Volume 5 Number 2 (2023)
July-December 2023
Page: 1691-1708

E-ISSN: 2686-4819
P-ISSN: 2686-1607
DOI: 10.37680/almanhaj.v5i2.3139

AL-MANHAJ
Jurnal Hukum dan Pranata Sosial Islam

Tinjauan Yuridis Kejahatan di dalam Sistem Elektronik pada Rekening Virtual

Bani David Soaloon Pakpahan[1], Parameshwara[2], Kartina Pakpahan[3], Margaretha Citra Novriyanti Saota[4], Franciscus Orlando Tambunan [5]

[1] Universitas Prima Indonesia, Medan; banidavidsp@gmail.com
[2] Universitas Prima Indonesia, Medan; parameshwara_advokat@yahoo.com
[3] Universitas Prima Indonesia, Medan; kartinapakpahan@unprimdn.ac.id
[4] Universitas Prima Indonesia, Medan; novisaota17@gmail.com
[5] Universitas Prima Indonesia, Medan; tambunanfrans7@gmail.com

Received: 25/05/2023 Revised: 22/08/2023 Accepted: 26/09/2023

Abstract

Virtual account is an electronic application that is created to connect to a large computer network when using the internet. This is very vulnerable to the threat of online crime, virtual accounts must provide security for customers. The aim of the research is to find out what electronic system crimes are, analyze the application of data protection laws, and legal sanctions for perpetrators of account burglary crimes. The research method is normative juridical. The research results show that the electronic systems currently in force in Indonesia are Mobile Banking, SMS Banking and Internet Banking. Regarding data protection in banking, it is regulated in article 40 (1) of Law no. 10 of 1998 concerning banking, namely that banks are obliged to keep confidential information regarding depositors and their deposits. Even though the Laws and Regulations have strictly regulated the protection of customer data, the fact is that in the field there is still a lot of misuse of customer personal data by irresponsible parties. Prohibitions for perpetrators of virtual account burglary crimes are regulated in Law Number 19 of 2016 concerning Information and Electronic Transactions Article 31 Paragraphs 1, 2, 3 and 4. The conclusion is that the application of the law regarding data protection in banking is regulated in Article 40 (1) of the Law No. 10 of 1998 concerning banking, namely that "banks are obliged to keep confidential information regarding depositors and their deposits.

Keywords

Crime; Electronic Systems; Virtual Accounts

Corresponding Author
Bani David Soaloon Pakpahan
Universitas Prima Indonesia, Medan; banidavidsp@gmail.com

1. PENDAHULUAN

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 menyatakan dalam Alenia 4 bahwa tujuannya adalah “terbentuknya Pemerintahan Negara Indonesia yang melindungi segenap bangsa Indonesia dan seluruh tumpah darah Indonesia serta memajukan kesejahteraan umum, mencerdaskan kehidupan bangsa, dan ikut melaksanakan ketertiban dunia berdasarkan tentang

kemerdekaan, dan seterusnya lain-lain." Untuk menjaga kesejahteraan rakyatnya di era globalisasi, setiap negara melakukan investasi dalam pembangunan di semua sector(Anon n.d.). Seperti yang kita ketahui bersama, era digitalisasi saat ini tidak diragukan lagi berkembang pesat, terutama dalam hal bagaimana teknologi digunakan untuk informasi, pendidikan, budaya, dan hal lainnya. Kecanggihan sebuah teknologi sedang dianut oleh banyak orang(Irawan 2020).

Mayoritas masyarakat Indonesia, baik di perkotaan maupun pedesaan, telah bertransformasi seiring berkembangnya sistem elektronik melalui teknologi informasi. Prevalensi penggunaan smartphone dalam kehidupan sehari-hari saat ini lebih tinggi di kalangan masyarakat Indonesia. Hampir sering, baik melalui media sosial atau metode seluler, orang berkomunikasi melalui telepon pintar. Karena koneksinya ke Internet, smartphone kini menjadi kebutuhan hampir semua aktivitas. Orang-orang di Indonesia menggunakan ponsel mereka untuk berbagai keperluan, seperti melakukan dan menerima panggilan telepon dan SMS, obrolan media sosial, menjalankan bisnis, dan melakukan transaksi keuangan online(Hendarsyah 2016). Orang dapat menggunakan teknologi modern yang lebih canggih dengan tepat dan cerdas karena teknologi itu ada. Persaingan di dunia bisnis saat ini lebih ketat dari sebelumnya, sehingga perusahaan harus lebih fokus dan bekerja keras untuk menang. Agar berhasil, perusahaan harus mampu melihat peluang dan memenuhi kebutuhan konsumen. Internet telah menjadi alat yang ampuh untuk komunikasi dan bisnis.

Bank menggunakan layanan perbankan online untuk memudahkan pelanggannya melakukan transaksi perbankan. Nasabah yang menggunakan online banking dapat melakukan transaksi keuangan dari rumah, tempat usaha, atau lokasi lain selain situs bank sebenarnya (cabang). dengan menggunakan perangkat elektronik untuk komunikasi, termasuk komputer atau ponsel. Automatic Teller Machines (ATM) dan layanan perbankan online lainnya (e-banking)(Irmadhani and Nugroho 2012).

Saat ini bisnis perbankan sangat diuntungkan oleh perkembangan berbasis teknologi informasi dalam hal efisiensi dan efikasi. Ketersediaan produk-produk perbankan elektronik seperti ATM, kartu kredit, kartu debit, online banking, SMS/mobile banking, phone banking, dan lain-lain telah memperluas jangkauan geografis dan temporal layanan perbankan. Akibatnya, nominal transaksi keuangan perbankan sangat meningkat. Cyber crime adalah ketika komputer digunakan untuk kegiatan jahat termasuk penipuan, perdagangan pornografi anak, pencurian identitas, dan pelanggaran privasi. Cyber crime berbeda dengan kejahatan tradisional karena teknologi berperan dalam memungkinkan terjadinya tindak kriminal yang sering terjadi saat ini(Putri 2022).

Teknologi penting bagi kehidupan masyarakat saat ini. Teknologi dapat membawa banyak hal, termaksud dampak positif, seperti adanya e-mail, belanja online, perbankan online, serta usaha online. Namun, ada juga dampak negatif, yakni dengan munculnya kejahatan internet seperti pencurian data

pribadi melalui aplikasi online yang sudah korban daftarkan sebelumnya. Menyebabkan terbentuknya kejahatan yang dikenal sebagai kejahatan dunia maya, yang meliputi perjudian ilegal, pencemaran nama baik, pornografi, pencurian akun, penghancuran jaringan peretasan dunia maya, serangan virus (penyebaran virus), dan lainnya (Suseno 2012).

