TANGGUNG JAWAB HUKUM PIHAK PERBANKAN DALAM PENCURIAN DATA PRIBADI NASABAH DENGAN TEKHNIK *"PHISING"* PADA TRANSAKSI PERBANKAN

Oleh :

Lis Julianti[1], Anak Agung Putu Wiwik Sugiantari

Fakultas Hukum Universitas Mahasaraswati Denpasar, Email: lisjulianti@unmas.ac.id

ABSTRAK

Perkembangan di bidang ilmu pengetahuan dan teknologi atau yang kita kenal dengan istilah Ilmu Pengetahuan Teknologi, serta perkembangan di bidang informasi dan komunikasi yang sangat pesat serta berdampak pada segala segi kehidupan manusia. Perkembangan informasi dan teknologi juga menimbulkan adanya penyalahgunaan media untuk keuntungan pribadi melalui perbuatan mengambil data identitas guna memperoleh *user id* atau *password* dengan menggunakan Teknik *Phising*. Hal tersebut tentunya menimbulkan kerugian bagi nasabah pengguna layanan jasa dalam transaksi perbankan dan mengharuskan bagi pihak bank untuk bertanggungjawab terhadap kerugian tersebut.

Kata Kunci : Phising, Data Pribadi, Perbankan.

ABSTRACT

Developments in the field of science and technology or what we know as Science Technology, as well as developments in the field of information and communication are very rapid and have an impact on all aspects of human life. The development of information and technology has also led to the abuse of the media for personal gain through the act of taking identity data in order to obtain a user id or password using phishing techniques. This of course causes losses for customers who use services in banking transactions and require the bank to be responsible for these losses.

Keywords: Phishing, Personal Data, Banking.

1. PENDAHULUAN

Perkembangan teknologi pada era globalisasi sekarang ini mempengaruhi kehidupan masyarakat dalam berbagai segi kehidupan masyarakat. Keberadaan teknologi sangat bermanfaat untuk mempermudah masyarakat Hadirnya teknologi ini pada akhirnya memudahkan masyarakat untuk memperoleh informasi secara cepat dan mudah tanpa ada halangan yang merintangi.

Kecanggihan alat informasi dan komunikasi setidaknya dapat mempermudah pekerjaan manusia. Banyak teknologi baru dengan berbagai inovasi bermunculan dengan harga yang semakin murah dan mudah didapatkan masyarakat seperti ponsel pintar, laptop, tablet yang semakin memudahkan masyarakat untuk saling berkomunikasi. Indonesia adalah salah satu negara di dunia yang sedang mengalami perkembangan. Salah satu ciri perkembangan ini adalah dengan banyaknya program pembangunan di berbagai bidang kehidupan berbangsa dan bernegara.

Perkembangan di bidang ilmu pengetahuan dan teknologi atau yang kita kenal dengan istilah Ilmu Pengetahuan Teknologi, serta perkembangan di bidang informasi dan komunikasi yang sangat pesat dan tidak terbendung, dewasa ini yang sudah tentu berdampak pada seluruh aspek atau seluruh sendi-sendi kehidupan masyarakatnya. Dengan demikian, tidaklah berlebihan apabila dikatakan bahwa perkembangan yang salah satunya dicirikan dengan banyaknya pembangunan senantiasa akan menimbulkan perubahan.[1]

Adanya perkembangan teknologi dan informasi khususnya dalam media internet sebagai salah satu media penyebaran informasi secara massif membawa berbagai dampak dalam bentuk penyalahgunaan media internet untuk memperoleh keuntungan dengan melakukan perbuatan mengambil data identitas guna memperoleh *user id* atau *password* dengan menggunakan Teknik *Phising*.

Teknik *Phising* adalah sebuah Tindakan memperoleh informasi pribadi seperti *user id* atau *password* (yang merupakan tanda pengenal untuk masuk dan mengakses internet), PIN (merupakan angka sandi rahasia antara pengguna dan sistem), nomor rekening, nomor kartu kredit Anda secara tidak sah melalui e-mail palsu kepada seseorang atau suatu perusahaan atau suatu organisasi dengan menyatakan bahwa pengirim adalah suatu entitas bisnis yang sah.[2] Informasi inilah yang digunakan untuk kemudian melakukan tindakan kejahatan perbankan untuk mengakses rekening, melakukan penipuan kartu kredit, atau memandu nasabah untuk melakukan transfer ke rekening tertentu dengan iming-iming hadiah.

