

BAB I

PENDAHULUAN

A. Latar Belakang Masalah

Bank memiliki peranan penting dalam dunia perbankan di Indonesia, di mana bank sebagai perantara dalam sarana lalu lintas pembayaran perekonomian di Indonesia. Dengan produk-produknya, perbankan mampu membantu masyarakat dalam sarana lalu lintas pembayaran setiap transaksinya. Kasmir menyatakan bahwa, “bank diartikan sebagai lembaga keuangan yang kegiatan usahanya adalah menghimpun dana dari masyarakat dan menyalurkan kembali dana tersebut ke masyarakat serta memberikan jasa-jasa lainnya.”¹

Menurut Pasal 1 Undang-Undang Nomor 7 Tahun 1992 sebagaimana diubah dengan Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan selanjutnya disebut UU Perbankan, 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.

Disinilah terlihat adanya hubungan yang sangat sinergi antara bank dengan nasabahnya, di mana nasabah yang menggunakan bank sebagai bagian dari kehidupan perekonomiannya dan menaruh kepercayaan yang sangat tinggi terhadap bank dikarenakan terdapatnya data-data nasabah yang harus dijaga kerahasiaannya oleh bank itu sendiri. Maka dari itu, bank sebagai lembaga penghimpun dan penyalur dana masyarakat dalam menjalankan usahanya, harus mematuhi aturan yang ada. Pada Pasal 40 Ayat (1) UU Perbankan, terdapat prinsip kerahasiaan bank yaitu prinsip yang dianut oleh setiap bank di dalam melaksanakan kegiatan operasionalnya. Prinsip kerahasiaan bank ini diperlukan guna melindungi data-data nasabah bank dari pihak-pihak yang tidak memiliki kepentingan yang dapat merugikan nasabah.

¹Kasmir, *Dasar-Dasar Perbankan*, Raja Grafindo Persada, Jakarta, 2012, hlm, 3.

Sektor perbankan sebagai bagian dari sektor keuangan menjelma menjadi bagian yang tidak terpisahkan dari kehidupan sehari-hari. “Perbankan merupakan sektor yang rentan terkena serangan siber, baik pelaku industri perbankan maupun nasabah terdampak oleh insiden siber di sektor tersebut. Ancaman siber sektor perbankan membutuhkan perhatian dari berbagai pihak agar tidak menjadi insiden siber.”²

“Bank yang merupakan salah satu penyelenggara sistem elektronik wajib menerapkan manajemen risiko terhadap kerusakan atau kerugian yang ditimbulkan dalam hal merumuskan langkah mitigasi dan penanggulangan untuk mengatasi ancaman, gangguan, dan hambatan terhadap sistem elektronik yang dikelolanya.”³ Bank meningkatkan kualitas layanan mereka demi mempermudah nasabah sekaligus menarik nasabah baru agar mau menabung di bank. Salah satu caranya adalah menggunakan perkembangan teknologi.

Kemajuan teknologi dalam dunia perbankan memberikan sumbangsih yang signifikan terhadap kemudahan bertransaksi, di mana bank harus meningkatkan teknologi untuk meningkatkan layanan pada nasabah. Semakin tinggi teknologi yang digunakan dalam melayani nasabah maka semakin besar peluang pasar. Sehingga terbentuk *image* oleh masyarakat bahwa bank yang *bonafide* adalah bank yang menggunakan teknologi yang canggih yang memudahkan nasabah bertransaksi baik dari waktu yang digunakan ataupun biaya yang dikeluarkan untuk melakukan transaksi. Teknologi yang dimaksud seperti ATM (*Auto Teller Machine*), kartu kredit, dan lain-lain. Dengan adanya teknologi ini tentu menimbulkan jaringan-jaringan atau penggunaan database bank, dimana database bank ini nantinya akan disimpan dalam suatu *server*.

²Badan Siber dan Sandi Negara, <https://bssn.go.id/bssn-terbitkan-profil-risiko-sektor-perbankan-sebagai-pelaku-industri-perbankan-dan-masyarakat-memitigasi-ancaman-kerentanan-siber>, diakses pada 30 November 2022.

³Pasal 13 Peraturan Pemerintah Republik Indonesia Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

Perkembangan teknologi saat ini membawa dampak yang sangat besar dalam berbagai bidang kehidupan. Indonesia mulai menerapkan teknologi dalam perkembangan kehidupan masyarakatnya. Pasal 28 (c) Undang-Undang Dasar 1945, menyatakan bahwa:

“Setiap orang berhak mengembangkan diri melalui pemenuhan kebutuhan dasarnya, berhak mendapat pendidikan dan memperoleh manfaat dari ilmu pengetahuan dan teknologi, seni dan budaya, demi meningkatkan kualitas hidupnya dan demi kesejahteraan umat manusia.”

