

Tinjauan Yuridis terhadap Perlindungan Nasabah Perbankan Yang Menggunakan Layanan *Internet Banking*

Indriana Syiffa Fauziah¹, Rani Apriani²

¹Program Studi S-1 Ilmu Hukum Universitas Singaperbangsa Karawang,

²Dosen Fakultas Hukum Universitas Singaperbangsa Karawang

Jl. HS.Ronggo Waluyo, Puseurjaya, Kec. Telukjambe Timur, Kabupaten Karawang, Jawa Barat 41361

Correspondence email: indrianasf@gmail.com¹, rani.apriani18088@gmail.com²

Abstrak. Dewasa ini perkembangan yang terjadi terhadap teknologi sangat cepat, khususnya dalam melakukan transaksi maupun komunikasi, yaitu dengan memanfaatkan internet sebagai media, salah satunya perbankan yang menggunakan peranan internet atau disebut juga *internet banking*. Tujuan dari penelitian ini adalah untuk mengetahui bagaimana keamanan informasi perbankan guna menjunjung asas kerahasiaan dalam melindungi identitas nasabah yang menggunakan produk atau jasa *Internet banking*, perlindungan hukum terhadap penggunaan *Internet banking*, serta tanggung jawab bank kepada nasabah yang mengalami kerugian akibat penggunaan *internet banking*. Metode penelitian yang digunakan adalah yuridis normatif dengan pendekatan deskriptif analitis, melalui teknik analisis kualitatif serta teknik pengumpulan data melalui studi pustaka dengan menggunakan data sekunder yang berasal dari bahan hukum primer, bahan hukum sekunder dan bahan hukum tersier. Dari hasil penelitian ini ditemukan bahwa perlindungan keamanan informasi perbankan yaitu dengan menerapkan mekanisme yang memiliki tujuan agar terhindar dari berbagai *cybercrime* atau dampak buruk terhadap keamanan atau kerahasiaan informasi nasabah pengguna *internet banking*, dalam perlindungan hukum, diatur dalam Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan dan Undang-Undang Nomor 11 tahun 2008 yang diubah menjadi Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen, Undang-Undang Nomor 36 Tahun 1999 Tentang Telekomunikasi dan Transaksi Elektronik, serta dalam hal tanggung jawab, bank memberikan kompensasi yang disepakati bersama nasabah melalui pengecekan terlebih dahulu.

Kata Kunci: *Perlindungan, Nasabah, Internet Banking*

Abstract. Nowadays technology is experiencing very rapid development, especially in conducting transactions and communication, namely by utilizing the internet as a medium, one of which is banking that uses the role of the internet or also called *internet banking*. The purpose of this study is to find out how the security of banking information is to uphold the principle of confidentiality in protecting the identity of customers who use products or services *Internet banking*, legal protection against the use of *Internet banking*, and the responsibility of banks to customers who suffer losses due to the use of *internet banking*. The research method used is normative juridical with analytical descriptive approach, through qualitative analysis techniques and data collection techniques through literature study using secondary data derived from primary legal materials, secondary legal materials and tertiary legal materials. From the results of this study found that the security protection of banking information by implementing a mechanism that has the purpose to avoid the various *cybercrime* or adverse impact on the security or confidentiality of customer information users, *internet banking* legal protections, regulated in Law Number 10 of 1998 concerning Banking and Law Number 11 of 2008 which was amended to Law Number 19 of 2016 concerning Electronic Information and Transactions, Law Number 8 of 1999 concerning Consumer Protection, Law Number 36 of 1999 concerning Telecommunications and Electronic Transactions, as well as in terms of responsibility, the bank provides compensation as agreed with the customer through prior checking.