Rahasia bank untuk melindungi kepentingan masyarakat agar kerahasiaannya terlindungi dan dapat lebih dipegang teguh tidak hanya ditetapkan sebagai kewajiban kontraktual diantara bank dannasabah, namun perlu ditetapkan sebagai kewajiban pidana (Ahmad, Anggraini, and Iswahyudi 2022).

2. METODE

Metodologi penelitian yang digunakan adalah yuridis empiris, dan data sekunder (data perpustakaan dan dokumen hukum), Tujuan penelitian pada penelitian ini untuk menganalisis dan mengetahui sistem elektronik yang berlaku di Indonesia, menganalisis penerapan hukum terkait perlindungan data perbankan, serta mengetahui sanksi hukum bagi pelaku kejahatan pembobolan data pribadi rekening virtual. Adapun metodologi penelitian yang digunakan adalah yuridis normatif, dan data sekunder (data perpustakaan dan dokumen hukum), atau disebut sebagai bahan hukum, meliputi bahan hukum utama, bahan hukum sekunder, bahan hukum tersier, dan bahan non hukum.

3. HASIL DAN PEMBAHASAN

3.1. Sistem Elektronik Yang Berlaku Di Indonesia

Berdasarkan Undang-Undang No. 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, pada Pasal (1) Ayat (5) menyebutkan "*Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan Informasi Elektronik".* Jenis-Jenis sistem elektronik, antara lain :

1. Internet Banking

Perbankan internet adalah praktik yang melibatkan pengiriman, penerimaan, transfer, atau melakukan aktivitas keuangan lainnya melalui situs web terenkripsi milik lembaga keuangan. Contohnya: OCBC NISP, menyediakan layanan tersebut untuk memudahkan Sobat OCBC melakukan kegiatan perbankan tanpa mengunjungi kantor cabang.

2. Mobile banking

Layanan yang memungkinkan nasabah bank melakukan transaksi perbankan melalui ponsel atau smartphone, dengan menggunakan menu yang sudah tersedia melalui aplikasi yang dapat diunduh dan diinstal oleh nasabah. Contohnya: Livin' by Mandiri: layanan mBanking Mandiri, BCA Mobile: layanan mBanking BCA, BNI Mobile Banking: layanan mBanking BNI

3. SMS Banking/*Short Message Service*

Metode ini memanfaatkan unsur teknologi berupa layanan nasabah bank yang memberikan nasabah akses ke rekening bank melalui fitur SMS. Kelebihan SMS Banking raktis tanpa harus keluar rumah, mudah serta bisa dilakukan kapanpun dan dimanapun, semua jenis SIM card bisa digunakan (Asmadi 2018).

4. Phone Banking

Layanan ini adalah salah satu cara untuk melakukan transaksi keuangan melalui komunikasi telepon. Misalnya, cara sederhana untuk melakukan transfer atau transaksi lainnya, dengan menghubungi saluran layanan pelanggan bank menggunakan nomor telepon mereka (Asmadi 2018).

5. Kartu Kredit

Sistem ini menggunakan kartu yang disediakan oleh bank atau bisnis manajemen kartu kredit. Ketersediaan kartu ini memberikan hak untuk menggunakannya sebagai metode pembayaran secara kredit untuk pembelian barang atau jasa. Contoh kartu kredit yang diterbitkan Bank di Indonesia ialah: BCA, Bank Mandiri, BNI, BRI, dll

6. Kartu Debit

Transaksi ini dilakukan dengan menggunakan kartu pembayaran yang sah dari suatu bank. Dilansir dari OJK, kartu debit merupakan kartu elektronik yang diterbitkan oleh bank sebagai fasilitas bagi pemegang rekening tabungan atau giro yang dapat dimanfaatkan untuk berbagai transaksi. Contohnya: Kartu debit BNI GPN (Gerbang Pembayaran Nasional), yaitu kartu yang digunakan sebagai fasilitas transaksi tunai dan non tunai bagi pemilik rekening taplus dan taplus bisnis, yang dapat digunakan di seluruh jaringan mesin EDC dan ATM manapun di seluruh Indonesia.

7. Charge Card

Suatu sistem dengan menggunakan kartu, yaitu kartu pinjaman yang dapat digunakan nasabah sebagai alat penarikan atau pembayaran uang tunai di tempat yang telah ditentukan. Setelah dipergunakan, uang pinjaman tersebut wajib dibayarkan kepada Bank pada waktu yang telah ditentukan.

8. Dompet Digital

Dompet digital merupakan produk layanan uang elektronik yang siap digunakan, mudah, cepat, dan aman. Contohnya: dana, ovo, gopay, LinkAja.

Organisasi pemerintahan yang memberikan layanan kepada pengguna Sistem Pemerintahan Berbasis Elektronik (SPBE) melalui teknologi informasi dan komunikasi. Terkait Sistem Pemerintahan Berbasis Elektronik, berlaku Peraturan Presiden Nomor 95 Tahun 2018. Prinsip SPBE meliputi pelayanan publik yang amanah dan berkualitas serta tata kelola pemerintahan yang bersih, efisien, akuntabel, dan transparan. Tata kelola dan manajemen juga diperlukan untuk meningkatkan integrasi

dan kemanjuran sistem *e-government* di tingkat nasional. SPBE tidak hanya sekedar memanfaatkan perangkat lunak atau teknologi informasi untuk menjalankan tugas-tugas operasional rutin pemerintah(Barat 2023).

Pengawasan terhadap Penyelenggara Sistem Elektronik terdapat di Peraturan Pemerintah RI No.82 Tahun 2012 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik, Pada Pasal (20) menyebutkan:

Ayat (1), Penyelenggara Sistem Elektronik wajib menetapkan metode dan sarana pengamanan Sistem Elektronik untuk mencegah terjadinya gangguan, malfungsi, dan kerugian.

Ayat (2), Penyelenggara Sistem Elektronik wajib menyelenggarakan sistem keamanan yang meliputi protokol dan mekanisme pencegahan dan penanggulangan ancaman dan serangan yang mengakibatkan gangguan, kegagalan, dan kerugian.

Ayat (3), Penyelenggara Sistem Elektronik wajib mengamankan data dan melaporkan setiap kegagalan atau gangguan sistem yang diakibatkan oleh tindakan pihak ketiga terhadap Sistem Elektronik dan berdampak signifikan sesegera mungkin kepada aparat penegak hukum atau lembaga pengawas dan pengatur sektor terkait

Ayat (4), Penyelenggara Sistem Elektronik wajib melakukan pengamanan data dan segera melaporkannya kepada aparat penegak hukum atau lembaga pengawas dan pengawas sektor terkait pada kesempatan pertama jika terjadi kegagalan atau gangguan sistem yang berdampak signifikan akibat perbuatan pihak lain pada sistem elektronik.