Salah satunya perkembangan teknologi yaitu internet. Internet adalah sarana teknologi yang paling berkembang saat ini, internet menghubungkan jutaan orang di seluruh dunia tanpa mengetahui keberadaan mitra komunikasi mereka. Informasi dapat dikirim dalam berbagai bentuk seperti audio, gambar, teks, data, atau kombinasinya.

Internet adalah singkatan dari *Interconnected Network* karena fungsinya untuk menghubungkan jaringan-jaringan komputer di seluruh dunia. Secara etimologis internet adalah “jaringan yang menghubungkan banyak komputer di tempat yang berbeda untuk terhubung dan bertukar data dan juga bertukar informasi.”⁴

Kehidupan manusia pada zaman sekarang tak luput dari Jaringan komputer dan internet. Perkembangan teknologi informasi dan komputer (TIK) telah membuat langkah yang cepat dan juga berjalan sedemikian rupa. Ini terjadi setelah ditemukannya teknologi penghubung komputer dan internet. Teknologi informasi adalah “teknologi yang digunakan untuk mengolah data, termasuk mengolah, mengumpulkan, menyusun, menyimpan, dan mengolah data dengan berbagai cara untuk menghasilkan informasi yang spesifik, berkualitas, informasi yang relevan, akurat, dan tepat waktu, digunakan untuk keperluan pribadi, perusahaan, pemerintahan dan merupakan informasi strategis untuk pengambilan keputusan. Teknologi ini menggunakan

⁴Jubilee Enterprise, *Panduan Memilih Koneksi Internet untuk Pemula*, PT Elex Media Komputindo, Jakarta, 2013, hlm, 2.

kumpulan komputer untuk memproses data dari jaringan untuk menghubungkan satu komputer ke komputer lain saat dibutuhkan.”⁵

Kemajuan teknologi informasi dan telekomunikasi telah membantu masyarakat dalam memudahkan pekerjaan menjadi lebih sederhana, sehingga hampir seluruh bidang kehidupan menggunakan teknologi.

Peran teknologi dalam dunia perbankan sangatlah mutlak, semakin berkembang dan kompleksnya fasilitas yang diterapkan perbankan untuk memudahkan pelayanan, itu berarti semakin beragam dan kompleks adopsi teknologi yang dimiliki oleh suatu bank. Tidak dapat dipungkiri, dalam setiap bidang termasuk perbankan penerapan teknologi bertujuan selain untuk memudahkan operasional internal perusahaan, juga bertujuan untuk semakin memudahkan pelayanan terhadap customers. Apalagi untuk saat ini, khususnya dalam dunia perbankan sistem semua produk yang ditawarkan kepada customers serupa, sehingga persaingan yang terjadi dalam dunia perbankan adalah bagaimana memberikan produk yang serba mudah dan serba cepat. Pemanfaatan teknologi ini tidak hanya berdampak positif saja kepada masyarakat, namun juga diikuti oleh dampak negatif. Salah satu efek/dampak yang ditimbulkan oleh kemajuan teknologi ini adalah Kejahatan Siber / *Cyber Crime*.

Kecenderungannya terbukti, bahwa semakin maju dan modern kehidupan masyarakat, maka semakin maju dan modern pula jenis dan modus operandi kejahatan yang terjadi di tengah masyarakat. Kejahatan teknologi informasi atau dikenal dengan istilah *cyber crime* merupakan permasalahan yang harus ditangani secara serius. Hal ini dikarenakan dampak dari kejahatan ini sangat luas dan banyak merugikan perekonomian masyarakat. Apabila tidak ditanggulangi secara dini, maka kejahatan tersebut akan berkembang dan dampaknya akan sangat fatal bagi kehidupan bermasyarakat.

⁵Agus Mulyanto, Sumarsono dan M. Taufiq Nuruzzaman, *Pengantar Teknologi Informasi*, Modul Bahan Ajar Teknik Informatika Universitas Islam Negeri Sunan Kalijaga, Yogyakarta, hlm, 2.

