yang berbasis pada penggunaan teknologi informasi adalah sangat berat, tidak mungkin lembaga perbankan dapat mengatasinya sendiri. Keterlibatan dari pemerintah, Otoritas Jasa Keuangan dan aparat penegak hukum sangat dibutuhkan dalam menangani setiap perkembangan kejahatan dengan modus dan cara berbasis teknologi informasi *(Cyber Crime)*.

B. Rumusan Masalah

Berdasarkan uraian tersebut di atas dapatlah dirumuskan beberapa permasalahan pokok dalam kaitannya dengan peran Pemerintah/negara khususnya aparat penegak hukum, dalam melindungi nasabah maupun bank dari kejahatan berbasis teknologi informasi, yaitu:

1. Modus kejahatan apa saja yang terjadi dalam penggunaan teknologi informasi dibidang perbankan (*cyber crime*) ?
2. Bagaimanakah antisipasi dan tindakan Pemerintah, Bank Indonesia dan/atau Otoritas Jasa Keuangan (OJK), maupun aparat Penegak Hukum, dalam melindungi nasabah maupun bank dari kejahatan berbasis teknologi informasi?

[4] Alan N. Peachey, *Bencana Keuangan Besar Masa Kini (Great Financial Disaster of Our Time)* (Jakarta: Indonesian Risk Profesional Association (IRPA), 2007), 71.

C. Hasil Penelitian dan Pembahasan

1. Pengertian

a. ***Bank*** adalah badan usaha yang menghimpun dana dari masyarakat dalam bentuk simpanan dan menyalurkannya kepada masyarakat dalam bentuk kredit dan/atau bentuk-bentuk lainnya dalam rangka meningkatkan taraf hidup rakyat banyak (Pasal 1 angka 2 UU Nomor 7 Tahun 1992 tentang Perbankan sebagaimana telah diubah dengan UU Nomor 10 Tahun 1998).

b. ***Nasabah*** adalah pihak yang menggunakan jasa bank.

c. ***Nasabah Penyimpan*** adalah nasabah yang menempatkan dananya di bank dalam bentuk simpanan berdasarkan perjanjian bank dengan nasabah yang bersangkutan.

d. ***Bank Indonesia*** adalah Bank Sentral Republik Indonesia sebagaimana dimaksud dalam undang-undang yang berlaku.

e. ***Otoritas Jasa Keuangan (OJK)*** adalah lembaga negara yang dibentuk berdasarkan UU Nomor 21 Tahun 2011 yang berfungsi menyelenggarakan sistem pengaturan dan pengawasan yang terintegrasi terhadap keseluruhan kegiatan di dalam sektor jasa keuangan.

f. ***Transaksi Elektronik*** adalah perbuatan hukum yang dilakukan dengan menggunakan komputer, jaringan komputer dan atau media elektronik lainnya. *(Pasal 1 angka 7 UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik).*

g. ***Teknologi Informasi*** adalah suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisis, dan atau menyebarkan informasi.

h. ***Perlindungan Konsumen*** adalah segala upaya yang menjamin adanya kepastian hukum untuk memberi perlindungan kepada konsumen **(*Pasal 1 angka 2 UU tentang Perlindungan Konsumen).***

i. ***Produk bank*** adalah produk dan atau jasa perbankan termasuk produk atau jasa lembaga keuangan bukan bank yang dipasarkan oleh bank sebagai agen pemasaran. ***(Pasal 1 angka 4 PBI Nomor 7/6/PBI/2005 tentang Transparansi Informasi produk dan Penggunaan Data Pribadi Nasabah).***

j. ***Layanan Perbankan melalui media elektronik*** adalah layanan yang memungkinkan nasabah Bank untuk memperoleh informasi bank melalui media elektronik antara lain

ATM, *phone banking*, *electronic fund transfer*, *internet banking*, *mobile banking*. ***(Pasal 1 angka 3 Peraturan Bank Indonesia Nomor 9/15/PBI/2007 tentang Penerapan Manajemen Risiko dalam Penggunaan teknologi Informasi oleh Bank Umum).***

k. ***Cyber Crime*** adalah istilah yang mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer menjadi alat, sasaran atau terjadi kejahatan di dunia maya. Andi Hamzah dalam bukunya "Aspek-aspek pidana di bidang komputer" (1989) mengartikan *cyber crime* sebagai kejahatan di bidang komputer secara umum dapat dapat diartikan sebagai penggunaan komputer secara ilegal.

l. ***Hacker*** adalah orang yang mempelajari, menganalisis, dan selanjutnya bila menginginkan, bisa membuat, memodifikasi, atau bahkan mengeksploitasi sistem yang terdapat di sebuah perangkat seperti perangkat lunak komputer dan perangkat keras komputer seperti program komputer, administrasi dan hal-hal lainnya terutama keamanan. *Hacker* juga mengacu pada seseorang yang punya minat besar untuk mempelajari sistem komputer secara detail dan bagaimana meningkatkan kapabilitasnya. Besarnya minat yang dimiliki seorang *hacker* dapat mendorongnya untuk memiliki kemampuan penguasaan sistem yang di atas rata-rata kebanyakan pengguna. Jadi sebenarnya *hacker* memiliki konotasi yang netral.