Selain itu, sebagaimana disebutkan dalam Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 4 Tahun 2016 Pasal (2) mengatakan:

Berdasarkan konsep risiko, peraturan menteri ini mengatur bagaimana penyelenggara sistem elektronik untuk pelayanan publik mengembangkan sistem manajemen keamanan informasi.

Dan Pasal (3) mengatakan:

Penyelenggara Sistem Elektronik Untuk Pelayanan Publik yang menyelenggarakan Sistem Manajemen Pengamanan Informasi sebagaimana dimaksud dalam Pasal 2 meliputi:

a) *Penyelenggara sistem elektronik untuk pelayanan publik sebagaimana dimaksud dalam Pasal 2 wajib menerapkan sistem manajemen keamanan informasi;*
b) *Korporasi yang beroperasi sebagai Badan Usaha Milik Negara, Badan Usaha Milik Daerah, atau Unit Kerja di lingkungan masyarakat setempat;*
c) *Organisasi independen yang dibentuk berdasarkan undang-undang dan/atau unit kerja pelaksana.*
d) *Berbagai organisasi yang terikat secara hukum untuk menyelenggarakan Pelayanan Publik dalam rangka melaksanakan Misi Negara.*

Kejahatan terkait sistem elektronik akhir-akhir ini meningkat di Indonesia, dan kejahatan tersebut sangat merugikan baik bagi orang maupun komunitas yang lebih luas. Berdasarkan hal tersebut, Indonesia menerbitkan Undang-Undang Informasi dan Transaksi Elektronik Nomor 19 Tahun 2016 (UU ITE) pada 25 November 2016. Selain pengenalan KUHP sebagai undang-undang tindak pidana umum, undang-undang ini juga memuat sejumlah pasal-pasal pidana yang mengatur tentang delik-delik tertentu. Undang-undang ini mengatur aspek keperdataan dari transaksi elektronik atau e-commerce selain aspek pidana.

Pengertian kejahatan apabila dilihat dari peraturan perundang-undangan (dalam hal ini pidana) yaitu norma yang termuat dalam peraturan pidana, dengan demikian kejahatan adalah perbuatan yang oleh undangundang dinyatakan sebagai tindak pidana. Kejahatan didefinisikan sebagai perbuatan yang dipandang sangat merugikan masyarakat luas, bagi kerugian terhadap materi maupun kerugian atau bahaya terhadap jiwa dan kesehatan manusia(Situmaeng 2021). Berikut ini jenis-jenis kejahatan sistem elektronik pada rekening virtual(Ratulangi, Wahongan, and Mewengkang 2021):

1. *Social engineering*

Rekayasa sosial adalah manipulasi psikologis seseorang dengan tujuan mendapatkan informasi tertentu dengan cara menyesatkan secara halus, baik disadari atau tidak, melalui telepon atau secara langsung. Dalam hal metode dasar rekayasa sosial ada beberapa hal untuk mengumpulkan informasi, yakni:

a. *Phishing*, digunakan dengan mengelabui atau memanipulasi para pemilik rekening bank, sehingga mereka memberikan data dan informasi yang bisa digunakan untuk mengakses akun perbankan milik nasabah. Pengelabuan yang dilakukan untuk mendapatkan informasi rahasia seperti password dengan menyamar sebagai orang atau bisnis terpercaya dalam sebuah komunikasi elektronik. Saluran yang digunakan sebagai email, layanan pesan instan (SMS), atau penyebaran link palsu di internet untuk mengarahkan korban ke website yang telah dirancang untuk menipu.
b. Vishing mengacu pada upaya penipu untuk mendekati korban untuk mendapatkan informasi atau membujuk mereka untuk bertindak. Biasanya, telepon digunakan untuk komunikasi.
c. Peniruan, upaya penipu untuk menyamar sebagai orang lain untuk mendapatkan informasi sensitif,

Ada pun cara antara yang sering penipu gunakan pada rekayasa sosial sebagai strategi, yakni:

a. Penipuan internet banking dan transaksi kartu kredit/debit *online* dimana pelakunya menyamar sebagai pegawai bank dan memberitahu korban tentang perubahan biaya layanan SMS/intemet banking, pemberian bonus pulsa, pembagian hadiah undangan, dll. Penipuan *online* penawaran pinjaman dengan bunga rendah juga dilakukan oleh para pelaku.

b. *Contact center* bank, terutama maling yang mengelabui ATM agar korban tidak bisa bertransaksi dan kartunya tertelan oleh mesin. Pada saat yang sama, anggota tim penipuan yang berada di dekat ATM menginstruksikan korban untuk menghubungi nomor cali center fiktif tersebut. Tim memberi tahu mereka bahwa ATM telah diblokir dan berpura-pura menjadi cali center. Mereka kemudian meminta identitas diri dari korban, beserta kode PIN ATM. Kartu ATM korban tertelan mesin, dan pelaku yang berada di dekatnya mencurinya.
c. Penipuan Korban penipuan SMS menerima pesan yang menjanjikan hadiah, diskon, bonus pulsa, paket perjalanan wisata, pinjaman *online*, dan insentif lainnya. Korban akan dibawa ke ATM dengan dalih mencairkan hadiah dan diinstruksikan untuk mengikuti instruksi pelaku, seperti mentransfer dana atau mengisi saldo *e-commerce*.

2. Skimming

Skimming adalah penyalinan data secara ilegal dari strip magnetik kartu debit atau kredit untuk mencuri informasi. Saat melakukan pembelian menggunakan ATM, metode skimming digunakan untuk mencuri informasi nasabah. Skimmer, kamera tersembunyi, dan keypad adalah 3 (tiga) alat utama yang digunakan untuk melakukan kejahatan ini. Tujuan alat skimmer adalah untuk merekam perilaku nasabah saat menggunakan mesin ATM; ketika kartu korban dimasukkan ke dalam ATM, alat skimmer dapat menangkap jalur elektromagnetik pada kartu korban. Kamera rahasia dan keypad mesin ATM digunakan untuk merekam tindakan korban saat dia memasukkan PIN-nya.

3. Pencurian Identitas (*Identity Theft*)

Pencurian identitas adalah ketika seseorang mengambil informasi pribadi korban, seperti alamat email, halaman situs *website*, dan informasi login pemilik akun. Hal ini memungkinkan seseorang mencuri uang, mengakses informasi pribadi, atau bahkan merugikan korban dengan cara lain(Sudama et al. 2020). Perbankan terbuka adalah salah satu metode pencurian. Perbankan terbuka adalah sistem yang memungkinkan interaksi pelanggan dan lembaga keuangan. Pelaku pencurian dapat membaca sistem ini dengan cara *"jamming*" atau men-tap info profil konsumen.

