JURNAL YUSTITIA
E-ISSN: 2723-0147
P-ISSN: 1978-9963
FACULTY OF LAW
UNIVERSITAS WIRALODRA
Jl. Ir. H. Djuanda KM. 03 Indramayu 45213 Telp. 0234-275599 Email: yustitia.fh@unwir.ac.id

KEJAHATAN ELEKTRONIK DENGAN PEMASANGAN SKIMER PADA SISTEM TRANSAKSI MESIN ATM

Murtiningsih

Universitas Wiralodra
Email : murti.kartini76@gmail.com

ABSTRACT

The pace of improvement in internet technology will not only have a positive impact, but negative things will also appear as side effects including skimming crimes which are included in the form of cybercrime. Skimmer crime with the mode of installing tools on ATMs as a form of cybercrime crime and legal steps in overcoming the Crime of using information systems and electronic transactions. Through primary and secondary data developed and analyzed and reviewing Law Number 11 of 2008 and Law Number 16 of 2019 concerning Electronic Information and Transaction where it is known that the mode of operation of ATM electronic crimes as a form of cybercrime and the application of electronic information and transaction laws as an effort to overcome the crime of using information systems and electronic transactions.

Keywords: Cybercrime, Skimmer crime, Crime of using information systems and electronic transactions.

I. PENDAHULUAN

Lembaga perbankan menjadi salah satu tumpuan harapan dalam menggerakan roda perekonomian nasional. Namun dari banyaknya perbankan baik swasta maupun pemerintah, tidak diiringi dengan pengawasan yang ketat terhadap praktek kejahatan perbankan yang semakin meningkat dari kuantitas dan kualitasnya dari waktu ke waktu serta munculnya berbagai kejahatan perbankan yang bersifat nasional maupun internasional.

Kejahatan perbankan tidak hanya dilakukan oleh pihak luar perbankan, namun ada juga yang melibatkan dari pihak perbankan itu sendiri. Banyak modus operandi kejahatan dalam dunia perbankan, salah satunya kejahatan dalam pemalsuan Kartu ATM dengan sarana internet. Mengingat tindak pidana pemalsuan Kartu ATM bersinggungan dengan suatu kegiatan atau ketentuan khusus dibidang perbankan dengan menggunakan kecanggihan teknologi.

Kemajuan dan perkembangan teknologi khususnya telekomunikasi, multimedia, dan teknologi informasi pada akhirnya dapat merubah tatanan organisasai dan hubungan

JURNAL YUSTITIA E-ISSN: 2723-0147 P-ISSN: 1978-9963
FACULTY OF LAW UNIVERSITAS WIRALODRA
Jl. Ir. H. Djuanda KM. 03 Indramayu 45213 Telp. 0234-275599 Email: yustitia.fh@unwir.ac.id

masyarakat. Hal ini tidaklah dapat dihindari karena flesibilutas dan kemampuan telematika dengan cepat memasuki aspek kehidupan manusia. Fenomena ini telah mengubah perilaku manusia dalam berinteraksi dengan manusia lain sehingga memunculkan norma-norma dan nilai-nilai baru[1].

Kebutuhan dan penggunaan teknologi informasi yang diaplikasikan dengan internet dalam segala bidang seperti e-banking, e-commerece, e-education dan masih banyak lagi menjadi suatu yang lumrah, apalagi di kota-kota besar. Internet telah menciptakan dunia baru yang dinamakan *cyberspace. Cyberspace* adalah istilah yang diciptakan oleh William Gibson, yaitu yang berhubungan dengan kumpulan komputer yang data elektroniknya dapat diakses satu sama lain[2].

Beberapa waktu terakhir ini sebagian warga masyarakat khususnya yang masih sering melakukan transaksi pengambilan uang melalui sejumlah ATM pada beberapa bank tertentu dibuat cukup gelisah. Sehubungan dengan cukup maraknya kasus pembobolan rekening nasabah pada beberapa bank tertentu dengan cara melakukan tindakan pemalsuan ATM. Kasus kejahatan perbankan dengan modus *card skimming* yang terjadi di Indonesia cukup meresahkan. Skimmer digunakan untuk mencuri data penting yang ada di Kartu ATM korban.