m. ***Cracker*** adalah sebutan untuk mereka yang masuk ke sistem orang lain dan *Cracker* lebih bersifat destruktif, biasanya di jaringan komputer, mem-*bypass* password atau lisensi program komputer, secara sengaja melawan keamanan komputer, men-*deface* (merubah halaman muka web) milik orang lain, bahkan hingga menghapus data orang lain, mencuri data dan umumnya melakukan *cracking* untuk keuntungan sendiri, maksud jahat, atau karena sebab lainnya karena ada tantangan. Beberapa proses pembobolan dilakukan untuk menunjukkan kelemahan keamanan sistem.

n. ***Penyelenggara Sistem Electronik***, adalah pemanfaatan Sistem Elektronik oleh penyelenggara negara, badan usaha, dan/atau masyarakat.

o. ***Penyelenggaraan Sertifikasi Elektronik,*** adalah badan hukum yang berfungsi sebagai pihak yang layak dipercaya, yang memberikan dan mengaudit Sertifikat Elektronik.

p. ***Lembaga Sertifikasi Keandalan*** adalah lembaga independen yang dibentuk oleh profesional yang diakui, disahkan, dan di awasi oleh Pemerintah dengan mengaudit dan mengeluarkan sertifikat keandalan dalam transaksi elektronik.

q. **Tanda tangan Elektronik,** adalah tanda tangan yang terdiri atas informasi Elektronik yang dilekatkan, terasosiasi atau terkait dengan informasi elektronik lainnya yang digunakan sebagai alat verifikasi dan autentifikasi.

2. Modus Kejahatan dalam Teknologi Informasi di bidang Perbankan.

Beberapa modus kejahatan di bidang perbankan yang menggunakan teknologi informasi antara lain:

a. ***Carding,*** merupakan kejahatan yang dilakukan untuk mencuri nomor kartu kredit milik orang lain dan digunakan dalam transaksi perdagangan di internet, yang akan merugikan pemilik kartu kredit secara materiil. Polda DI Yogyakarta menangkap lima *carder* dan mengamankan barang bukti bernilai puluhan juta yang didapat dari *merchant* luar negeri. Para *carder* beberapa waktu lalu juga menyadap data kartu kredit dari dua *outlet* pusat perbelanjaan yang cukup terkenal. Caranya, saat kasir menggesek kartu pada mesin EDC waktu pembayaran, pada saat data berjalan ke bank tertentu itulah data dicuri. Akibatnya, banyak laporan pemegang kartu kredit yang mendapatkan tagihan terhadap transaksi yang tidak pernah dilakukannya. Begitu juga dengan yang dilakukan mahasiswa sebuah perguruan tinggi di Bandung, akibat perbuatannya selama setahun, beberapa pihak di Jerman dirugikan sebesar 15.000 DM (sekitar 70 juta).

b. ***Unauthorized Access to Computer and Service***

c. Kejahatan yang dilakukan dengan memasuki/menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya. Biasanya pelaku kejahatan akan membuat tidak berfungsinya suatu servis atau layanan. Para penyerang dengan sengaja membuat suatu layanan tidak berfungsi yang menyebabkan kerugian finansial.

d. ***Card Scimming,*** yaitu suatu modus kejahatan pembobolan rekening nasabah ATM, di mana pelaku kejahatan memasang *Skimmer* dan kamera pengintai di ruang ATM. *Skimmer* digunakan untuk mencuri data-data penting yang ada di kartu ATM korban,

sementara kamera pengintai digunakan untuk mencuri nomor PIN korban. Pembobolan ATM melalui *skimmer* sudah banyak terjadi di mancanegara. Banyak negara telah menjadikan pembobol ATM dengan *skimmer* sebagai *public enemy*, karena bisa menggoyahkan stabilitas ekonomi, khususnya bisnis perbankan yang berdasar pada kepercayaan.

e. ***Phising,*** *Phising* ada didalam dunia internet, *phising* dikenal juga sebagai aksi penipuan *online* yang mencoba mencuri data-data penting pengguna internet seperti *username, password, dan detil informasi kartu kredit.* Para pelaku sangat pandai memanfaatkan isu-isu terkini seperti bencana alam, ajang kompetisi, atau piala dunia. Teknik ini digunakan untuk mengelabui kita agar mau menyerahkan informasi pribadi, seperti *User ID*, PIN, Nomor Rekening Bank, serta Nomor kartu kredit. Informasi ini kemudian bakal dimanfaatkan oleh pelaku *phising* untuk mengakses rekening, melakukan penipuan kartu kredit atau memandu nasabah untuk melakukan transfer ke rekening tertentu dengan iming-iming hadiah.

Modus-modus kejahatan dengan memanfaatkan teknologi informasi di atas adalah contoh sebagian kecil dari sekian banyaknya kejahatan perbankan yang dilakukan melalui penggunaan teknologi informasi, baik yang dilakukan oleh pihak ketiga maupun dilakukan antara pihak ketiga bekerja sama dengan orang di dalam bank itu sendiri.