Keywords: *Protection, Costumer, Internet Banking*

PENDAHULUAN

Perkembangan yang terjadi terhadap teknologi saat ini begitu cepat, hal ini ditandai dengan rutinitas manusia yang tidak dapat terlepas dari peranan teknologi, teknologi telah diatur sedemikian rupa untuk mempermudah dan disesuaikan dengan kebutuhan masyarakat, sehingga dapat menjadi efektif dan efisien dalam penggunaannya. Kemajuan teknologi ini tentu dimanfaatkan oleh berbagai sektor, salah satunya yaitu Perbankan. Teknologi dalam Informasi serta Komunikasi telah melahirkan pembaharuan di sektor perbankan yaitu berupa *internet banking*, yang berfungsi memberikan layanan kepada nasabah perbankan melalui internet, tentunya dengan begitu nasabah perbankan memperoleh berbagai keuntungan, salah satunya efisiensi waktu, yang mana nasabah tidak perlu datang dan antre di bank apabila layanan yang dibutuhkan telah tersedia dalam *internet banking*. Tetapi, dalam mengeluarkan suatu produk, bank tetap harus memperhatikan peraturan yang berlaku berdasarkan pada jenis bank sebagaimana yang tercantum di dalam UU No. 7 tahun 1992 yang telah berubah menjadi UU No. 10 Tahun 1998 tentang Perbankan (selanjutnya disebut dengan UU Perbankan)

Segala hal memiliki risiko, begitu pun dengan penggunaan *internet banking*, karena dibalik kemudahan yang didapat dari penggunaan *Internet Banking*, ada pula risiko yang rentan didapat oleh nasabah, seperti kasus yang terjadi

pada Tahun 2015 kepada beberapa nasabah *Bank Central Asia* (BCA) yang menjadi korban pencurian uang secara online. Dengan kronologi, dimana perangkat *Personal Computer* (PC) yang digunakan oleh nasabah yang menjadi korban tanpa diketahui telah terkena virus atau *malware*, virus tersebut disebut juga dengan *zeus malware*, merupakan virus jahat yang digunakan dalam melakukan aksi jahat atau menyerang akun nasabah yang melakukan transaksi perbankan melalui internet. Virus tersebut akan meminta angka token atau kode melalui pop-up yang muncul saat mengunjungi *klikbca.com*, karena tidak mengetahui adanya virus maka nasabah akan menuruti perintah yang ada dalam pop-up dan secara tidak sadar sedang melakukan transaksi.

Sebagaimana dalam Pasal 29 Ayat (4) UU Perbankan, dimana menyebutkan bahwa demi kepentingan nasabah, bank wajib menyediakan informasi mengenai kemungkinan timbulnya risiko yang menimbulkan kerugian bagi nasabah ketika melakukan transaksi perbankan, namun pada kenyataannya tidak adanya informasi yang didapat nasabah pengguna *internet banking* untuk menghindari penyerangan virus jahat atau yang disebut juga dengan *zeus malware* ketika melakukan transaksi *internet banking*, dengan minimnya informasi maka dapat menimbulkan kerugian bagi nasabah yang tidak mengetahui tentang virus tersebut, selain itu karena kurangnya informasi terkait *zeus malware* tentu mengancam keamanan informasi nasabah, dimana informasi atas nasabah tersebut bocor dan dapat disalahgunakan.

Maka dari itu, perlu adanya peningkatan keamanan informasi perbankan dalam menjaga dan melindungi nasabah pengguna *Internet banking*, karena hal tersebut merupakan hak nasabah sebagai konsumen dari produk atau jasa perbankan. Sehingga penulis ingin melakukan penelitian lebih lanjut terkait apa saja aspek yang harus diperhatikan dalam melindungi keamanan informasi nasabah perbankan, bagaimana perlindungan hukum terhadap nasabah perbankan yang mejadi pengguna *Internet banking*, serta bagaimana tanggung jawab diberikan oleh bank sebagai penyelenggara pelayanan perbankan atas kerugian yang dialami nasabah akibat penggunaan *internet banking*.

METODE

Pendekatan Penelitian

Dalam penulisan artikel ini pendekatan yang penulis gunakan yakni yuridis normatif, pendekatan dengan teknik melihat hukum sebagai norma yang tertulis dan dibuat serta diundangkan oleh pejabat yang memiliki wewenang, pendekatan ini melihat hukum sebagai sistem normatif yang berdiri sendiri, bersifat tertutup dan terlepas dari kenyataan yang hidup di dalam masyarakat.