4. Malware

Perangkat lunak berbahaya, sering dikenal sebagai perangkat lunak yang tidak disukai di sistem komputer atau malware, adalah singkatan yang digunakan untuk jenis program ini. Perangkat lunak apa pun yang digunakan untuk menganalisis, mengubah, atau bahkan memata-matai sistem dapat dianggap malware. Ungkapan yang digunakan untuk mengkarakterisasi perangkat lunak jahat adalah malware. Malware dapat menyebar melalui sejumlah saluran, termasuk internet, email, pesan pribadi, dan halaman situs web. Sistem komputer sangat sulit mendeteksi malware. Karena malware dapat masuk ke sistem komputer melalui 2 (dua) saluran berbeda, USB *drive* dan jaringan internet. Malware terus menjadi ancaman signifikan bagi internet di seluruh dunia.

5. Hacking

Peretasan sistem elektronik adalah tindak pidana yang cukup lazim. Dengan mendapatkan akses tidak sah ke sistem komputer korban, aktivitas ini dilakukan. Peretas akan memanfaatkan keahlian mereka untuk melakukan berbagai pelanggaran publik. Contohnya, aksi hacking yang kerap terjadi adalah pembobolan kata sandi.

3.2. Penerapan Hukum terkait Perlindungan Data dalam Perbankan

Terkait perlindungan data pribadi telah resmi dinyatakan sah oleh DPR RI dan telah diundangkan oleh Presiden RI pada tanggal 17 Oktober 2022, sehingga Undang-undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) menjadi bentuk perwujudan hukum secara normatif untuk memberikan pelindungan data pribadi bagi warga negara. Secara umum, ruang lingkup pengaturan UU PDP berlaku, baik bagi sektor publik (pemerintah) dan sektor privat (perorangan maupun korporasi, baik yang berbentuk badan hukum maupun tidak berbadan hukum).

Data pribadi adalah informasi yang dapat digunakan untuk mengidentifikasi atau menemukan seseorang, baik sendiri atau digabungkan dengan pengetahuan lain yang diperoleh secara langsung atau tidak langsung melalui komputer atau metode non-elektronik. Untuk menegakkan hak konstitusional subjek data pribadi, perlindungan data pribadi mengacu pada semua tindakan yang diambil untuk melindungi data pribadi di seluruh rangkaian pemrosesan data pribadi.

Perlindungan Data Pribadi adalah upaya total untuk menjaga Data Pribadi sepanjang rangkaian pemrosesan Data Pribadi untuk menegakkan hak konstitusional subjek Data Pribadi.

Jenis-jenis Data Pribadi terdiri dari:

1. Data Pribadi yang bersifat spesifik
    a) Data dan informasi kesehatan;
    b) Data biometrik;
    c) Data genetika;
    d) Catatan kejahatan;
    e) Data anak;
    f) Data keterangan pribadi; dan/ atau
    g) Data lainnya sesuai dengan ketentuan peraturan perundang-undangan.
2. Data Pribadi yang bersifat umum.
    a) Nama lengkap
    b) Jenis kelamin
    c) Kewarganegaraan
    d) Agama
    e) Status perkawinan

f) Data pribadi yang dikombinasikan untuk mengidentifikasi seseorang

Adapun larangan dalam penggunaan data pribadi yang bukan miliknya diatur dalam Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi, yaitu larangan melakukan perbuatan tersebut diatur dalam Pasal 65 ayat (1) yang berbunyi:

Setiap Orang dilarang secara melawan hukum memperoleh atau mengumpulkan Data Pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian Subjek Data Pribadi.

Melanggar larangan Pasal 65 ayat (1) dipidana berdasarkan Pasal 67 ayat (`) yang berbunyi:

Setiap Orang yang dengan sengaja dan melawan hukum memperoleh atau mengumpulkan Data Pribadi yang bukan milikya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian Subjek Data Pribadi sebagaimana dimaksud dalam Pasal 65 ayat 1, dipidana dengan pidana penjara paling lama lima tahun dan/atau denda paling banyak Rp. 5.00.000.000,00 (lima miliar rupiah).

Dan Pasal 68 juga berbunyi:

Setiap orang yang sebagaimana dimaksud dalam Pasal 66 dengan sengaja membuat Data Pribadi palsu atau memalsukan Data Pribadi dengan tujuan untuk memperoleh sesuatu bagi diri sendiri atau orang lain atas biaya orang lain. Ancaman pidana maksimal enam (enam) tahun penjara, atau enam (enam) tahun penjara dan denda maksimal Rp. 6.000.000.000,00 (enam miliar rupiah).

Tanggung jawab Bank terhadap data nasabah yang digunakan oleh pihak lain dalam layanan mobile banking dikaitkan dengan Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen adalah tanggung jawab produk yang dikenal dengan *product liabilit*y yaitu bentuk tanggung jawab perdata yang secara langsung dari pelaku usaha atas kerugian yang dialami oleh nasabah pengguna mobile banking. Pertanggung jawaban ini diterapkan dalam hal tidak terdapat hubungan perjanjian *(no privity of contract)* antara bank dan nasabah sejalan dengan bentuk perjanjian pada mobile banking yang terwujud dalam bentuk paperless. Sedangkan tindakan hukum yang dapat dilakukan oleh nasabah jika terjadi akses tidak sah atas data pribadi dalam layanan mobile banking berdasarkan Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen maka dapat diselesaikan melalui jalur pengadilan (litigasi) atau di luar pengadilan (non-litigasi).

Penerapan hukum terkait perlindungan data dalam perbankan diatur dalam Pasal 40(1) Undang-Undang Nomor 10 Tahun 1998 Tentang Perbankan menyatakan bahwa *"Bank Wajib Menyimpan Rahasia Mengenai Penyimpan dan Simpanannya"*. Sesuai dengan persyaratan berat pasal ini, bank harus menjaga kerahasiaan informasi mengenai nasabah yang berperan sebagai penabung. Otoritas Jasa Keuangan (OJK) menerbitkan Surat Edaran No. 14/SEOJK.07/2014 tentang Kerahasiaan dan Keamanan Data dan/atau Informasi Pribadi Konsumen sesuai dengan Pasal tersebut di atas. Peraturan Otoritas Jasa

Keuangan No. 1/POJK.07/2013 tentang Perlindungan Konsumen di Sektor Jasa Keuangan dilaksanakan bersamaan dengan diterbitkannya surat edaran ini. Surat Edaran OJK ini mengamanatkan bahwa Penyedia Jasa Keuangan (PUJK) termasuk bank wajib menjaga informasi nasabah dan melarang dengan cara apapun pengungkapan informasi pribadi nasabah.