Kelemahan sistem keamanan bank juga pernah terjadi pada bulan Agustus tahun 2000 yaitu *:"Barclays Bank, yang menyatakan memiliki 1,25 juta nasabah online terpaksa menutup layanan online mereka setelah cacat keamanan membuat nasabah dapat mengakses rekening nasabah lain. Bank mengatakan bahwa kesalahan itu disebabkan oleh perbaikan perangkat lunak yang membuat rincian rekening terubah urutannya saat dua orang memasuki sistem pada saat yang bersamaan "*[5] Masalah demikian hanya berkontribusi pada kurangnya kepercayaan terhadap *e-commerce* secara umum. Jajak pendapat terbaru dari Dewan Konsumen Nasional Inggris menemukan 40 persen pengguna internet segan menggunakan kartu kredit secara online karena khawatir adanya penipuan.

[5] *Ibid.*, 272.

3. Perlindungan Hukum bagi Nasabah dari Kejahatan Menggunakan Teknologi Informasi *(Cyber Crime)*.

Dalam pembahasan tentang perlindungan hukum bagi nasabah maupun bank dari *cyber crime* yang berkaitan dengan UU Nomor 8 Tahun 1999 tentang Perlindungan Konsumen dan UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, pertama-tama kita akan melihat dari beberapa teori mengenai perlindungan hukum. Menurut pendapat Philipus M. Hadjon bahwa perlindungan hukum bagi rakyat sebagai tindakan pemerintah yang bersifat preventif dan represif. [6] Perlindungan hukum yang preventif bertujuan untuk mencegah terjadinya sengketa yang mengarahkan tindakan pemerintah bersikap hati-hati dalam pengambilan keputusan berdasarkan diskresi, dan perlindungan yang represif bertujuan untuk menyelesaikan terjadinya sengketa termasuk penanganannya di lembaga peradilan.

Dalam konteks yang sama dengan perlindungan hukum nasabah dapat kita lihat pada UU Nomor 8 Tahun 1999 tentang Perlindungan konsumen juga diatur tentang Perlindungan Konsumen yaitu segala upaya yang menjamin adanya kepastian hukum untuk memberi perlindungan kepada konsumen. Konsumen adalah setiap orang pemakai barang dan/atau jasa yang tersedia dalam masyarakat, baik bagi kepentingan diri sendiri, keluarga, orang lain, maupun makhluk hidup lain dan tidak untuk diperdagangkan.

Teori perlindungan konsumen selanjutnya adalah ***due care theory*** dalam doktrin ini dinyatakan bahwa pelaku usaha memiliki kewajiban untuk berhati-hati dalam memasyarakatkan produknya, baik berupa barang maupun jasa. Selama berhati-hati dengan produknya, ia tidak dapat dipersalahkan. Secara *a-contrario*, maka untuk dapat mempersalahkan pelaku usaha maka konsumen harus dapat membuktikan bahwa pelaku usaha melanggar prinsip kehati-hatian. Dalam hal ini yang aktif dalam membuktikan kesalahan pelaku usaha adalah konsumen sedangkan pelaku usaha bersifat pasif.

Apabila kita mengacu pada teori perlindungan hukum yang disampaikan oleh Philipus M. Hadjon, maka untuk perlindungan preventif kepada nasabah yang menderita kerugian dapat kita lihat dari beberapa sudut pandang yaitu:

[6] Philipus M. Hadjon, *Op. Cit.*, 2.

a. Perlindungan Hukum oleh Pemerintah terhadap nasabah bank yang menderita kerugian akibat kejahatan yang menggunakan teknologi informasi.

Lahirnya UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik; adalah wujud dari tanggung jawab yang diemban oleh negara yang memberikan perlindungan kepada masyarakat dalam aktivitas pemanfaatan teknologi informasi. Salah satu materi penting dari UU Informasi dan Elektronik, antara lain adanya pengakuan informasi dan/atau dokumen elektronik sebagai alat bukti hukum yang sah, pengakuan atas tandatangan elektronik, penyelenggaraan sertifikasi elektronik dan sistem elektronik.

Dalam UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, pemerintah juga mewajibkan kepada setiap penyelenggaraan elektronik untuk melakukan sebagai berikut :

"*Setiap Penyelenggara Sistem Elektronik harus menyelenggarakan Sistem Elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya Sistem Elektronik sebagaimana mestinya (Pasal 15 ayat (1))";*
"*Penyelenggara Sistem Elektronik bertanggung jawab terhadap penyelenggaraan Sistem Elektroniknya" (Pasal 15 ayat (2))";*
"Ketentuan sebagaimana dimaksud pada ayat (2) tidak berlaku dalam hal dapat dibuktikan terjadinya keadaan memaksa, kesalahan, dan/atau kelalaian pihak pengguna Sistem Elektronik (Pasal 15 ayat 1)".