Cybercrime memiliki karakter yang khas dibandingkan kejahatan konvensional, antara lain:

1. Perbuatan yang dilakukan secara ilegal, tanpa hak atau tidak etis tersebut terjadi di ruang/wilayah maya (cyberspace), sehingga tidak dapat dipastikan yurisdiksi hukum negara mana yang berlaku terhadapnya;
2. Perbuatan tersebut dilakukan dengan menggunakan peralatan apapun yang bisa terhubung dengan internet; dan
3. Perbuatan tersebut mengakibatkan kerugian materil maupun immateril (waktu, nilai, jasa, uang, barang, harga diri, martabat, kerahasiaan informasi) yang cenderung lebih besar dibandingkan kejahatan konvensional.
4. Pelakunya adalah orang yang menguasai penggunaan internet beserta aplikasinya. Perbuatan tersebut seringkali dilakukan secara transnasional atau melintasi batas negara.⁶

Tindak pidana *cybercrime* di Indonesia telah diatur dalam Undang-Undang Nomor 11 tahun 2008 dan telah diperbarui dengan Undang-Undang Nomor 19 tahun 2016 tentang informasi dan transaksi elektronik (ITE). Undang-Undang ITE tidak memberikan definisi mengenai *cybercrime*, tetapi membaginya menjadi beberapa pengelompokan yang mengacu pada *Conventions on cybercrime*.⁷

Secara ringkas dapat dikatakan bahwa “*cybercrime* dapat di definisikan adalah segala bentuk kejahatan yang terjadi di dunia maya atau internet. *Cybercrime* merupakan tindakan kriminal yang dilakukan dengan menggunakan teknologi komputer sebagai alat kejahatan utama.”⁸ *Cybercrime* yaitu “kejahatan yang memanfaatkan perkembangan teknologi komputer khususnya internet. *Cybercrime* didefinisikan sebagai perbuatan melanggar hukum yang memanfaatkan teknologi komputer yang berbasis pada kecanggihan perkembangan teknologi internet.”⁹

⁶Deris Setiawan, *Sistem Keamanan Komputer*, PT Elex Media Komputindo, Jakarta, 2005, hlm, 40.

⁷Josua Sitompul, *Landasan Hukum Penanganan Cybercrime Di Indonesia* <https://www.hukumonline.com/klinik/detail/ulasan/cl5960/landasan-hukum-penanganan-crime-di-indonesia/>, diakses pada tanggal 30 November 2022.

⁸Agus Rahardjo, *Cybercrime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, PT Citra Aditya Bakti, Bandung, 2002, hlm, 12.

⁹Budi Raharjo, *Memahami Teknologi Informasi*, Elexmedia Komputindo, Jakarta, 2002, hlm, 2.

Cybercrime telah banyak terjadi di Indonesia, yang baru baru ini terjadi adalah *skimming* yang dilakukan melalui mesin anjungan tunai mandiri (ATM). Menurut Dian Eka Kudusma Wardani dalam jurnalnya, menjelaskan “*skimming ATM* adalah tindakan pencurian informasi kartu kredit atau debit dengan cara menyalin informasi yang terdapat pada kartu ATM secara ilegal. Pelaku bisa mendapatkan data nomor kartu kredit atau debit korban dengan menggunakan perangkat elektronik kecil yaitu *skimmer* untuk menggesek kartu lalu menyimpan ratusan nomor kartu debit korban.”¹⁰

ATM merupakan terminal elektronik yang disediakan bank yang membolehkan nasabahnya untuk melakukan berbagai transaksi, diantaranya untuk melakukan penarikan tunai dari rekening simpanannya di bank, melakukan setoran, cek saldo, atau transaksi pemindahan dana. Pemanfaatan ATM “merupakan sejauh mana seseorang yakin bahwa dengan menggunakan teknologi dapat meningkatkan kinerja pekerjaannya sehingga mengambil keputusan untuk menggunakan ATM karena dinilai lebih efisien dan efektif.”¹¹

Skimming ATM dilakukan dengan mekanisme mencuri data nasabah tersimpan dalam magnetik strip pada kartu ATM dan dikirim secara nirkabel. Cara pencurian data ini dilakukan dengan beberapa langkah, yaitu umumnya pertama- tama pelaku memasang alat *skimmer* pada mulut mesin ATM sehingga pelaku mendapatkan data di kartu si nasabah, lalu pelaku memasang kamera tersembunyi untuk menangkap gerakan jari nasabah saat menekan pin ATM yang ditutupi.¹²

Skimming ATM tersebut telah melanggar Undang-Undang Nomor 11 Tahun 2008 dan telah diperbarui dengan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan

¹⁰Dian Eka Kusuma Wardani dan Maskun, “Kejahatan Skimming Sebagai Salah Satu Bentuk Cyber Crime”, *Jurnal Jurisprudentie*, Vol. 6, No. 1, 2019, hlm, 169.

¹¹Delima Sari Lubis, “Faktor-Faktor yang Mempengaruhi Pemanfaatan ATM bagi Nasabah Perbankan”, *Jurnal At- qTijarah*, Vol. 3, No. 1, 2017, hlm, 112.

¹²R. Toto Sugiharto, *Tips ATM Anti Bobol: Mengenal Modus-modus Kejahatan Lewat ATM dan Tips Cerdik Menghindarinya*, Media Pressindo, Yogyakarta, 2010, hlm, 144.