Walaupun peraturan perundang-undangan telah mengatur secara ketat keamanan data nasabah, namun kenyataannya masih banyak terjadi penyalahgunaan data pribadi konsumen oleh pihak-pihak yang tidak hati-hati. Bahkan jika kita tidak pernah memberikan informasi pribadi kita kepada seseorang, kita sering dapat menerima telepon, pesan SMS, atau email dari orang asing dengan tawaran untuk kartu kredit, asuransi, pinjaman, dan layanan lainnya. Tentu kita merasa dirugikan sebagai konsumen dan pelanggan(Rasyid 2017).

Setidaknya ada dua elemen di antara berbagai insiden yang terjadi yang mengarah pada pengungkapan informasi pribadi pelanggan. Variabel ini dapat dibagi menjadi dua kategori: internal dan eksternal. Terkait aspek internal, oknum pegawai bank yang tidak bertanggung jawab memperdagangkan data pribadi nasabah kepada pihak ketiga menjadi penyebab kebocoran data konsumen. Sedangkan pada faktor eksternal, menurut Kartika Wirjoatmodjo, Direktur Utama PT Bank Mandiri, volume transaksi nasabah yang besar di merchant (penjual barang/jasa) dengan pembayaran nontunai menggunakan kartu debit atau transaksi perdagangan elektronik (e-commerce) dapat mengakibatkan kebocoran data pribadi pelanggan. Beberapa pengecer memiliki teknologi perekaman (penangkapan). Di mesin merchant dan peralatan EDC (Electronic Data Capture), kartu pelanggan terkadang dapat digesek ganda. Bahkan jika gesek pertama cukup untuk menyelesaikan transaksi di mesin EDC, maka gesek kedua di mesin merchant dapat mencatat identitas pelanggan.

1. Hubungan Hukum Para Pihak Dalam Transaksi Elektronik

Suatu jaringan sistem elektronik berbasis komputer dan sistem komunikasi yang terintegrasi membentuk transaksi yang pada hakekatnya adalah perjanjian atau interaksi hukum. Adanya jaringan komputer global seperti internet semakin memudahkan proses ini (Pasal 1 angka 2 UU ITE)(Kemenkumham RI 2008). Hubungan antara dua orang atau lebih (subjek hukum) yang diatur oleh hukum dan memiliki sebab hukum disebut hubungan hukum. Jadi, hak seseorang (pemilik) adalah kekuasaan untuk mengambil tindakan atas sesuatu yang menjadi pokok bahasan hak itu kepada orang lain. Sedangkan tanggung jawab adalah segala sesuatu yang perlu dilakukan atau dilakukan oleh seseorang agar ia memperoleh haknya atau karena ia telah melakukannya dalam suatu hubungan hukum. Objek hukum adalah sesuatu yang dapat dimanfaatkan sebagai topik interaksi hukum dan bernilai, berguna, dan bernilai bagi subjek hukum. Masalah hukum ialah sesuatu yang bisa mendukung hak atau kewajiban seseorang serta mempunyai kedudukan hukum(Kemenkumham RI 2008).

Menurut ketentuan Pasal 23 Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen, "Pelaku usaha yang menolak dan/atau tidak menanggapi dan/atau tidak memenuhi ganti kerugian atas tuntutan konsumen dapat digugat melalui badan penyelesaian sengketa konsumen atau mengajukan kepada badan peradilan di tempat kedudukan konsumen." Sesuai dengan hukum Indonesia, tuntutan hukum perdata dapat dimulai baik untuk wanprestasi maupun perbuatan melawan hukum (onrechtmatigedaad). Landasan hukumnya ditetapkan Buku III Pasal 1243 BW untuk wanprestasi dan 1365 BW untuk perbuatan melawan hukum.

Harus selalu ada hubungan hukum kontraktual (kesepakatan) antara para pihak agar ada hak dan kewajiban hukum. Di sini yang dimaksud dengan prestasi (kinerja) adalah cara-cara untuk membuktikan hak dan kewajiban. Wanprestasi *(default)* adalah apa yang terjadi ketika suatu prestasi tidak diselesaikan, dilakukan, atau dilakukan sebagaimana mestinya sesuai dengan kesepakatan para pihak. Meskipun tidak ada kesepakatan atau hubungan kontraktual antara para pihak dalam gugatan perbuatan melawan hukum, dasar gugatannya adalah kepentingan pihak tertentu yang terkena dampak perbuatan pihak lain.

Tindakan hukum akan lebih tepat dalam kasus kerugian konsumen dalam transaksi perdagangan elektronik jika didasarkan pada wanprestasi daripada perbuatan melawan hukum, khususnya dengan menyebutkan kewajiban pelaku usaha dalam kontrak elektronik yang telah putus dan mengakibatkan kerugian. Menurut Pasal 19 Ayat (4) UU Perlindungan Konsumen yang menyebutkan bahwa "*Ganti rugi tidak menghilangkan kemungkinan adanya tuntutan pidana berdasarkan pembuktian lebih lanjut adanya unsur kesalahan", pelanggaran dalam transaksi elektronik yang termasuk unsur pidana, seperti penipuan, juga dapat ditangani secara pidana".*

2. Kontrak Elektronik dan Klausula Baku

Dokumen elektronik yang mengikat secara hukum para pihak melahirkan suatu hubungan keperdataan antara pihak-pihak yang melakukan transaksi elektronik. Kesepakatan yang dicapai antara pihak-pihak yang menggunakan teknologi disebut sebagai kontrak elektronik. Dalam situasi seperti ini, dokumen-dokumen elektronik harus di lihat menjadi perjanjian antara pihak-pihak yang tidak hanya dinyatakan dalam bentuk perjanjian elektronik tetapi melalui karakteristik yang ditawarkan, seperti setuju dan menerima sebagai tanda persetujuan atau kesepakatan. Mempertimbangkan desainnya, kontrak elektronik adalah kontrak yang khas(RI 2008).

Klausula baku diartikan sebagai sesuai dengan Pasal 1 Angka 10 Undang-Undang Nomor 8 Tahun 1999 Perlindungan Konsumen, "*setiap peraturan atau ketentuan yang diberlakukan dan ditetapkan terlebih dahulu secara sepihak oleh pelaku usaha sebagaimana dituangkan dalam suatu alat dan/atau perjanjian yang mengikat yang harus dipatuhi oleh konsumen*."