Berdasarkan isi Pasal 15 ayat (1), (2), (3) tersebut di atas, secara jelas tanggung jawab Penyelenggara Sistem Elektronik dalam hal ini bank terhadap kerugian yang menimpa nasabahnya akibat tidak andalnya sistem elektronik yang ada pada bank tersebut, terkecuali apabila bank dapat membuktikan bahwa kerugian tersebut disebabkan oleh karena kesalahan dan/ kelalaian dari nasabah itu sendiri.

b. Peran dari Otoritas Moneter dalam hal ini Bank Indonesia dan /atau Otoritas Jasa Keuangan (OJK) dalam menanggulangi kejahatan berbasis teknologi informasi

Dalam rangka melakukan fungsi pengawasan terhadap perbankan, Bank Indonesia telah mengeluarkan Peraturan BI, khususnya yang menyangkut penggunaan teknologi informasi, antara lain:

(1) Peraturan Bank Indonesia Nomor 14/2/PBI/2012 tentang Perubahan Atas PBI No. 11/11/PBI/2009 tentang Penyelenggaraan Kegiatan Alat Pembayaran dengan Menggunakan Kartu.
(2) Surat Edaran Bank Indonesia Nomor 6/18/DPNP tanggal 20 April 2004 Perihal Penerapan Manajemen Risiko Pada Aktivitas layanan Jasa Bank Melalui Internet (*Internet Banking*).
(3) Peraturan Bank Indonesia Nomor 9/15/PBI/2007 tentang Penerapan Manajemen Risiko Dalam Penggunaan Teknologi Informasi Oleh bank Umum.

Peraturan-peraturan yang dikeluarkan oleh Bank Indonesia tersebut pada dasarnya ditujukan untuk meningkatkan keamanan, integritas data, dan ketersediaan layanan *electronik banking*, misalnya kewajiban bagi bank untuk melakukan hal-hal sebagai berikut :

(1) Bank wajib menerapkan manajemen risiko secara efektif dalam penggunaan Teknologi Informasi, yang dilakukan secara terintegrasi dalam setiap tahapan penggunaan TI, sejak proses perencanaan, pengadaan, pengembangan, operasional, pemeliharaan hingga penghentian dan penghapusan sumber daya Teknologi Informasi (TI).
(2) Bank wajib memiliki Komite Pengarah Teknologi Informasi (*Information Technology Steering Committee*) ;
(3) Bank wajib menyiapkan *Disaster Recovery Center* (DRC), yaitu fasilitas pengganti pada saat Pusat Data (Data Center) mengalami gangguan atau tidak dapat berfungsi oleh sebab terjadinya gangguan komputer ataupun sebab lainnya, yang digunakan sementara waktu selama dilakukan pemulihan Pusat data bank untuk menjaga kelangsungan kegiatan usaha (*business continuity*).
(4) *Business Continuity Plan* (BCP) adalah kebijakan dan prosedur yang memuat rangkaian kegiatan yang terencana dan terkoordinir mengenai langkah-langkah pengurangan risiko, penanganan dampak gangguan /bencana dan proses pemulihan agar kegiatan operasional Bank dan pelayanan kepada nasabah tetap dapat berjalan.
(5) Bank yang menyelenggarakan kegiatan *Electronic Banking* wajib memenuhi ketentuan BI yang berlaku dan bank harus memberikan edukasi kepada nasabah

mengenai produk *Electronic Banking* dan pengamanannya secara berkesinambungan.

(6) Setiap rencana penerbitan produk *electronik banking* baru harus di muat dalam Rencana Bisnis Bank.

Bank Indonesia membolehkan apabila bank menggunakan pihak penyedia jasa teknologi informasi sepanjang bank dan penyedia jasa teknologi informasi tersebut memenuhi persyaratan antara lain :

(1) Bank tetap bertanggung jawab atas penerapan manajemen risiko;
(2) Bank mampu untuk melakukan pengawasan atas pelaksanaan kegiatan Bank yang diselenggarakan oleh pihak penyedia jasa teknologi informasi.
(3) Pihak Penyedia Jasa harus menerapkan prinsip pengendalian Teknologi Informasi secara memadai yang dibuktikan dengan hasil audit yang dilakukan oleh pihak independen.
(4) Pihak Penyedia Jasa teknologi Informasi harus menyediakan akses bagi auditor intern bank, auditor ekstern yang ditunjuk bank, dan auditor Bank Indonesia untuk memperoleh data dan informasi yang diperlukan secara tepat waktu setiap kali dibutuhkan.
(5) Pihak penyedia jasa harus menyatakan tidak berkeberatan bila Bank Indonesia hendak melakukan pemeriksaan terhadap kegiatan penyediaan jasa tersebut.

c. Tanggung Jawab Bank selaku Penyelenggara Teknologi Informasi terhadap kerugian nasabah penyimpan

Pada prinsipnya hubungan antara Bank dengan Nasabah penyimpan dana bukan sekedar hubungan kontraktual biasa tetapi juga mengandung hubungan yang dilandasi dasar kepercayaan *(fiduciary relation).* Perjanjian antara Bank dengan nasabahnya khususnya nasabah yang menggunakan produk dan/atau jasa bank yang berbasis pada teknologi informasi seperti ATM maupun *Internet banking* merupakan bagian dari perjanjian pembukaan rekening, ATM, SMS-Banking ataupun *internet banking* adalah fasilitas yang dapat dipilih oleh nasabah dalam melakukan transaksi perbankan. Jadi perjanjian penggunaan produk/jasa yang berbasis teknologi informasi tidak dapat dipisahkan dari perjanjian pembukaan rekening yang dituangkan dalam formulir permohonan pembukaan rekening.