Kejahatan Informasi Teknologi (IT) atau *cybercrime* memiliki karakter yang berbeda dengan tindak pidana umum baik dari segi pelaku, korban, modus operandi, dan tempat kejadian perkara sehingga butuh penanganan dan pengaturan khusus di luar KUHP. Penggunaan Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana dirubah dengan Undang-undang Nomor 19 Tahun2016 tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, memberikan referensi hukum untuk menjerat aksi kriminalitas yang menggunakan sistem elektroni. Dalam UUITE telah diatur perbuatan yang terkait dengan tindak pidana siber termasuk perbuatan yang dilarang mendistribusikan informasi elektronik yang memiliki muatan penginaan atau pencemaran nama baik, perbuatan yang mengakibatkan terganggunya sistem elektronik, perbuatan yang dapat diaksesnya informasi elektronik yang memiliki muatan yang melanggar kesusilaan dan perjudian.

[1] Marwah Effendy, *Direksi, Penemuan Hukum, Korporasi & Tax amnesty dalam penegakan hukum*. Referensi, Jakarta, 2012, hlm. 45.
[2] https://glosarid.com/index.php/term/komputerinternet.cyberspace.xhtml. Data diakses tanggal 30 Oktober 2022, pkl 20:00wib.

JURNAL YUSTITIA E-ISSN: 2723-0147 P-ISSN: 1978-9963
FACULTY OF LAW UNIVERSITAS WIRALODRA
Jl. Ir. H. Djuanda KM. 03 Indramayu 45213 Telp. 0234-275599 Email: yustitia.fh@unwir.ac.id

UUITE juga jelas telah mengatur perbuatan yang dilarang untuk memperoleh informasi elektronik dan/atau dokumen elektronik serta yang merusak, menghilangkan, memindahkan informasi elektronik dan/ atau dokumen elektronik milik orang lain. Dengan demikian UUITE telah mengatur tentang konsekwensi hukum atas perusakan alat untuk memasukan Kartu ATM yang diganti dengan skimmer yang terjadi pada mesin-mesin ATM. Hal tersebut diatas menimbulkan masalah bagaimana pengaturan hukum terhadap kejahatan system elektronik ATM serta upaya pemerintah dalam menanggulangi kejahatan system elektronik ATM dengan pemasangan skimmer.

II. IDENTIFIKASI MASALAH

1. Bagaimanakah Pengaturan Hukum Terhadap Kejahatan System Elektronik ATM?
2. Bagaimana Upaya Pemerintah dalam Menanggulangi Kejahatan Sistem Elektronik ATM Dengan Pemasangan Skimmer?

III. METODE

Metode penelitian yang dipergunakan dalam penulisan ini adalah dengan yuridis normatif, yaitu melakukan penelitian terhadap peraturan perundang-undangan dan berbagai literatur yang berkaitan dengan penulisan. Tekhnik pengumpulan data yang menggunakan studi kepustakaan (library resreach) yaitu melakukan penelitian terhadap berbagai sumber bacaan seperti buku-buku, pendapat sarjana, bahan kuliah, surat kabar, artikel dan juga berita yang didapat dari internet yang bertujuan untuk memperoleh atau mencari konsepsi-konsepsi, teori-teori atau bahan-bahan atau doktrin-doktrin yang berkenaan dengan penulisan ini, dimana data yang diapakai adalah analisis kualitatif yaitu data yang didapat secara primer maupun sekunder disusun dengan sistematis kemudian disimpulkan sehingga diperoleh gambaran yang jelas.

IV. HASIL DAN PEMBAHASAN

A. Pengaturan Hukum Terhadap Kejahatan System Elektronik ATM

Teknologi informasi menyentuh setiap aspek kehidupan manusia yang dapat menimbulkan kejahatan, baik kejahatan itu dilakukan dengan menggunakan sarana-sarana dari sistem atau jaringan komputer, di dalam sistem atau jaringan komputer. Dalam kejahatan pencurian dana nasabah bank melalui