Bank merupakan Lembaga keuangan yang memiliki fungsi dan peran yang sangat strategis sebagai penghimpun dan menyalurkan dana masyarakat. Dana masyarakat yang dihimpun oleh bank wajib dikelola dengan baik dan dilindungi keberadaannya sehingga memberikan kenyamanan dan keamanan bertransaksi serta tidak menimbulkan kerugian yang

[1] Kristian dan Yopi Gunawan, 2013, *Sekelumit tentang Penyadapan Dalam Hukum Positif di Indonesia*, Bandung, Nuansa Aulia, hal.1.

[2] Sutan Remy Syahdeini, 2009, *Kejahatan & Tindak Pidana Komputer*, Jakarta, Grafiti, hal. 63-64.

berdampak pada sistem perekonomian negara. Pengaturan aktivitas perbankan diatur dalam Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan dan peraturan perundang-undangan lainnya. Berdasarkan pengaturan tersebut bank berkewajiban mematuhi segala peraturan yang ditentukan oleh Undang-Undang dan menerapkan prinsip kehati-hatian.

Menurut Johanes Gunawan, perlindungan hukum atau tanggung jawab bank terhadap nasabah selaku konsumen dapat dilakukan pada saat sebelum terjadinya transaksi *(pre purchase)* atau sesudah terjadinya transaksi *(post purchase)*[3]. Namun di sisi lain, transaksi dalam bidang perbankan banyak menyebabkan kejahatandalam transaksi perbankan akibat pencurian data pribadi nasabah. Pencurian data pribadi nasabah dalam bidang perbankan merupakan salah satu bentuk tindak pidana yang pada akhirnya merugikan nasabah dan memerlukan adanya pertanggungjawaban dari pihak perbankan untuk mengganti kerugian nasabah yang diakibatkan dari pencurian data nasabah. Hingga saat ini pihak kepolisian maupun pihak perbankan masih sangat sulit untuk menemukan pelaku kejahatan pencurian data pribadi nasabah karena belum adanya aturan yang jelas dan pasti yang mengatur mengenai data pribadi.

Berdasarkan latar belakang tersebut, maka penulis tertarik untuk mengangkat tulisan yang berjudul **" Tanggung Jawab Hukum Pihak Perbankan dalam Pencurian Data Pribadi dengan Teknik *Phising* Pada Transaksi Perbankan"** untuk menjadi sebuah artikel ilmiah dalam karya ilmiah yang dipublikasikan. Adapun permasalahan yang dibahas dalam karya ilmiah ini adalah sebagai berikut:

1. Bagaimanakah pengaturan tentang pencurian data pribadi nasabah pada transaksi perbankan?
2. Bagaimanakah tanggung jawab pihak perbankan dalam pencurian data pribadi nasabah dengan Teknik *Phising* pada transaksi perbankan?

2. METODE PENELITIAN

Metode penelitian yang digunakan dalam penelitian ini adalah metode penelitian hukum normatif dengan pendekatan perundang-undangan (statute approach). Bahan hukum yang dipergunakan dalam penelitian ini dibedakan menjadi 2 (dua) macam yaitu bahan hukum primer dan sekunder. Kegiatan yang dilakukan dalam analisis data penelitian hukum normatif dengan cara data yang diperoleh di analisis secara deskriptif kualitatif yaitu analisa terhadap data yang tidak bisa dihitung.

3. HASIL DAN PEMBAHASAN

a. Pengaturan Tentang Pencurian Data Pribadi Nasabah Pada Transaksi Perbankan

Ketentuan peraturan perundangan utama yang mengatur tentang dana pribadi dan identitas nasabah ialah Undang-Undang Nomor 24 Tahun 2013 jo. Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan. Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan yang

[3] Johanes Gunawan, 1999, *Hukum Perlindungan Konsumen*, Bandung, Universitas Katolik Parahyangan, hal. 3.

merumuskan bahwa data pribadi adalah data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya. Frasa "disimpan, dirawat, dijaga kebenaran, dilindungi kerahasiaannya".