Aspek yang dapat menimbulkan kerugian bagi nasabah bank berkenaan dengan produk/jasa yang berbasiskan teknologi informasi secara umum dapat dibedakan, sebagai berikut:

(1) Akibat perbuatan manusia (*human error*) Perbuatan oleh manusia ini bisa dilakukan oleh pegawai bank baik dilakukan sendiri atau bekerja sama dengan pihak lain; perbuatan itu dilakukan sepenuhnya oleh pihak ketiga atau perbuatan itu dilakukan oleh nasabah baik sendiri maupun bekerja sama dengan pihak lain. Umumnya yang melakukan kejahatan-kejahatan ini dilakukan oleh orang-orang yang ingin mengambil keuntungan dan biasanya dilakukan oleh mereka yang ahli atau mengetahui tentang komputer.

(2) Akibat kesalahan Sistem (*system error*), mesin / komputer ataupun lemahnya pengamanan pada sistem komunikasi/jaringan maupun aplikasi.

Aspek-aspek yang dapat menimbulkan kerugian bagi nasabah bank berkenaan dengan produk/jasa yang berbasiskan teknologi informasi secara umum dapat dibedakan, sebagai berikut:

(1) Akibat perbuatan manusia *(human error)*, perbuatan oleh manusia ini bisa dilakukan oleh pegawai bank baik dilakukan sendiri atau bekerja sama dengan pihak lain; perbuatan itu dilakukan sepenuhnya oleh pihak ketiga atau perbuatan itu dilakukan oleh nasabah baik sendiri maupun bekerja sama dengan pihak lain. Umumnya yang melakukan kejahatan-kejahatan ini dilakukan oleh orang-orang yang ingin mengambil keuntungan dan biasanya dilakukan oleh mereka yang ahli atau mengetahui tentang komputer.

(2) Akibat oleh kesalahan Sistem (*system error*), mesin/komputer ataupun lemahnya pengamanan pada sistem komunikasi/jaringan maupun aplikasi.

(3) *Selain penyelesaian gugatan perdata, para pihak dapat menyelesaikan sengketa melalui arbitrase, atau lembaga penyelesaian sengketa alternatif lainnya sesuai dengan ketentuan Peraturan Perundang-undangan. (Pasal 39 ayat 2).*

Dari ketentuan tersebut di atas menjadi jelas bahwa seorang nasabah yang dirugikan oleh transaksi elektronik harus bisa membuktikan di Pengadilan bahwa kerugian yang ia derita adalah bukan karena kesalahan atau kelalaiannya namun oleh kelemahan atau kesalahan dari bank selaku penyelenggara sistim elektronik. Sebab

apabila nasabah tersebut tidak dapat membuktikannya dan pihak pihak bank yang dapat membuktikan sebaliknya bahwa kerugian nasabah terjadi oleh karena kesalahan atau kelalaian dari nasabah sendiri, maka gugatan nasabah tersebut akan ditolak oleh pengadilan. Apabila kerugian nasabah terjadi oleh karena dan sebab kejahatan yang dilakukan oleh pihak lain (pihak ketiga) di luar bank akibat kelemahan sistem teknologi informasi pada bank akan bank bertanggung jawab atas kerugian dari nasabah tersebut.

Bentuk tanggung jawab bank terhadap kerugian yang diderita oleh nasabah akibat kesalahan bank baik, oleh karena gagalnya sistem teknologi informasi bank maupun akibat kesalahan pegawai bank sesuai dengan Pasal 1367 ayat (1) KUH Perdata yang menyebutkan: " *Seseorang tidak saja bertanggung jawab untuk kerugian yang disebabkan perbuatannya sendiri, tetapi juga untuk kerugian yang disebabkan perbuatan orang-orang yang menjadi tanggungannya atau disebabkan oleh barang-barang yang berada di bawah pengawasannya"*.

Bentuk tanggung jawab bank terhadap kerugian nasabahnya juga diatur dalam UU Nomor 8 Tahun 1999 tentang Perlindungan Konsumen antara lain dalam Pasal 7 disebutkan beberapa kewajiban pelaku usaha :

- Huruf *f "Memberi kompensasi , ganti rugi, dan/atau penggantian atas kerugian akibat penggunaan, pemakaian, dan pemanfaatan barang dan/atau jasa yang diperdagangkan"*
- Huruf g *"Memberi kompensasi, ganti rugi , dan/atau penggantian apabila barang dan/atau jasa yang diterima atau dimanfaatkan tidak sesuai dengan perjanjian"*

Selanjutnya dalam Pasal 19 UU Nomor 8 Tahun 1999 tentang Perlindungan Konsumen, juga disebutkan:

(1) *Pelaku Usaha bertanggung jawab memberikan ganti rugi atas kerusakan, pencemaran, dan atau kerugian konsumen akibat mengonsumsi barang dan/atau jasa yang dihasilkan atau diperdagangkan.*

(2) *Ganti rugi sebagaimana dimaksud pada ayat (1) dapat berupa pengembalian uang atau penggantian barang dan/atau jasa yang sejenis atau setra nilainya, atau perawatan kesehatan dan/atau pemberian santunan yang sesuai dengan ketentuan peraturan perundang-undangan yang berlaku.*

(3) *Pemberian ganti rugi dilaksanakan dalam tenggang waktu 7 (tujuh) hari setelah tanggal transaksi.*

(4) *Pemberian ganti rugi sebagaimana dimaksud pada ayat (1) dan ayat (2) tidak menghapuskan kemungkinan adanya tuntutan pidana berdasarkan pembuktian lebih lanjut mengenai adanya unsur kesalahan.*