JURNAL YUSTITIA E-ISSN: 2723-0147 P-ISSN: 1978-9963
FACULTY OF LAW UNIVERSITAS WIRALODRA
Jl. Ir. H. Djuanda KM. 03 Indramayu 45213 Telp. 0234-275599 Email: yustitia.fh@unwir.ac.id

penggandaan kartu ATM, tindak kejatan tersebut dilakukan dengan menggunkan sarana dari sistem komputer dan terhadap sistem atau jaringan komputer, yaitu dengan mengambil data elektronik yang terdapat dalam kartu ATM korbannya dan memindahkan data elektronik tersebut pada pita magenik kartu ATM yang baru, dengan demikian pelaku dapat dengan leluasa menggunakan kartu ATM tersebut dan mengambil uang korbannya melalui mesin ATM[3]

Skimming adalah aktivitas menggandakan informasi yang terdapat dalam pita magnetik (magnetik srtpe) yang terdapat pada kartu kredit maupun ATM / Debit secara ilegal. Ini artinya dapat disimpulkan bahwa skimming adalah aktivitas yang berkaitan dengan upaya pelaku untuk mencuri data dari pita magnetik kartu ATM/Debit secara ilegal untuk memiliki kendali atas rekening korban. Laman bank tech menerangkan bahwa teknik pembobolan kartu ATM nasabah melalui teknik skimming pertama kali teridentifikasi pada 2009 lalu di ATM Citibank, Woodland Hills, California. Saat itu diketahui jika tenik skimming dilakukan dengan cara menggunakan alat yang ditempelkan pada slot mesin ATM (tempat memasukan kartu ATM) dengan alat yang dikenal dengan nama skimmer. Modus operasinya adalah mengkloning data dari magnetic stripe yang terdapat pada kartu ATM milik nasabah.

Sebagai informasi magnetic stripe adalah garis lebar hitam yang berada dibagian belakang kartu ATM. Fungsinya kurang lebih seperti tape kaset, material ferromagnetic yang dapat dipakai untuk menyimpan data (suara, gambar atau bit biner). Secara teknis, cara kerjanya mirip CD Writer pada komputer yang mampuh membaca CD berisi data, kemudian menyalinnya ke CD lain yang masih kosong. Dan isinya dapat dipastikan akan sama persis dengan CD asluinya. Skimmer bukan satu-satunya alat yang digunakan oleh para pelaku skimming. Para pelaku biasanya juga memanfaatakan kamera pengintai (spy cam) untuk mengetahui gerakan jari nasabah saat memasukan PIN kartu ATM.

Namun kamera pengintai sudah jarang digunakan seiring dengan semakin canggihnya alat skimmer yang digunakan para pelaku. Laman How Stuff Works melaporkan jika kini telah beredar pula jenis skimmer yang dilengkapi dengan

[3] Barda Nawawi Arief. MasalahPenegakan Hukum Dan Kebijakan Hukum Pidana Dalam Penanggulangan Kejahatan. Kencana Jakarta 2007 hal 243

JURNAL YUSTITIA E-ISSN: 2723-0147 P-ISSN: 1978-9963
FACULTY OF LAW UNIVERSITAS WIRALODRA
Jl. Ir. H. Djuanda KM. 03 Indramayu 45213 Telp. 0234-275599 Email: yustitia.fh@unwir.ac.id

kemampuan membaca kode PINkartu ATM. Dan hebatnya lagi, skimmer jenis ini juga bisa langsung mengirimkan data-data yang didapat via SMS pada pelaku. Berikut sistematis cara kerja pelaku skimming;

a) Pelaku mencari target mesin ATM yang ingin dipasangi skimmer. Keriteria yang dicari adalah mesin ATM yang tidak ada penjagaan keamanan, sepi dan tidak ada pengawasan yang memadai seperti CCTV yang tidak maksimal;
b) Pelaku memulai aksipencurian data nasabah dengan memasang alat skimmer pada mulut mesin ATM;
c) Melaui alat skimmer para pelaku menduplikasi data magnetic stripe pada kartu ATM lalu mengkloningnya ke dalam kartu ATM kosong. Proses ini bisa dilakukan dengan cara manual, dimana pelaku kembali ke ATM dan mengambil chip data yang sudah disiapkan sebelumnya. Atau bila pelaku sudah menggunakan alat skimmer yang lebih canggih, data-data yang telah dikumpulkan dapat diakses dari manapun. Umpamanya data dikirimkan via SMS.