Spesifikasi penelitian yang digunakan dalam penelitian ini adalah deskriptif, yang bertujuan untuk menjelaskan dan menggambarkan kondisi atau gejala dari suatu objek yang akan diidentifikasi dengan suatu keyakinan tertentu. Data yang dikumpulkan adalah keseluruhan data yang didasarkan dan diintegrasikan pada peraturan perundang-undangan yang telah ada, lalu diambil kesimpulan dari data dan bahan tentang obyek masalah yang akan diidentifikasi dengan keyakinan tertentu, sehingga dapat mengembangkan pengetahuan yang mendalam mengenai gejala-gejala yang akan diteliti.

Teknik dalam menganalisis penelitian ini yaitu kualitatif, teknik menganalisis secara kualitatif merupakan penelitian yang memberikan hasil bahan hukum deskriptif berupa kata-kata tertulis. identifikasi dengan cara kualitatif mempergunakan aspek-aspek normatif yuridis melalui metode yang bersifat deskriptif analitis, dimana menguraikan gambaran dari bahan-bahan hukum yang diperoleh dan dihubungkan satu sama lain untuk mendapatkan kesimpulan.

Rancangan Kegiatan dan Ruang Lingkup Penelitian

Rancangan kegiatan meliputi mengumpulkan data, kemudia data yang dikumpulkan adalah keseluruhan data yang didasarkan dan diintegrasikan pada peraturan perundang-undangan yang ada, lalu membuat kesimpulan berdasarkan data dan bahan tentang obyek masalah yang akan diidentifikasi dengan keyakinan-keyakinan tertentu, sehingga dapat mengembangkan pengetahuan yang mendalam mengenai gejala-gejala yang akan diteliti. Ruang lingkup atau objek pada penelitian yakni perlindungan bagi nasabah perbankan yang menjadi pengguna layanan *internet banking*.

Jenis Data dan Bahan Penelitian

Jenis data yang digunakan yaitu data sekunder, data yang berasal dari mengolah bahan hukum primer berupa perundang-undangan, bahan hukum sekunder berupa jurnal-jurnal hukum dan bahan hukum tersier berupa kamus bahasa hukum atau ensiklopedia yang dapat mendukung bahan hukum primer dan sekunder, serta berkaitan dengan tema sentral penelitian.

Lokasi Penelitian

Lokasi atau yang menjadi tempat penelitian dalam penelitian ini yaitu perpustakaan Universitas Singaperbangsa Karawang dan website-website Jurnal Hukum. Teknik pengumpulan data yang digunakan adalah studi pustaka (*library research*), yaitu mengumpulkan literatur-literatur yang berkaitan dengan tema penelitian.

Definisi Operasional Variabel dan Teknik Analisis

Operasionalisasi variabel diperlukan untuk menentukan jenis, indikator, serta skala dari variabel-variabel yang terkait dalam suatu penelitian. Variabel-variabel tersebut tersusun atas variabel independen dan dependen, variabel yang terkait dalam penelitian ini adalah tinjauan yuridis sebagai variabel independen dan perundang-undangan terkait nasabah pengguna *internet banking* sebagai variabel dependen. Teknik analisis data adalah kualitatif, yakni menjelaskan dan menguraikan teori-teori, doktrin-doktrin, asas-asas, serta norma-norma hukum yang ada pada pasal-pasal utama yang relevan dengan perundang-undangan.