Pembahasan tentang pengaturan data pribadi adalah titik awal dalam pemanfaatan data pribadi seperti melakukan hubungan hukum dengan bank, oleh karena pemilik data pribadi telah memiliki identitas yang jelas dan sah seperti nama lengkap, alamat, jenis kelamin dan lain-lainnya dalam proses pengisian formulir di loket bank (offline) maupun secara tidak langsung yakni dengan online.[4] Identitas nasabah berdasarkan data pribadi digunakan untuk pembukaan layanan perbankan bagi nasabah, seperti pembukaan deposito, rekening tabungan, dan lain-lain. Sehingga hubungan hukum antara bank dengan nasabah adalah hubungan yang didasarkan pada hubungan saling ketergantungan (symbiosis mutualisme) yang menempatkan nasabah sebagai konsumen jasa perbankan.

Kendati nasabah dikategorikan sebagai konsumen jasa layanan perbankan yang dilindungi oleh Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen, namun pengaturan melalui Undang-Undang tersebut tidak secara khusus mengatur mengenai perlindungan terhadap data pribadi dan identitas nasabah bank. Terkait dengan pencurian data pribadi nasabah dalam transaksi perbankan adalah termasuk bentuk kategori pencurian yang tidak terlepas dari pengaturan dari berbagai sumber hukum lainnya.

Kejahatan pencurian merupakan suatu tindak pidana yang menurut Pasal 362 KUHP yang berbunyi ""Barangsiapa mengambil barang sesuatu yang seluruhnya atau sebagian kepunyaan orang lain, dengan maksud untuk dimiliki secara melawan hukum, diancam karena pencurian dengan pidana penjara paling lama lima tahun dan denda paling banyak enam puluh rupiah". [5] Pencurian data pribadi dan rekening nasabah sebenarnya tidak secara langsung menyebabkan kerugian terhadap pemilik data dan rekening bank, namun berpotensi besar akan menimbulkan kerugian apabila terjadi kebocoran data tersebut.[6] Data pribadi dan identitas nasabah dalam transaksi perbankan adalah data atau informasi yang sifatnya rahasia, maka menjadi tugas dan kewajiban bank untuk menjaga kerahasiaan data tersebut.

Perlindungan data pribadi dalam bidang perbankan telah diatur dalam Pasal 40 Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan. Berdasarkan ketentuan tersebut bank wajib merahasiakan keterangan mengenai nasabah penyimpan dan simpanannya. Namun demikian, terdapat beberapa pengecualian untuk perlindungan tersebut yaitu:[7] (1) Dalam hal perpajakan, (2) Pimpinan Bank Indonesia memberikan izin kepada pejabat Badan Urusan Piutang dan

[4] Rovel Prasakti Maramis, 2019, "Penggunaan Data Pribadi dan Identitas Nasabah Pada Kejahatan Perbankan", Lex Privatum Volume VIII Nomor 7, Oktober 2019, hal. 99.

[5] Moeljatno, 2001, *Kitab Undang-Undang Hukum Pidana (KUHP*), Jakarta, Bumi Aksara, hal. 128.

[6] Rovel Prasakti Maramis, *Op.Cit,* hal. 102.

[7] Sinta Dewi Rosadi dan Garry Gumelar Pratama, 2018, "Urgensi Perlindungan Privasi dan Data Diri Dalam Era Ekonomi Digital di Indonesia", Veritas at Justitia Volume 4 Nomor 1 2018, hal. 96.

Lelang Negara/Panitia Urusan Piutang Negara untuk memperoleh keterangan dari bank; (3) Pimpinan Bank Indonesia memberikan izin kepada polisi, jaksa, atau hakim untuk kepentingan peradilan dalam perkara pidana untuk memperoleh keterangan dari bank mengenai simpanan tersangka atau terdakwa pada bank; (4) Direksi bank dapat memberitahukan keadaan keuangan nasabahnya kepada bank lain dalam rangka tukar menukar informasi antar bank; (5) Atas permintaan, persetujuan atau kuasa dari Nasabah Penyimpanan secara tertulis, bank wajib memberikan keterangan mengenai simpanan Nasabah Penyimpan pada bank yang bersangkutan dan (6) Dalam hal Nasabah Penyimpan telah meninggal dunia, ahli waris yang sah dari Nasabah Penyimpan yang bersangkutan berhak memperoleh keterangan mengenai simpanan Nasabah Penyimpan tersebut.