Pengaturan hukum sebagai penegakan aturan terhadap tindak pidana di bidang teknologi informasi diatur di dalam Undang-undang Nomor 11 tahun 2008 tentang Informasi dan Teknologi Elektronik jo Undang-undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yang mana memuat ketentuan tentang unsur-unsur tindak pidana (perbuatan yang dilarang) di bidang ITE, antara lain dalam ketentuan pasal 27 sampai dengan pasal 36 Undang-undang Nomor 11 tahun 2008 tentang Informasi dan Teknologi Elektronik jo Undang-undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Adapun ketentuan pasal 27 ayat (1) sampai ayat (4) beserta perubahan penjelasannya sebagai berikut:

(1) Setiap orang dengan sengaja atau tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya informasi elektronik

JURNAL YUSTITIA E-ISSN: 2723-0147 P-ISSN: 1978-9963
FACULTY OF LAW UNIVERSITAS WIRALODRA
Jl. Ir. H. Djuanda KM. 03 Indramayu 45213 Telp. 0234-275599 Email: yustitia.fh@unwir.ac.id

dan/atau dokumen elektronik yang memiliki muatan yang melanggar kesusilaan;

(2) Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat dapat diaksesnya informasi elektronik dan/atau dokumen elektronik yang memiliki muatan perjudian;

(3) Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau membuat dapat diaksesnya informasi elektronik dan/atau dokumen elektronik yang memiliki muatan penginaan dan/atau pencemaran nama baik;

(4) Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dn/atau membuat dapat diaksesnya informasi elektronik dan/atau dokumen elektronik yang memiliki muaran pemerasan dan/atau pengancaman.

Perubahan dari penjelasan pasal tersebut adalah

(1) Yang dimaksud dengan "mendistribusikan" adalah mengirimkan dan/atau menyebarkan informasi elektronik dan/atau dokumen elektronik kepada orang banyak atau berbagai pihak melalui sistem elektronik.

Yang dimaksud dengan "mentransmisikan" dalah mengirimkan informasi elektronik dan/atau dokumen elektronik ditujukan kepada satu pihak lain melaui sistem elektronik.

Yang dimaksud dengan "membuat dapat diakses" adalah semua perbuatan lain selain mendistribusikan dan mentransmisikan melalui bsistem elektronik yang menyebabkan informasi elektronik dan/atau dokumen elektronik dapat diketahui pihak lain atau publik

(2) Cukup jelas.

(3) Ketentuan ini mengacu pada ketentuan pencemaran nama baik dan/atau fitnah yang daitur dalam Kitab Undang-undang Hukum Acara Pidana.

(4) Ketentuan ini mengacu pada ketentuan pemerasan dan/atau pengancaman yang diatur dalam Kitab Undang-undang Hukum Pidana (KUHP).

JURNAL YUSTITIA E-ISSN: 2723-0147 P-ISSN: 1978-9963
FACULTY OF LAW UNIVERSITAS WIRALODRA
Jl. Ir. H. Djuanda KM. 03 Indramayu 45213 Telp. 0234-275599 Email: yustitia.fh@unwir.ac.id

Ketentuan pasal 28 ayat (1) dan ayat (2) sebagai berikut :

(1) Setiap orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dan transaksi elektronik;
(2) Setiap orang dengan sengaja dan tanpa hak menyebarkan informasi yang diyunjukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama dan antar golongan (SARA).

Ketentuan pasal 29 sebagai berikut :

"Setiap orang dengan sengaja dan tanpa hak mengirimkan informasi elektronik atau dokumen elektronik yang berisi ancaman kekerasan atau menakut-nakuti yang ditunjukan secara pribadi"

Ketentuan pasal 30 ayat (1), ayat (2) dan ayat (3) sebagai berikut :

(1) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apapun;
(2) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apapun dengan tujuan untuk memperoleh informasi elektronik dan/atau dokumen elektronik;
(3) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atausistem elektronik dengan cara apapun dengan melanggar, menerobos, melampoi atau menjebol sistem keamanan.