(5) *Ketentuan sebagaimana dimaksud pada ayat (1) dan ayat (2) tidak berlaku apabila pelaku usaha dapat membuktikan bahwa kesalahan tersebut merupakan kesalahan konsumen".*

Dari uraian di atas menjadi jelas bagi kita bahwa tanggung jawab bank selaku penyelenggara usaha terhadap nasabahnya selaku konsumen telah ada semenjak terjadinya perjanjian antara bank dengan nasabah (penyimpan) dan kewajiban bank apabila terjadi kerugian secara jelas telah diatur dalam UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik maupun UU Nomor 8 Tahun 1999 tentang Perlindungan Konsumen.

d. Upaya bank dalam mengantisipasi tindak kejahatan di bidang Teknologi Informasi

Upaya-upaya yang perlu dilakukan oleh bank dalam mengantisipasi kejahatan berbasiskan teknologi informasi, yaitu dengan pengamanan sistem dilakukan secara terintegrasi pada keseluruhan sub sistemnya, dengan tujuan mempersempit atau bahkan menutup celah-celah *unauthorized action* yang merugikan. Pengamanan secara personal dilakukan mulai dari tahap instalasi sistem, sampai pada akhirnya menuju pada tahap pengamanan fisik dan pengamanan data. Pengamanan jaringan dilakukan melalui pemasangan *firewall* pada Data Center, DRC dan pengamanan Web Server.

Manajemen Bank harus meyakini bahwa penerapan ***teknologi informasi*** di banknya mempunyai tujuan, sebagai berikut :

(1) Teknologi informasi secara langsung maupun tidak langsung harus memiliki dampak terhadap penciptaan produk pelayanan yang jauh lebih baik dari sebelumnya sehingga meningkatkan kinerja dan daya saing bank (*value adding activity*) ;

(2) Teknologi informasi harus dapat meningkatkan kualitas pengambilan keputusan dari manajemen dalam bentuk penyediaan informasi dan pengetahuan yang relevan, tepat, akurat, terpercaya, dan bernilai tinggi ;

(3) Teknologi informasi harus mampu untuk meningkatkan level perolehan pendapatan bank ***(revenue)*** dengan cara memanfaatkannya untuk semakin mendekatkan bank dengan para nasabahnya ;

(4) Teknologi informasi bank harus mampu menjamin adanya kepastian dan perlindungan hukum bagi para nasabah maupun pengguna jasa bank (non nasabah) dari setiap transaksi yang dilakukannya.

e. Peran Penegak Hukum dalam Mencegah Kejahatan Berbasis teknologi Informasi

Upaya memerangi kejahatan perbankan berbasis teknologi informasi merupakan tanggung jawab berskala internasional, hal ini tertuang dalam Resolusi Kongres PBB VIII/1990 mengenai *computer related crimes* yang menghimbau negara-negara anggota untuk mengintensifkan upaya-upaya penanggulangan penyalahgunaan komputer yang lebih efektif dengan mempertimbangkan langkah-langkah sebagai berikut[7]:

(1) Melakukan Modernisasi hukum pidana material dan hukum acara pidana;

(2) Mengembangkan tindakan-tindakan pencegahan dan pengamanan komputer;

(3) Melakukan langkah-langkah untuk membuat peka warga warga masyarakat, aparat pengadilan dan penegak hukum, terhadap pentingnya pencegahan kejahatan yang berhubungan dengan komputer;

(4) Melakukan upaya-upaya pelatihan bagi para hakim, pejabat dan aparat penegak hukum mengenai kejahatan ekonomi dan *cyber crime.*

(5) Memperluas *rule of ethics* dalam penggunaan komputer dan mengajarkannya melalui kurikulum informatika.

(6) Mengadopsi kebijakan perlindungan korban *cyber crime* sesuai dengan deklarasi PBB mengenai korban dan mengambil langkah-langkah untuk mendorong korban melaporkan adanya *cyber crime.*

[7] Roman V Veresha, "Preventive Measures Against Computer Related Crimes: Approaching An Individual", *Informatologia* 51, no. 3-4 (March 2018): 198.

Pendekatan yang bersifat preventif yang menjadi agenda PBB dalam upaya penanggulangan/pencegahan kejahatan, sebagaimana sering juga dikemukakan dalam kongres-kongres PBB mengenai "*the prevention of crime and the treatment of offenders*", yaitu :

(1) Pencegahan kejahatan dan peradilan pidana tidak diperlakukan/dilihat sebagai problem yang terisolir dan ditangani dengan metode yang simplistis dan fragmentaris, tetapi seyogianya dilihat sebagai masalah yang lebih kompleks dan ditangani dengan kebijakan / tindakan yang luas dan menyeluruh.

(2) Pencegahan kejahatan harus didasarkan pada penghapusan sebab-sebab dan kondisi-kondisi yang menyebabkan timbulnya kejahatan. upaya penghapusan sebab-sebab dan kondisi-kondisi yang demikian harus merupakan "strategi pokok / mendasar dalam upaya pencegahan kejahatan" (*the basic crime prevention strategy*).