Sampai saat ini masih terjadi ketidakpastian perlindungan privasi dan data pribadi, karena Indonesia belum memiliki instrumen hukum yang responsif terhadap adanya kebutuhan masyarakat untuk memperoleh perlindungan yang lebih kuat. Instrumen hukum yang ada di era ekonomi digital. Suatu instrumen hukum perlindungan privasi dan data pribadi di era ekonomi digital setidaknya harus memenuhi 3 kriteria: (1) memiliki karakter internasional; dan (2) merupakan elemen perekat individu dan masyarakat ekonomi.

b. Tanggung Jawab Pihak Perbankan Dalam Pencurian Data Pribadi Nasabah dengan Teknik *Phising* Pada Transaksi Perbankan

Bank adalah lembaga kepercayaan, dalam menjalankan kegiatan *electronic banking* (*e-banking*) maupun *non electronic banking* dengan tetap memperhatikan ketentuan maupun prinsip-prinsip kehati-hatian dan manajemen risiko terkait penyelenggaraan transaksi khususnya risiko reputasi dan risiko hukum. Pemanfaatan teknologi informasi bagi industri perbankan dalam inovasi produk jasa bank juga dibayang-bayangi oleh potensi risiko kegagalan sistem dan/atau risiko kejahatan elektronik (*cybercrime*) yang dilakukan oleh orang- orang yang tidak bertanggungjawab. Salah satu bentuk kejahatan dalam pencurian data diri nasabah pada transaksi perbankan dilakukan dengan Teknik *Phising*.

Phising (password harvesting fishing) adalah tindakan penipuan yang menggunakan email palsu atau situs website palsu yang bertujuan untuk mengelabui user sehingga pelaku bisa mendapatkan data user tersebut.[8] Tindakan penipuan ini berupa sebuah email yang seolah-olah berasal dari sebuah perusahaan resmi, misalnya bank dengan tujuan untuk mendapatkan data-data pribadi seseorang, misalnya PIN, nomor rekening, nomor kartu kredit, dan sebagainya.

Menurut IGN Mantra dosen peneliti cyber war dan security inspection menjelaskan bahwa phising adalah percobaan penipuan menggunakan surel (surat elektronik) dengan tujuan untuk mendapatkan username, password, token, dan informasi-informasi sensitif lainnya yang dikirim melalui surel. Surel phising datang seolah-olah dari

[8] Dikdik M. Arief Mansur dan Elisatris Gulton, 2009, *Cyberlaw Aspek Hukum Teknologi Informasi,* Bandung, PT Refika Aditama, hal. 10.

dari perusahaan/organisasi di mana user adalah anggota/member.[9]

Tindakan pencurian data pribadi dengan menggunakan Teknik *Phising* ini merupakan tindak kejahatan elektronik (*cybercrime)* yang banyak terjadi dalam industri perbankan saat ini yang tentunya merugikan nasabah sebagai pengguna jasa layanan perbankan. Dalam hal terjadi kerugian yang diderita oleh nasabah, permasalahan kemudian yang timbul adalah siapa yang akan bertanggung jawab terhadap kerugian tersebut. Pemahaman mengenai bentuk tanggung jawab para pelaku dimulai dari adanya hubungan hukum yang terjadi diantara kedua belah pihak dalam suatu perikatan. Hubungan hukum antara penyedia jasa dan konsumen (nasabah) pada akhirnya melahirkan suatu hak dan kewajiban yang mendasari terciptanya.[10] Mengenai permasalahan pertanggungjawaban, beberapa negara telah mengatur, sebagai berikut :[11]