Ketentuan pasal 31 ayatv (1) dan ayat (2) sebagai berikut :

(1) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas informasi elektronik dan/atau dokumen elektronik dalam suatu komputer dan/atau sistem elektronik tertentu milik orang lain;
(2) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atas transmisi informasi elektronik dan/atau dokumen elektronik yang tidak bersifat publik dari, ke, dan di dalam suatu komputer dan/atau sistem elektronik tertentu milik orang lain, baik yang tidak menyebabkan

JURNAL YUSTITIA E-ISSN: 2723-0147 P-ISSN: 1978-9963
FACULTY OF LAW UNIVERSITAS WIRALODRA
Jl. Ir. H. Djuanda KM. 03 Indramayu 45213 Telp. 0234-275599 Email: yustitia.fh@unwir.ac.id

perubahan apapun maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian informasi elektronik dan/atau dokumen elektronik yang sedang ditransmisikan.

Penambahan ayat (3) dan ayat (4) pada pasal 31 sebagai berikut :

(3) Ketentuan sebagaimana dimaksud pada ayat (1) dan ayat (2) tidak berlaku terhadap intersepsi atau penyadapan yang dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, atau instansi lainnya yang kewenangannya ditetapkan berdasarkan undang-undang;
(4) Ketentuan lebih lanjut mengenai tatacara intersepsi sebagaimana dimaksud pada ayat (3) diatur dengan undang-undang.

Ketentuan pasal 32 ayat (1) dan ayat (2) sebagai berikut :

(1) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apapun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu informasi elektronik atau dokumen elektronik milik orang lain atau milik publik;
(2) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apapunmemindahkan atau menstransfer informasi elektronik atau dokumen elektronik kepada sistem elektronik orang lain yang tidak berhak

Ketentuan pasal 33 sebagai berikut :

"Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apapun yang berakibat terganggunya sistem elektronik atau mengakibatkan sistem elektronik menjadi tidak bekerja sebagaimana mestinya".

Ketentuan pasal 34 ayat (1) sebagai berikut:

(1) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum memproduksi, menjual, menagadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki :
    a. Perangkat keras atau perangkat lunak komputer yang dirancang atau secara khusus dikembangkan untuk memfasilitasi perbuatan sebagaimana dimaksud dalam pasal 27 sampai dengan pasal 33;

JURNAL YUSTITIA E-ISSN: 2723-0147 P-ISSN: 1978-9963
FACULTY OF LAW UNIVERSITAS WIRALODRA
Jl. Ir. H. Djuanda KM. 03 Indramayu 45213 Telp. 0234-275599 Email: yustitia.fh@unwir.ac.id

b. 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.

Ketentuan pasal 35 sebagai berikut :

"Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan informasi elektronik dan/atau Dokumentasi elektronik dengan tujuan agar informasi elektronik dan/atau dokumen elektronik tersebut dianggap seolah-olah data yang autentik".

Ketentuan pasal 36 sebagai berikut :

"Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan perbuatan sebagaimana dimaksud dalam pasal 27 sampai dengan pasal 34 yang mengakibatkan kerugian bagi orang lain".

Berkenaan dengan unsur-unsur tindak pidana di bidang ITE tersebut, di dalam Undang-undang Nomor 11 tahun 2008 tentang Informasi dan Teknologi Elektronik jo Undang-undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, dirumuskan juga sejumlah ketentuan pidana di bidang ITE sebagaimana tercantum dalam pasal 45 sampai dengan pasal 52 dengan ketentaun sebagai berikut:

Ketentuan pasal 45 ayat (1), ayat (2) dan ayat (3) sebagai berikut:

(1) Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam pasal 27 ayat (1), ayat (2), ayata (3) dan ayat (4) dipidana dengan pidana penjara paling lama 6 (enam) tahun atau dendan paling banyak Rp 1.000.000.000,00 (satu milyar rupiah);
(2) Setiap orang memenuhi unsur sebagaimana dimaksud pasal 28 ayat (1) dan ayat (2) dipidana dengan pidana penjara paling lama 6 (enam) tahunatau denda paling banyak Rp 1,000.000.000,00 (satu milyar rupiah);

JURNAL YUSTITIA E-ISSN: 2723-0147 P-ISSN: 1978-9963
FACULTY OF LAW UNIVERSITAS WIRALODRA
Jl. Ir. H. Djuanda KM. 03 Indramayu 45213 Telp. 0234-275599 Email: yustitia.fh@unwir.ac.id

(3) Setiap orang yang memnuhi unsur sebagaimana dimaksud dalam pasal 29 dipidana dengan pdana penjara paling lama 12 (dua belas) tahun atau denda paling banyak Rp. 2.000.000.000,00 (dua milyar rupiah).