(3) Penyebab utama dari kejahatan di banyak negara ialah ketimpangan sosial, diskriminasi rasial dan diskriminasi nasional, standar hidup yang rendah, pengangguran dan buta huruf (kebodohan) di antara golongan besar penduduk.

(4) Pencegahan kejahatan dan peradilan pidana seyogianya dipertimbangkan dalam hubungannya dengan pembangunan ekonomi, sistem politik, nilai-nilai sosio kultural dan perubahan masyarakat, juga dalam hubungannya dengan tata ekonomi dunia /internasional baru.

Dalam lingkup nasional pendekatan yang dapat dilakukan oleh aparat penegak hukum yang preventif antara lain :

(1) Menerapkan proteksi internet. Banyak sekali proteksi gratis yang bisa di download dan diinstal ke *personal computer* (PC). Apabila menggunakan *Microsoft Internet Explorer,* bukalah fitur proteksi *built-in* lewat menu *[Tools] [Internet Options] [Content] [Content Advisor]*. Sistem *content advisor* akan membaca *tag* khusus yang ada pada sebuah halaman *web*, lantas akan mengidentifikasikannya.

(2) Upaya preventif dengan pendekatan budaya/kultural pada dasarnya merupakan penanggulangan dengan cara mengetahui dan mematuhi etika dalam penggunaan internet, sehingga dapat menghindari penyalahgunaan dan dampak negatifnya.

Pendekatan ini merupakan salah satu kebijakan non penal dalam Resolusi Kongres PBB VII/1990 mengenai *computer related crimes*, yang menyatakan perlunya membangun/membangkitkan kepekaan warga masyarakat dan aparat penegak hukum terhadap masalah *cyber crime* dan menyebarluaskan/mengajarkan etika penggunaan komputer melalui media pendidikan[8].

(3) Kebijakan non penal dengan pendekatan *moral/edukatif* sangat dibutuhkan dalam penanggulangan *cyber crime* bahkan dapat dikatakan bahwa pendekatan ini sangat strategis apabila pendekatan teknologi dan etika kurang efektif. Adanya penanaman pendidikan moral dan agama, pengetahuan akan dampak negatif *cyber porn* dan semaksimal mungkin menutup potensi untuk mengakses pornografi akan lebih dapat menumbuhkan kesadaran dari setiap orang untuk menghindari pornografi, apa pun jenis dan medianya.[9]

(4) Pendekatan Global mengingat Internet sebagai ruang tanpa batas-batas teritorial antar negara di dunia (*transnasional*), menunjukkan bahwa dunia maya ini dalam pengaturan dan penanggulangan dampak negatifnya tidak mungkin dilakukan oleh negara secara sendiri-sendiri. Oleh karena itu diperlukan adanya ***pendekatan global*** dengan melakukan kerja sama antara aparat penegak hukum dalam bentuk kerja sama Internasional.

(5) Kerja sama aparat penegak hukum dengan instansi-instansi dan lembaga pendidikan. Instansi-instansi dan lembaga pendidikan yang memasang wi-fi, harus dibarengi dengan pemasangan *firewall*, sehingga semua konten tidak dapat masuk, termasuk konten yang mengandung porno aksi dan pornografi. Selain itu juga sering melakukan sidak terhadap ponsel dan memberikan sanksi yang tegas dan menimbulkan efek jera.

(6) Aparat Penegak Hukum (Polisi) hendaknya membentuk sebuah unit kesatuan khusus *(Cyber Police)* bekerja sama dengan institusi lainnya dan para ahli teknologi informasi yang menangani masalah kejahatan di dunia maya, termasuk

[8] Michael W Carroll, "Computer-Related Crimes American", *Criminal Law Review* 32, (2000): 193.
[9] Hukumonline.com, "Aturan tentang Cyber Pornography di Indonesia", https://www.hukumonline.com/klinik/a/aturan-tentang-icyber-pornography-i-diindonesia-lt4b86b6c16c7e4 (diakses 12 Desember 2021).

cyber crime. Jika di dunia nyata polisi berpatroli di jalan raya, maka *cyber police* berpatroli di dunia maya. Unit ini berupa tenaga teknis yang dibekali oleh software khusus yang dapat mengawasi serta melindungi transaksi elektronik di internet.

(7) Pemerintah melalui aparat penegak hukum melakukan sosialisasi secara luas melalui sekolah/kampus, instansi, LSM, paguyuban, menanamkan moral dan etika yang dimulai dari keluarga. Sebagai orang tua wajib untuk menanamkan moral dan etika bagi anak-anaknya. Keluarga merupakan lingkungan pendidikan yang pertama bagi anak-anak, untuk itu orang tua berkewajiban untuk mendidik, mengajarkan nilai-nilai agama dan edukasi bagi anak-anaknya, sehingga mereka memiliki moral, dan mental yang kuat dan mantap untuk tidak mudah menerima tanpa menyaring terlebih dahulu khususnya untuk hal-hal yang berbau pornografi yang sedang marak beredar lewat berbagai media seperti *handphone*, internet, majalah, dan VCD, orang tua harus tanggap dan bisa mengontrol dengan baik segala fasilitas yang diberikan kepada anak. Mengajarkan cara penggunaan teknologi ponsel, internet secara bijak.