3. Tanggung Jawab Penyelenggara Sistem Elektronik dalam *Transaksi Electronic Banking* (*e-Banking)*

Bank adalah lembaga terkemuka, tetapi ketika melakukan operasi perbankan elektronik (*e-banking*), kehati-hatian harus diberikan untuk mematuhi aturan dan pedoman kehati-hatian dan manajemen risiko terkait penerapan *e-banking*, khususnya risiko hukum dan reputasi. *E-banking* adalah metode pengiriman yang digunakan oleh sektor perbankan, dan ikatan sipil yang dipupuknya berupa interaksi akun antara bank dan pelanggan mereka. Jika transaksi elektronik gagal dalam situasi ini, siapa yang harus bertanggung jawab atas kegagalan transaksi? Memahami jenis pertanggungjawaban pelaku dimulai dengan mengakui bahwa ada hubungan hukum antara kedua pihak dalam suatu perikatan. Pada akhirnya, pengaturan kontraktual antara penyedia layanan dan klien (pelanggan) menetapkan hak dan kewajiban yang menjadi landasan akuntabilitas(Edmon Makarim 2005).

Padahal menurut Pasal 7 Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen, Tanggung Jawab Pelaku Usaha (dalam hal ini Penjual *Online*) adalah:

a. Memiliki keyakinan dalam menjalankan kegiatan komersialnya;
b. Informasi tentang persyaratan dan garansi produk atau layanan, serta detail tentang cara menggunakan, memelihara, dan memperbaikinya, harus akurat, transparan, dan jujur;
c. Melayani atau memperlakukan pelanggan secara adil, jujur, dan tanpa diskriminasi;
d. berdasarkan ketentuan standar mutu yang berlaku untuk produk dan/atau jasa, yang diproduksi, dan/atau diperdagangkan;
e. Memberikan kemungkinan kepada konsumen untuk menguji dan/atau mencoba barang dan/atau jasa tertentu dan memberikan jaminan dan/atau jaminan atas barang yang dibuat dan/atau ditukar;
f. Membayar kompensasi, ganti rugi, dan/atau pembayaran kembali atas kerugian yang diakibatkan oleh penggunaan produk dan/atau jasa yang diperdagangkan;
g. Jika barang atau jasa yang Anda peroleh atau gunakan tidak mengikuti ketentuan perjanjian, Anda harus membayar kompensasi, kompensasi, dan/atau penggantian.

Pasal 8 Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen melarang pelaku usaha memperdagangkan barang/jasa yang tidak sesuai dengan tuntutan yang dibuat atas label, kemasan, deskripsi, iklan, atau promosi atas penjualan barang dan/atau jasa tersebut. Menurut keterangan dalam artikel ini, adalah ilegal atau dilarang bagi pelaku usaha untuk memperdagangkan produk jika detail barang yang Anda terima berbeda dengan yang tertera di iklan atau foto. Apabila barang dan/atau jasa yang Anda terima tidak sesuai dengan kontrak atau tidak sebagaimana mestinya, Anda berhak mendapatkan kompensasi, kompensasi, dan/atau penggantian sebagai pelanggan berdasarkan Pasal 4 huruf h Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Pelanggan. Sementara itu, apabila barang dan/atau jasa yang diperoleh atau digunakan tidak sesuai dengan

perjanjian, maka pelaku usaha sendiri wajib memberikan kompensasi, kompensasi, dan/atau penggantian berdasarkan Pasal 7 huruf g UUPK :

> *Ancaman pidana penjara paling lama 5 (lima) tahun atau denda paling banyak Rp. 2.000.000.000,00 (dua miliar rupiah) dapat dikenakan kepada pelaku usaha yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 8, Pasal 9, Pasal 10, Pasal 13 ayat (2), Pasal 15, dan Pasal 17 ayat (1) huruf a, huruf b , huruf c, huruf e, ayat (2) dan Pasal 18.).*

Di Indonesia, UU ITE merupakan Peraturan Perundang-Undangan positif yang mengatur kewajiban mengatur transaksi elektronik selain perjanjian yang mengatur interaksi keperdataan. UU ITE mengatur penggunaan teknologi netral dalam transaksi elektronik dalam rangka perlindungan konsumen dan mensyaratkan kontrak untuk memanfaatkan sistem elektronik.

Selain itu, setiap operator sistem elektronik bertanggung jawab atas berjalannya sistem secara efisien dan harus menghadirkan sistem elektronik yang andal dan aman. Kendali sistem elektronik berada di tangan penyelenggara sistem elektronik. Namun, jika dapat dibuktikan bahwa penggunaan sistem elektronik tersebut karena force majeure, kesalahan, atau kelalaian pengguna, maka klausul ini tidak berlaku (Pasal 15 UU ITE).

Melalui Peraturan Bank Indonesia dan Surat Edaran Bank Indonesia, Bank Indonesia telah menerbitkan beberapa ketentuan (peraturan) terkait penggunaan teknologi informasi bagi bank dan lembaga yang menyelenggarakan sistem pembayaran sesuai dengan UU ITE. Aturan-aturan ini dimaksudkan untuk menawarkan keselamatan dan keamanan saat melakukan operasi transaksi elektronik. Perjanjian tersebut antara lain mengamanatkan agar semua penerbit kartu memasang chip pada kartu pembayarannya, menerapkan autentikasi dua faktor untuk transaksi keuangan *online*, dan mengenkripsi transaksi untuk meningkatkan ketersediaan, keamanan, dan integritas data layanan keuangan elektronik(Indonesia 2005).

Ketentuan mengenai Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank dalam PBI No.9/15/PBI/2007 memuat prinsip-prinsip utama penerapan manajemen risiko dalam penggunaan teknologi informasi yang wajib diterapkan oleh Bank untuk memitigasi risiko. terkait dengan penerapan teknologi informasi. Hal ini mempertimbangkan potensi ancaman yang dapat merugikan Bank dan nasabahnya selain risiko perbankan yang lebih konvensional seperti risiko likuiditas dan risiko kredit. Risiko tersebut meliputi risiko operasional, risiko hukum, dan risiko reputasi(Indonesia 2007).