Transaksi Elektronik (ITE). Didalam KUHP dan Undang-undang ITE tidak ditemukan pengertian terkait tindak pidana *skimming*, tetapi tindak pidana *skimming* termasuk kedalam tindak pidana yang secara melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dimana hal tersebut diatur didalam Undang-undang ITE.

Sebagai salah satu contoh kasus bahwa pada tanggal 14 Februari 2021 terdapat pengaduan dari beberapa nasabah Bank BRI yang berjumlah 35 (tiga puluh lima) nasabah melapor ke Kantor BRI Cab. Tegal, KCP BRI Adiwerna, dan Kanca BRI Slawi yang intinya menyampaikan bahwa 35 (tiga puluh lima) nasabah tersebut tidak pernah melakukan transaksi keuangan. Setelah di telusuri berdasarkan laporan tersebut kemudian diketahui telah terjadi *skimming* di mesin ATM BRI Batalyon Yonif 407 Tegal Slawi. Bahwa dari penelusuran tersebut berdasarkan rekaman CCTV di ATM BRI Batalyon Yonif 407 Tegal Slawi diketahui terdapat 2 (dua) orang pelaku menggunakan jaket dan helm memasang alat *skimmer* nya tanggal 15 Januari 2021 pukul **05.02:23** (waktu system) dan melepas alatnya tanggal 16 Januari 2021 **04.33:49** (waktu system). Bahwa setelah pihak Bank BRI melakukan audit keuangan berdasarkan laporan rekening 35 (tiga puluh lima) nasabah tersebut di ketahui jumlah keseluruhan uang nasabah tersebut jumlah total nominal sebesar Rp202.850.000,- (dua ratus dua juta delapan ratus lima puluh ribu rupiah).

Pada tanggal 31 Januari 2022 telah diputuskan oleh Pengadilan Negeri Slawi mengenai pembedaan Kedua Terdakwa dalam Putusan dengan nomor perkara 106 /Pid.Sus/2021/PN Slw dengan menetapkan pidana penjara masing-masing pelaku selama 3 (tiga) tahun dan denda sebesar Rp200.000.000,- (dua ratus juta) subsidair 2 (dua) bulan kurungan.¹³

¹³Direktori Putusan Mahkamah Agung Republik Indonesia
<https://putusan3.mahkamahagung.go.id/direktori/putusan/zaebc999cb5746aa8a3a313031333134.html>,
diakses pada tanggal 21 Desember 2022.

Undang-Undang Nomor 11 Tahun 2008 yang telah diperbaharui dengan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (ITE) dijadikan acuan dan dasar hukum oleh Hakim dalam menjatuhkan putusan perkara nomor 106 /Pid.Sus/2021/PN Slw, meskipun belum diatur secara khusus mengenai *skimming* tetapi hakim dalam menjatuhkan putusan menimbang dan meyakini untuk menjatuhkan dalam Undang-Undang ini, lebih jelasnya di atur dalam Pasal 30 ayat (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”

Ancaman pidana Pasal 46 ayat (2):

“Setiap orang yang memenuhi unsur sebagaimana 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).”

Berdasarkan Pasal 50 Undang-Undang Nomor 48 Tahun 2009 tentang Kekuasaan Kehakiman dinyatakan bahwa putusan pengadilan harus memuat alasan dan dasar putusan, serta memuat pasal tertentu dari peraturan perundang-undangan yang bersangkutan atau sumber hukum tak tertulis yang dijadikan dasar untuk mengadili. Setiap putusan pengadilan harus ditandatangani oleh ketua serta hakim yang memutus dan panitera yang ikut serta bersidang. Putusan pengadilan haruslah bersifat objektif dan didukung oleh pertimbangan pertimbangan hukum yang menjadi alasan bagi hakim dalam memutus perkara. Pertimbangan pertimbangan hukum tersebut harus mampu dipertanggungjawabkan oleh hakim yang mengeluarkan putusan.

Berdasarkan hal tersebut diatas, penanggulangan kejahatan *skimming* ATM harus dilakukan dengan kebijakan formulasi hukum agar diharapkan menekan atau menanggulangi kejahatan ini. Indonesia sendiri belum mengatur secara khusus perundang-undangan tentang kejahatan *skimming* ATM, untuk itulah perlu dilakukan upaya pencegahan dan penanggulangan terhadap perbuatan *skimming* ATM sebagai sebuah tindak pidana agar tidak

semakin meluas dan membahayakan masyarakat. Beranjak dari segala permasalahan di atas, maka penulis melakukan penelitian dengan judul “Kebijakan Hukum Pidana Terhadap *Skimming* ATM Berbasis Transaksi Elektronik.”