1. Di Amerika Serikat, *Electronic Fund Trasfer Act* 1978 (EFTA) mengatur kerangka dasar penetapan hak, kewajiban dan tanggung jawab peserta suatu tanggung jawab yang terlibat dalam transfer dana elektronik. Istilah "Transfer Dana Elektronik" secara luas meliputi transaksi elektronik yang dimulai melalui terminal, telepon, komputer, atau pita perekam suara yang berisi perintah konsumen bagi lembaga keuangan untuk mendebet atau mengkredit rekening konsumen. (*Federal Trade Commission, 2006*).
2. Di Australia,Kode Etik(Pedoman)Transfer Dana Elektronik telah dirilis pada tahun 2002. Kode ini bertujuan untuk perlindungan konsumen dalam bentuk penggunaan teknologi netral untuk penyelenggaraan *e-banking* dan pembayaran produk. *(Sneddon, 2001).*
3. Di Denmark,dibawahundang-undang Instrumen Pembayaran tertentu, diatur bahwa dalam hal terjadi pelanggaran/penipuan oleh orang lain yang menyebabkan kerugian bagi pemegang kartu, maka penerbit yang bertanggung jawab, kecuali karena PIN digunakan oleh orang lain. Sebagaimana diketahui PIN bersifat pribadi dan rahasia sehingga PIN menjadi tanggung jawab pemegang kartu.

Di Indonesia, selain perjanjian yang mengatur hubungan keperdataan, hukum positif yang mengatur tentang tanggung jawab penyelenggaraan transaksi elektronik adalah Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Dalam rangka perlindungan konsumen, UU ITE mengatur adanya teknologi netral yang dipergunakan dalam transaksi elektronik, serta mensyaratkan adanya kesepakatan penggunaan sistem elektronik yang dipergunakan. Namun demikian ketentuan tersebut tidak berlaku dalam hal dapat dibuktikan terjadinya keadaan memaksa, kesalahan, dan/atau kelalaian pihak pengguna system elektronik (*vide* Pasal 15 UU ITE).

Terkait dengan para pihak yang melakukan kegiatan transaksi elektronik diatur bahwa pengirim atau penerima dapat melakukan transaksi elektronik sendiri, melalui pihak yang dikuasakan

[9] IGN Mantra, "Potensi Ancaman Keamanan Email Perusahaan", Info Komputer, (9 September 2015), hal. 71.

[10] Edmon Makarim. *Pengantar Hukum Telematika*, Badan penerbit FH UI, Rajawali Pers, hlm 368-378.

[11] *Ibid.*

olehnya, atau melalui agen elektronik.[12] Dalam hal ini pihak yang bertanggung jawab atas segala akibat hukum dalam pelaksanaan transaksi elektronik adalah :

1. Jika dilakukan sendiri, segala akibat hukum dalam pelaksanaan transaksi elektronik menjadi tanggung jawab para pihak yang bertransaksi.
2. Jika dilakukan melalui pemberian kuasa, segala akibat hukum dalam pelaksanaan transaksi elektronik menjadi tanggung jawab pemberi kuasa.
3. Jika dilakukan melalui agen elektronik segala akibat hukum dalam pelaksanaan transaksi elektronik menjadi tanggung jawab penyelenggara agen elektronik.
4. Jika kerugian transaksi elektronik disebabkan gagal beropersinya agen elektronik akibat tindakan pihak ketiga secara langsung terhadap sistem elektronik, segala akibat hukum menjadi tanggung jawab penyelenggara agen elektronik. Namun demikian jika kerugian transaksi elektronik disebabkan gagal beroperasinya agen elektronik akibat kelalaian pihak pengguna jasa layanan, segala kibat hukum menjadi tanggung jawab pengguna layanan. Ketentuan tersebut tidak berlaku dalam hal dapat dibuktikan terjadinya keadaan memaksa, kesalahan, dan /atau kelalaian pihak pengguna sistem elektronik.

Terkait dengan pelayanan transaksi perbankan, keberadaan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Elektronik sebenarnya dapat meningkatkan keamanan dan kenyamanan nasabah saat melakukan kegiatan perbankan melalui sistem elektronik yang disediakan bank. Ada beberapa alasannya. Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Elektronik menegaskan bahwa bank, sebagai pihak yang menyelenggarakan sistem elektronik dalam memfasilitasi pelayanan jasa bank via Internet (e-banking), bertanggung jawab secara hukum terhadap kerugian yang dialami nasabah berkaitan dengan pemanfaatan layanan yang disediakannya. Namun, jika kerugian disebabkan oleh force majeur atau kesalahan dan kelalaian nasabah, maka bank tidak dapat dimintai pertanggungjawaban.