3.3. Sanksi Hukum Bagi Pelaku Kejahatan Pembobolan Rekening Virtual

Seluruh Untuk memerangi kejahatan dunia maya secara efektif, sistem peradilan pidana secara keseluruhan harus ditingkatkan. Ini termasuk menciptakan budaya, struktur, dan konten sistem peradilan pidana yang lebih kuat. Hukum pidana modern dan transaksi internet dikembangkan

sebagian besar oleh kebijakan hukum pidana(Doni 2022). Tidak semua aspek kejahatan dunia maya tercakup dalam Undang-Undang Nomor 19, yang mengubah Undang-Undang Nomor 11 Tahun 2008. Undang-undang pidana baru harus ditulis untuk menangani semua aspek kejahatan dunia maya. Pemikiran baru tentang Kitab Undang-Undang Hukum Pidana (KUHP) diperlukan karena KUHP yang sudah usang tidak dapat lagi menangani delik kontemporer. Ilmuwan kriminal mengklaim bahwa sebagian besar kejahatan komputer adalah ilegal dan hanya sedikit yang berubah di bidang ini dalam beberapa tahun terakhir. KUHP yang membahas semua pelanggaran ini harus digunakan sebagai dasar untuk menangani kejahatan komputer, bukan Undang-Undang yang terpisah(Kemenkumham RI 2008).

Nama Undang-Undang yang diusulkan diubah dari Penggunaan Teknologi Informasi menjadi Transaksi Elektronik dan kemudian menjadi Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Namun, Undang-Undang yang mengatur topik ini berbeda dengan Undang-Undang Indonesia di negara lain. Ancaman pidana terhadap siapa pun yang tidak mematuhi hukum yang melindungi telekomunikasi dapat dihukum penjara atau denda yang signifikan. Menurut Undang-Undang Informasi dan Transaksi Elektronik, pelaku kejahatan dunia maya kini dapat dijerat Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik Pasal 31. Dalam Undang-Undang Nomor 19 Tahun 2016 Pasal 31 Ayat 1, 2, 3, dan 4, dibahas tentang hukuman yang akan dijatuhkan oleh pelaku. menderita jika mereka melanggar hukum dengan sengaja atau tanpa wewenang(RI 2008). Ketentuan Undang-Undang No. 3 Tahun 2011 tentang Transfer Dana

Pasal 85:

"Setiap orang yang dengan sengaja menguasai dan mengakui sebagai miliknya Dana hasil transfer yang diketahui atau patut diketahui bukan haknya dipidana dengan pidana penjara paling lama 5 (lima) tahun atau denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah)."

Pasal ini termasuk dalam kategori pembobolan rekening nasabah karena perbuatan yang dilakukan pelaku adalah pelaku dengan sengaja menguasai dan mengakui miliknya dana dari hasil pembobolan rekening nasabah pengguna mobile banking. Ketentuan Undang-Undang Nomor 8 Tahun 2010 mengenai Pencegahan dan Pemberantasan Tindak kejahatan Pidana Pencucian Uang

Pasal 3:

"Setiap orang yang menempatkan, mentransfer, membelanjakan, membayarkan, menghibahkan, menitipkan, membawa ke luar negeri, mengubah bentuk, menukarkan dengan mata uang atau surat berharga, atau melakukan perbuatan lain atas harta kekayaan yang diketahuinya atau patut diduganya diperoleh melalui tindak pidana sebagaimana dimaksud dalam Pasal 2 ayat (1) dipidana karena pencucian uang dengan pidana penjara paling lama 20 (dua puluh) tahun dan denda paling banyak Rp. 10,000,000,000,00"

Pasal ini termasuk dalam kategori pembobolan rekening nasabah pengguna mobile banking karena perbuatan yang dilakukan pelaku adalah menempatkan, mengalihkan harta kekayaan dengan maksud untuk menyembunyikan atau menyamarkan sumbernya, baik ia mengetahuinya atau mempunyai alasan yang kuat untuk mengira bahwa itu adalah hasil tindak pidana.

Pasal 4:

"Setiap Orang yang menyembunyikan atau menyamarkan asal usul, sumber, lokasi, peruntukan, pengalihan hak-hak, atau kepemilikan yang sebenarnya atas Harta Kekayaan yang diketahuinya atau patut diduganya merupakan hasil tindak pidana sebagaimana dimaksud dalam Pasal 2 ayat (1) dipidana karena tindak pidana Pencucian Uang dengan pidana penjara paling lama 20 (dua puluh) tahun dan denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah)."

Pasal ini termasuk dalam kategori pembobolan rekening nasabah pengguna mobile banking karena perbuatan yang dilakukan pelaku adalah menyembunyikan atau menyamarkan asal usul, sumber, lokasi, peruntukan, pengalihan hak-hak, atau kepemilikan yang sebenarnya atas Harta Kekayaan yang diketahuinya atau patut diduganya merupakan hasil tindak pidana.

Pasal 5:

1. *Setiap Orang yang menerima atau menguasai penempatan, pentransferan, pembayaran, hibah, sumbangan, penitipan, penukaran, atau menggunakan Harta Kekayaan yang diketahuinya atau patut diduganya merupakan hasil tindak pidana sebagaimana dimaksud dalam Pasal 2 Ayat (1) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).*
2. *Ketentuan sebagaimana dimaksud pada Ayat (1) tidak berlaku bagi Pihak Pelapor yang melaksanakan kewajiban pelaporan sebagaimana diatur dalam undang-undang ini.*

Merujuk kedalam UU ITE, *Cracking* adalah istilah yang digunakan untuk menggambarkan perbuatan-perbuatan yang dilarang oleh Pasal 30 ayat 2. Menurut ayat (2) Penjelasan Pasal 30, Secara teknis antara lain perbuatan yang dilarang tersebut dalam ayat ini:

a. *berkomunikasi, mengirim, mengirim, atau dengan sengaja mencoba agar hal-hal ini terjadi pada siapa pun yang tidak berwenang untuk menerimanya.*
b. *Sengaja menghalangi agar informasi dimaksud tidak dapat atau gagal diterima oleh diizinkan untuk menerimanya di dalam pemerintah nasional atau daerah. Ternyata isi penjelasan Pasal 30 ayat (2) tidak sesuai dengan penjelasan Pasal 30 ayat (2); Penjelasan Pasal 30 ayat (2) lebih tepat menjelaskan Pasal 32 ayat (2), bukan untuk menjelaskan Pasal 30 ayat (2).*
c. *Membobol Komputer dan/atau Sistem Elektronik yang bertujuan selain untuk mengakses juga untuk menaklukkan sistem pengamanan dari sistem komputer yang diakses itu.*

Larangan melakukan perbuatan tersebut diatur dalam Pasal 30 ayat (3) yang berbunyi:

Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

Pelanggaran terhadap larangan Pasal 30 ayat 3 akan dikenakan sanksi Pasal 46 ayat 3 yang berbunyi:

Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (3) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/ atau denda paling banyak Rp 800.000.000,00 (delapan ratus juta rupiah).

Actus reus dari tindak pidana tersebut di atas adalah "mengakses". Mens rea dari tindak pidana tersebut di atas adalah "dengan sengaja". Objek dari actus reus tindak pidana sama dengan obyek "Komputer dan/atau Sistem Elektronik" actus reus ayat (1) dan ayat (2) Pasal 30.