Penambahan ayat (4) dan ayat (5) pada pasal 45 sebagai berikut :

(4) Setiap orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentrasmisikan dan/atau membuat dapat diaksesnya informasi elektronik dan/atau dokumen elektronik yang memiliki muatan pemerasan dan/atau pengancaman sebagaimana dimaksud dalam pasal 27 ayat (4) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp 1.000.000.000,00 (satu milyar rupiah);

(5) Ketentuan sebagaimana dimaksud pada ayat (3) merupakan delik aduan.

Ketentuan pasal 45A Perubahan sebagai berikut:

(1) Setiap orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik sebagaimana dimaksud dalam pasal 28 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp 1.000.000.000,00 (satu milyar rupiah);

(2) Setiap orang dengan sengaja dan tanpa hak menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras dan anyar golongan (SARA) sebagaimana dimaksud dalam pasal 28 ayat (2) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp 1.000.000.000,00 (satu milyar rupiah).

Ketentuan pasal 45B Perubahan sebagai berikut :

“Setiap orang yang dengan sengaja dan tanpa hak mengirimkan informasi elektronik dan/atau dokumen elektronik yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi sebagaimana dimaksud dalam pasal 29 dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau denda paling banyak Rp 750.000.000,00 (tujuh ratus limapuluh juta rupiah)”.

JURNAL YUSTITIA E-ISSN: 2723-0147 P-ISSN: 1978-9963
FACULTY OF LAW UNIVERSITAS WIRALODRA
Jl. Ir. H. Djuanda KM. 03 Indramayu 45213 Telp. 0234-275599 Email: yustitia.fh@unwir.ac.id

Ketentuan pasal 46 ayat (1), ayat (2) dan ayat (3) 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 sebagaiman dimaksud dalam pasal 30 ayat (2) dipidana dengan pidana penjara paling lama 7 (tujuh) tahun atau denda paling banyak Rp 700.000.000,00 (tujuh ratus juta rupiah);
(3) Setiap orang yang memenuhi unsur sebagaiman dimaksud dalam pasal 30 ayat (3) dipidana dengan pidana penjara paling lama 8 (delapan) tahun atau denda paling banyak Rp 800.000.000,00 (delapan ratus juta rupiah)

Ketentuan pasal 47 sebagai berikut :

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

Ketentuan pasal 48 ayat (1), ayat (2) dan ayat (3) sebagai berikut :

(1) Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam pasal 32 (1) dipidana dengan pidana penjara paling lama 8 (delapan tahun) atau denda paling banyak Rp 2.000.000.000,00 (dua milyar ruiah);
(2) Setiap orang yang memenuhi usur sebagaiaman dimaksud dalam pasal 32 ayat (2) dipidana paling paling lama 9 (sembilan) tahun atau denda Rp 3.000.000.000,00 (tiga milyar rupiah);
(3) Setiap orang yang memenuhi unsur sebagaiman dimaksud dalam pasal 32 ayat (3) dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun atau denda paling banyak Rp 5.000.000.000,00 (lima milyar rupiah).

Ketentuan pasal 49 sebagai berikut :

"Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam pasal 33 dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun atau denda paling banyak Rp 10.000.000.000,00 (sepuluh milyar rupiah)".

JURNAL YUSTITIA E-ISSN: 2723-0147 P-ISSN: 1978-9963
FACULTY OF LAW UNIVERSITAS WIRALODRA
Jl. Ir. H. Djuanda KM. 03 Indramayu 45213 Telp. 0234-275599 Email: yustitia.fh@unwir.ac.id

Ketentuan pasal 50 sebagai berikut:

"Setiap orang yang memenuhi unsur sebagaimana yang dimaksud dalam pasal 34 ayat (1) dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun atau denda paling banyak Rp 10.000.000.000,00 (sepuluh milyar rupiah)".