Berdasarkan paparan di atas, pihak perbankan akan tetap bertanggungjawab terhadap setiap kerugian yang dialami oleh nasabah dalam penggunaan fasilitas perbankan, apabila terbukti bahwa kesalahan terkait dengan kebocoran data nasabah disebabkan oleh kelalaian dari pihak perbankan. Pihak Bank juga memberikan perlindungan hukum kepada nasabah Bank yang mengalami kerugian sebagaimana yang telah diatur dalam Undang-undang Nomor 10 Tahun 1998 tentang perbankan dan UUITE.

4. PENUTUP

4.1. Simpulan

1. Pengaturan tentang pencurian data pribadi nasabah pada transaksi perbankan dikategorikan sebagai bentuk tindak pidana pencurian sebagaimana diatur dalam Pasal 362 KUHP sedangkan terkait dengan perlindungan data nasabah diatur lebih lanjut dalam Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan.

[12] Lihat Pasal 20 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

2. Tanggung jawab pihak perbankan dalam pencurian data pribadi nasabah dengan Teknik *Phising* pada transaksi perbankan adalah dengan memberikan ganti kerugian kepada nasabah yang dirugikan apabila apabila terbukti bahwa kesalahan terkait dengan kebocoran data nasabah disebabkan oleh kelalaian dari pihak perbankan.

4.2. Saran

1. Hendaknya Pemerintah Indonesia dapat segera membuat Undang-Undang yang secara khusus mengatur mengenai perlindungan data diri pribadi dan penyalahgunaan terhadap penggunaan data privasi oleh pihak-pihak yang tidak bertanggungjawab.
2. Pihak perbankan dalam hal ini hendaknya meningkatkan kualitas dan keamanan jasa layanan dalam bertransaksi secara elektronik sehingga dapat memberikan suatu kenyamanan bagi nasabah dalam bertransaksi.

DAFTAR PUSTAKA

BUKU

Gunawan, Johanes, 1999, *Hukum Perlindungan Konsumen*, Bandung, Universitas Katolik Parahyangan.

Kristian dan Yopi Gunawan, 2013, *Sekelumit tentang Penyadapan Dalam Hukum Positif di Indonesia*, Bandung, Nuansa Aulia.

Makarim. Edmon, *Pengantar Hukum Telematika*, Badan penerbit FH UI, Rajawali Pers.

Mansur, Dikdik M. Arief dan Elisatris Gulton, 2009, *Cyberlaw Aspek Hukum Teknologi Informasi*, Bandung, PT Refika Aditama.

Moeljatno, 2001, *Kitab Undang-Undang Hukum Pidana (KUHP*), Jakarta, Bumi *Aksara*.

Syahdeini, Sutan Remy, 2009, *Kejahatan & Tindak Pidana Komputer*, Jakarta, Grafiti.

JURNAL

Maramis, Rovel Prasakti, 2019, "Penggunaan Data Pribadi dan Identitas Nasabah Pada Kejahatan Perbankan", Lex Privatum Volume VIII Nomor 7, Oktober 2019.

Rosadi, Sinta Dewi dan Garry Gumelar Pratama, 2018, "Urgensi Perlindungan Privasi dan Data Diri Dalam Era Ekonomi Digital di Indonesia", Veritas at Justitia Volume 4 Nomor 1 2018.

ARTIKEL

IGN Mantra, "Potensi Ancaman Keamanan Email Perusahaan", Info Komputer, (9 September 2015).

PERATURAN PERUNDANG-UNDANGAN

Undang-Undang Negara Republik Indonesia Nomor 10 Tahun 1998 tentang Perbankan.

Undang-Undang Negara Republik Indonesia Nomor 8 Tahun 1999 tentang Perlindungan Konsumen.

Undang-Undang Negara Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Negara Republik Indonesia Nomor 24 Tahun 2013 tentang Administrasi Kependudukan.

Undang-Undang Negara Republik Indonesia Nomor 19 Tahun 2016 tentang Informasi dan Elektronik