4. KESIMPULAN

Sistem Elektronik ialah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan informasi elektronik. Dan sistem elektronik yang berlaku di Indonesia saat ini Mobile Banking, SMS Banking, dan Internet Banking. Adapun jenis-jenis kejahatan sistem elektronik pada rekenig virtual ialah Social engineering, Skimming, Pencurian Identitas (Identity Theft), Malware, Hacking.

Data Pribadi merupakan data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau nonelektronik. Diatur dalam UU PDP Nomor 27 Tahun 2022. Penerapan hukum terkait perlindungan data dalam perbankan diatur dalam pasal 40 (1) UU No. 10 Tahun 1998 tentang perbankan, yaitu ''bank wajib merahasiakan keterangan mengenai nasabah penyimpan dan simpanannya''. Pasal ini secara tegas mengatur bahwa bank wajib merahasiakan keterangan tentang nasabah dalam kedudukannya sebagai nasabah penyimpan. Padahal Undang-Undang telah mengatur secara ketat perlindungan data konsumen, namun faktanya di lapangan masih banyak terjadi penyalahgunaan data pribadi nasabah oleh pihak-pihak yang tidak bertanggung jawab.

Sanksi Hukum Bagi Pelaku Kejahatan Pembobolan Rekening Virtual diatur dalam Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik Pasal 31 Ayat 1, 2, 3, dan 4, dibahas tentang hukuman yang akan dijatuhkan oleh pelaku diatur dalam pasal 45.

REFERENSI

Ahmad, Hakam, Sri Anggraini, and Gesang Iswahyudi. 2022. "Perlindungan Hukum Terhadap Keamanan Rahasia Bank Dalam Menjaga Kepentingan Nasabah Perbankan." *AL-MANHAJ: Jurnal Hukum Dan Pranata Sosial Islam* 4(2). doi: 10.37680/almanhaj.v4i2.1800.

Anon. n.d. "Undang-Undang Dasar Negara Republik Indonesia Tahun 1945."

Asmadi, Erwin. 2018. "Aspek Perlindungan Hukum Bagi Konsumen Dalam Penggunaan Aplikasi Pembayaran Elektronik (Electronic Payment)." *Doktrina: Journal of Law* 1(2):90–103.

Barat, Pemkab Pesisir. 2023. "Sistem Pemerintahan Berbasis Elektronik." *Pemkab Pesisir Barat*. Retrieved February 2, 2023 (https://pesisirbaratkab.go.id/spbe/tentang).

Doni. 2022. "Penyelenggara Sistem Elektronik Wajib Mendaftarkan Diri Sebelum 20 Juli 2022." *Kementerian Komunikasi Dan Informatika Republik Indonesia*. Retrieved February 2, 2023 (https://www.kominfo.go.id/content/detail/43044/penyelenggara-sistem-elektronik-wajib-mendaftarkan-diri-sebelum-20-juli-2022/0/artikel).

Edmon Makarim. 2005. *Pengantar Hukum Telematika Suatu Kompilasi Kajian*. Jakarta: Raja Grafindo Persada.

Hendarsyah, Decky. 2016. "Penggunaan Uang Elektronik Dan Uang Virtual Sebagai Pengganti Uang Tunai Di Indonesia." *IQTISHADUNA: Jurnal Ilmiah Ekonomi Kita* 5(1):1–15. doi: 10.46367/iqtishaduna.v5i1.74.

Indonesia, Bank. 2005. "Peraturan Bank Indonesia Nomor :7/52/PBI/2005 Tentang Penyelengggaraan Kegiatan Alat Pembayaran Dengan Mengguanakan Kartu."

Indonesia, Bank. 2007. "Peraturan Bank Indonesia Nomor: 9/15/PBI/2007 Tentang Penerapan Manajemen Risiko Dalam Penggunaan Teknologi Informasi Oleh Bank Umum." 1–32.

Irawan, Moh Dendy. 2020. "Pengaruh Kualitas Layanan Pembukaan Rekening Online Melalui Mobile Banking Mandiri Syariah Mobile Terhadap Kepuasan Nasabah Di Area Surabaya Kota." Universitas Airlangga Surabaya.

Irmadhani, and Mahendra Adhi Nugroho. 2012. "Pengaruh Persepsi Kebermanfaatan, Persepsi Kemudahan Penggunaan Dan Computer Self Efficacy, Terhadap Penggunaan Online Banking Pada Mahasiswa S1 Fakultas Ekonomi Universitas Negeri Yogyakarta." *Kajian Pendidikan Akuntansi Indonesia* 1(3):1–20.

Kemenkumham RI. 2008. "Tanggung Jawab Penyelenggara Sistem Elektronik Perbankan Dalam Kegiatan Transaksi Elektronik Pasca UU No. 11 Tahun 2008." *Kemeterian Hukum Dan Hak Asasi Manusia Repubik Indonesia*. Retrieved November 22, 2022 (https://ditjenpp.kemenkumham.go.id/index.php?option=com_content&view=article&id=665:tanggung-jawab-penyelenggara-sistem-elektronik-perbankan-dalam-kegiatan-transaksi-elektronik-pasca-uu-no-11-tahun-2008&catid=107&Itemid=187).

Putri, Vanya Karunia Mulia. 2022. "Cyber Crime: Definisi, Jenis, Dan Contohnya." *Kompas*. Retrieved

November 22, 2022 (https://www.kompas.com/skola/read/2022/04/25/100000169/cyber-crime--definisi-jenis-dan-contohnya?page=all).

Rasyid, Abdul. 2017. "Perlindungan Data Nasabah Perbankan." *Binus University*.

Ratulangi, Christian Henry, Anna S. Wahongan, and Franky R. Mewengkang. 2021. "Tindak Pidana Cyber Crime Dalam Kegiatan Perbankan." *Lex Privatum* 9(5):179–87.

RI. 2008. "Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik."

Situmaeng, Sahat Maruli T. 2021. *Buku Ajar Kriminologi*. Rajawali Buana Pusaka.

Sudama, I. Wayan, Martin Aryana Imanto, Sukma Wahyu Wijayanti, Tuty Yulia Agustini, and Zainal Fatoni. 2020. "Pengaruh Risiko Pencurian Identitas Dan Persepsi Atas Risiko Terhadap Niat Belanja Online." *Indonesian Business Review* 3(2):180–218. doi: 10.21632/ibr.3.2.180-218.

Suseno, Sigid. 2012. *Yurisdiksi Tindak Pidana Siber*. Bandung: Refika Aditama.