Ketentuan pasal 51 ayat (1) dan ayat (2) sebagai berikut :

(1) Setiap orang yang memenuhi unsur sebagaimana yang dimaksud dalam pasal 35 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun atau denda paling banyak Rp 12.000.000.000,00 (dua belas milyar rupiah);
(2) Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam pasal 36 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun atau denda paling banyak Rp 12.000.000.000,00 (dua belas milyar rupiah).

Ketentuan pasal 52 ayat (1) dan ayat (2) sebagai berikut :

(1) Dalam hal tindak pidana sebagaimana dimaksud dalam pasal 27 ayat (1) menyangkut kesusilaan atau eksploitasi seksual terhadap anak dikenakan pemberatan sepertiga dari pidana pokok;
(2) Dalam hal perbuatan sebagaimana dimaksud dalam pasal 30 samapai dengan pasal 37 ditujukan terhadap komputer dan/atau sistem elektronik serta informasi elektronik dan/atau dokumen elektronik milik pemerintah dan/atau yang digunakan untuk layanan publik dipidana dengan pidana pokok ditambah sepertiga.

B. Upaya Pemerintah Dalam Menanggulangi Kejahatan System Elektronik ATM Dengan Pemasangan Skimmer

Perkembangan ilmu pengetahuan dan teknologi khususnya teknologi informasi dan komunikasi telah menimbulkan pengaruh hamper dalam seluruh aspek kehidupan manusia dan kegiatannya di masyarakat termasuk di bidang perbankan nasional memberikan kemudahan bagi nasabah bank, sebagian besar bank pada saat ini bahkan mengandalkan teknologi informasi dan media elektronik sebagai dasar pelayanannya, seiring dengan kemudahan untuk melakukan transformasi secara cepat melalui pemanfaatan teknologi ternyata dari

JURNAL YUSTITIA E-ISSN: 2723-0147 P-ISSN: 1978-9963
FACULTY OF LAW UNIVERSITAS WIRALODRA
Jl. Ir. H. Djuanda KM. 03 Indramayu 45213 Telp. 0234-275599 Email: yustitia.fh@unwir.ac.id

segi hokum membawa konsekwensi tersendiri. Konsekwensi hukum yang terlihat yakni bentuk kejahatan hokum yang mengarah kepada suatu perbuatan kriminal[4].

Penanggulangan kejahatan dengan menggunakan hokum pidana merupakan bagian dari kebijakan criminal. Penanggulangan kejahatan tersebut adalah dalam rangka untuk mencapai tujuan akhir dari kebijakan criminal itu sendiri yaitu memberikan perlindungan masyarakat dalam rangka untuk mencapai kesejahteraan bagi masyarakat. Dalam hal ini, terhadap tindak pidana pencurian nasabah bank melalui penggandaan kartu ATM harus dilakukan upaya represif atau tindakan hukum. Upaya represif atau tindakan hukum yang dilakukan oleh polisi atau penyidik dilaksanakan sesuai dengan peraturan perundang-undangan yang berlaku. Banyak sekali kasus-kasus yang terjadi akibat imbas dari undang-undang informatika dan transaksi elektronik yang banyak dipertanyakan oleh para ahli. Sehingga terjadilah revisi undang-undang informasi dan transaksi elektronik pada tahun 2016. Perubahan undang-undang informasi dan transaksi elektronik telah disahkan menjadi Undang-undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Maka ditinjau dari modus operasi yang dilakukan oleh para pelaku kejahatan penggunaan system elektronik dengan modus operasi skiming dengan menggunakan alat skimmer dapat dikategorikan dalam UUITE tersebut.

Tindakan hukum terhadap pencurian atau pembobolan dana pada bank diantaranya dengan menjerat pelaku pencurian dana nasabah bank melalui modus skimmer. Hal tersebut menandakan bahwa harus terdapat aturan dan sanksi yang tegas kepada para pelaku tindak pidana pencurian atau pembobolan dana pada bank, dengan tujuan agar masyarakat dan pelaku takut serta tidak akan melakukan tindak pencurian dana nasabah dengan modus skimmer dan sebagai efek jera.