Kebijakan melalui beberapa pendekatan dan beberapa upaya di atas diharapkan dapat menjadi filter maraknya *cyber crime*, khususnya dalam upaya penanggulangannya di Indonesia. Namun dalam aplikasi kebijakan ini sangat membutuhkan adanya kesadaran, kerja sama dan partisipasi semua pihak, baik pemerintah, aparat penegak hukum, dunia usaha, lembaga keuangan dan perbankan, dunia usaha, penyedia jasa internet, sekolah, kampus, orang tua, *user* dan kerja sama internasional agar dapat menghindari dampak negatif *cyber crime* dan memanfaatkan internet secara sehat sebagai sumber informasi dan untuk memperluas wawasan dan ilmu pengetahuan.

D. Penutup

Bank sebagai lembaga keuangan dalam menjalankan fungsi intermediasi adalah salah satu penggerak roda ekonomi suatu negara, yang mana dalam aktivitasnya tidak lepas dari penggunaan teknologi informasi guna mendukung operasionalnya. Penggunaan teknologi informasi oleh bank selain membawa dampak positif juga membawa dampak negatif yang

akan mengancam dan merugikan bank maupun nasabah apabila tidak dikelola secara baik. Kejahatan perbankan yang menggunakan teknologi *informasi (cyber crime)* tidak saja menimbulkan kerugian bagi nasabah maupun bank itu sendiri, namun dapat mengganggu perekonomian secara nasional.

Guna melindungi masyarakat (nasabah) dari *cybe rcrime* tesebut pemerintah maupun Otoritas Moneter (BI) dan Otoritas Jasa Keuangan (OJK) selaku pengawas bank berkoordinasi dengan aparat penegak hukum serta melalui lembaga perbankan itu sendiri baik dalam asosiasi maupun sendiri-sendiri perlu melakukan sosialisasi dan edukasi kepada masyarakat akan bahaya *cyber crime* karena dampak kerugian ekonomi yang ditimbulkan oleh kejahatan tersebut. Di samping itu perlu adanya peningkatan pengawasan terhadap bank-bank terutama dalam mengeluarkan izin prinsip bagi produk dan jasa bank yang berhubungan dengan teknologi informasi dan media internet.

Kepada para pelaku *cyber crime* perlu diberikan sanksi yang lebih berat dan hal penting yang juga perlu diperhatikan adalah peningkatan kualitas SDM dari para pengawas internal bank maupun pengawas eksternal dari Otoritas Jasa Keuangan (OJK); disamping itu lembaga perbankan selaku penyelenggara produk dan jasa yang berbasiskan pada teknologi informasi perlu memperketat sistem pengamanannya baik dari aplikasi dan sistem pada *Core Banking System* (CBS) yang ada di Data Center (DC) maupun pengamanan dari jaringan komunikasi yang digunakan oleh bank.

Mengingat *cyber crime* adalah lintas negara di mana modus operandi dapat dilakukan dari semua tempat (*global crime*) maka perlu adanya kerja sama antara penegak hukum dan Otoritas Moneter dengan lembaga sejenis baik secara bilateral, regional, dan internasional antara lain melalui perjanjian ekstradisi, *mutual assistance treaty* yang akan mempersempit para pelaku kejahatan dalam melakukan kegiatannya. Di samping itu perlunya mengikutsertakan masyarakat dalam memerangi kejahatan *Cyber Crime* merupakan salah satu upaya yang perlu dilakukan dalam mencegah dan memberantas para pelaku kejahatan ini.

Daftar Pustaka

Artikel Jurnal

Carroll, Michael W. "Computer-Related Crimes American". *Criminal Law Review* 32, (2000): 183-210. https://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=2535&context=facsch_lawrev.

Sari, Nani Widya. "Kejahatan Cyber Dalam Perkembangan Teknologi Informasi Berbasis Komputer". *Jurnal Surya Kencana Dua: Dinamika Masalah Hukum dan Keadilan* 5, no. 2 (Desember 2018): 577-593. http://download.garuda.kemdikbud.go.id/article.php?article=1696085&val=18449&title=kebijakan%20kriminal%20pemerintah%20terhadap%20kejahatan%20dunia%20maya%20cyber%20crime%20di%20indonesia/1000.

Veresha, Roman V. "Preventive Measures Against Computer Related Crimes: Approaching An Individual". *Informatologia* 51, no. 3-4 (March 2018): 189-199. https://doi.org/10.32914/i.51.3-4.7.

Buku

Hadjon, Philipus M. *Perlindungan hukum bagi rakyat Indonesia*. Surabaya: PT. Bina Ilmu, 1987.

Hamzah, Andi. *Hukum Pidana yang Berkaitan Dengan Komputer*. Jakarta: Sinar Grafika, 1993.

Peachey, Alan N. *Bencana Keuangan Besar Masa Kini (Great Financial Disaster of Our Time)*. Jakarta: Indonesian Risk Profesional Association (IRPA), 2007.

Artikel Online

Hukumonline.com. "Aturan tentang Cyber Pornography di Indonesia". https://www.hukumonline.com/klinik/a/aturan-tentang-icyber-pornography-i-diindonesia-lt4b86b6c16c7e4 (diakses 12 Desember 2021).

Peraturan Perundangan-Undangan

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Dan Transaksi Elektronik.

Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan Undang-Undang Nomor 7 Tahun 1992 Tentang Perbankan.

Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen.

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