V. PENUTUP

A. Simpulan

Dari pembahasan-pembahasan sebelumnya dapat disimpulkan antara lain sebagai berikut:

[4] Budi Agus Riswandi, *Aspek hukum internet banking*, Rajawali pres, Jakarta 2005, hlm. 188.

JURNAL YUSTITIA E-ISSN: 2723-0147 P-ISSN: 1978-9963
FACULTY OF LAW UNIVERSITAS WIRALODRA
Jl. Ir. H. Djuanda KM. 03 Indramayu 45213 Telp. 0234-275599 Email: yustitia.fh@unwir.ac.id

1. Kejahatan perbankan yang berbasis teknologi dan informasi salah satunya yang menterang system perbankan berupa skiming melalui penggandaan kartu ATM dengan menggunakan teknologi komputer dan memanipulasi data dengan cara memindahkan data elektronik yang terdapat pada kartu ATM korbannya ke kartu ATM milik pelaku. Pencurian dana nasabah bank melalui penggandaan kartu ATM atau skimmer telah menjadi ancaman stabilitas dan rasa aman nasabah bank. Oleh karenanya pengaturan hukum terhadap kejahatan system elektronik ATM telah diatur pemerintah dengan merubah UUITE yaitu melalui Undang-undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

2. Penanggulangan kejahatan system elektronik ATM dengan pemasangan skimmer oleh pemerintah dilakukan melalui dua tindakan yaitu melalui tindakan represif dan preventif. Tindakan atau kebijakan represif melalui penegakan sarana pidana, yaitu perumusan pidana dan pemidanaan yang telah dilegalkan melalui perundang-undangan. Sedangkan tindakan atau kebijakan prefentif yaitu upaya penanggulangan kejahatan dengan tidak melakukan hukum pidana, yakni upaya penanggulangan oleh pihak perbankan dan nasabah serta stoke holder yang terkait (penegak hukum).

B. Saran

1. Perbankan harus melakukan pengendalian pengamanan fisik terhadap peralatan dan ruangan yang digunakan terhadap bahaya pencurian, pengerusakan dan tindakan kejahatan lainnya oleh pihak yang tidak berwenang. Selain itu perbankan juga harus melakukan pemantauan secara rutin untuk menjamin keamanan dan kenyamanan bagi nasabah pengguna jasa perbankan. Seperti peningkatan keamanan pada system elektronik, diantaranya pada kondisi mesin ATM sebagai alat transaksi.

2. Pemerintah juga harus melakukan tindakan hukum dan upaya represif yang dapat dilakukan terhadap tindak pencurian dana pada bank, diantaranya dengan menerapkan Undang-undang Nomor 11 tahun 2008 tentang Informasi dan Teknologi Elektronik jo Undang-undang Nomor 19 Tahun 2016 tentang

Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik untuk menjerat pelaku pelaku pencurian dana nasabah bank melalui modus skimmer. Hal tersebut diharapakan terdapat aturan dan sanksi yang tegas terhadap para pelaku tindak pidana pencurian atau pembobolan dana nasabah pada bank, sebagai tujuan agar masyarakat dan pelaku takut serta tidak akan melakukan tindakan pencurian dana nasabah bank dengan modus skimmer juga sebagai efek jera terhadap pelaku kejahatan tersebut.

DAFTAR PUSTAKA

1. Buku & Jurnal

Barda Nawawi Arief. MasalahPenegakan Hukum Dan Kebijakan Hukum Pidana Dalam Penanggulangan Kejahatan. Kencana Jakarta 2007

Budi Agus Riswandi, *Aspek hukum internet banking*, Rajawali pres, Jakarta 2005,

Marwah Effendy, *Direksi, Penemuan Hukum, Korporasi & Tax amnesty dalam penegakan hukum*. Referensi, Jakarta, 2012,

2. Peraturan Perundang-undangan

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

Undang-undang Nomor 16 Tahun 2019 tentang Informasi dan Transasksi Elekrtonik

3. Sumber Lainya

https://glosarid.com/index.php/term/komputerinternet.cyberspace.xhtml. Data diakses tanggal 30 Oktober 2022,