HASIL DAN PEMBAHASAN

Kemanan Informasi Perbankan

Keamanan informasi merupakan perlindungan yang diberikan dalam upaya menghindar dari ancaman atas keamanan informasi guna melancarkan usaha, meminimalisir risiko dalam berbisnis, dan memberi tingkatan yang lebih tinggi atas keuntungan, serta peluang usaha. Ada beberapa aspek yang perlu diperhatikan dalam perancangan sistem keamanan atas sistem informasi. Aspek-aspek tersebut diantaranya¹, Kerahasiaan, yaitu terkait jaminan atas rahasia informasi serta data, selain itu memastikan bahwa informasi atau data tidak dapat diakses tanpa seizin yang memiliki wewenang. Integritas, yaitu terkait jaminan bahwa data tidak dapat diubah tanpa seizin yang memiliki wewenang atas data tersebut, hal tersebut merupakan upaya menjaga kelengkapan informasi dan data asli dari ancaman dan kerusakan. Serta Ketersediaan, yaitu jaminan data dan informasi yang dibutuhkan akan selalu dapat diakses tanpa hambatan oleh nasabah.

Informasi merupakan salah satu kepentingan yang harus dilindungi keamanannya. Dalam melindungi keamanan tersebut perusahaan harus memberikan fokus dan perhatiannya pada keamanan informasi yang dimilikinya, karena apabila terdapat kebocoran atas informasi dengan kata lain telah terjadi kegagalan pada sistem keamanan, hal tersebut akan mengakibatkan kerugian, baik secara keuangan maupun kinerja perusahaan. Keamanan secara umum dapat diartikan sebagai "*quality or state of being secure-to be free from danger*". Yang menjadi bahan telaah dalam keamanan informasi antara lain Keamanan Secara Fisik, yaitu salah satu cara dengan memfokuskan pada pengamanan anggota organisasi, aset fisik, akses tanpa wewenang dan tempat kerja dari berbagai ancaman, salah satunya bahaya kebakaran. Lalu, Keamanan Pribadi, cara yang lebih terfokus untuk memberi perlindungan kepada orang-orang dalam organisasi. Kemudian, Keamanan Operasi, cara untuk memberi keamanan pada kemampuan organisasi atau perusahaan untuk bekerja tanpa adanya gangguan maupun ancaman. Adapun Keamanan Berkomunikasi, cara yang ditujukan untuk melindungi media informasi dan teknologi informasi. Serta Keamanan Jaringan, cara untuk fokus mengamankan peralatan jaringan yang ada pada data organisasi.

Keamanan informasi adalah upaya untuk menjaga informasi dari ancaman yang mungkin terjadi dalam kelangsungan bisnis, diantaranya mengurangi tingkat risiko, memberikan rasa percaya sehingga mempercepat investor mengambil keputusan untuk investasi dan menjadi peluang untuk kelancaran bisnis. Tingginya keamanan suatu informasi tidak dapat terlepas dari pentingnya informasi tersebut di dalam basis data, apabila informasi tidak terlalu penting maka keamanannya sedikit longgar, sebaliknya, untuk informasi yang sangat penting maka keamanannya sangat kuat apabila ingin mengakses informasi tersebut. Keamanan atas suatu informasi perbankan dapat didefinisikan sebagai bentuk penerapan dari sebuah sistem dari semua bentuk mekanisme yang memiliki tujuan agar terhindar dari berbagai *cybercrime* atau efek buruk terhadap keamanan atau kerahasiaan informasi nasabah pengguna *internet banking*. Tujuan penerapan keamanan informasi perbankan guna menjalankan asas kerahasiaan dalam perbankan.

Dalam melaksanakan tujuan keamanan informasi perbankan, bank menerapkan beberapa jenis sistem keamanan yang diterapkan dalam *internet banking*², yaitu³ **Cryptography System**, sistem memakai berbagai angka dalam sistemnya atau sering disebut juga dengan istilah *key*. Memiliki kegunaan untuk mengenali nasabah dan memberi perlindungan terhadap semua informasi keuangan nasabah. **Firewall System**, sistem satu ini memiliki kegunaan untuk membatasi akses kepada pihak-pihak yang tidak memiliki izin atau diberi izin untuk memasuki area yang dilindungi atau dijaga dalam Unit Pusat Kerja suatu perusahaan.⁴

Perlindungan Hukum Terhadap Nasabah Internet Banking

Seiring perkembangan zaman, maka semakin inovatif pula produk dan/atau jasa yang dikeluarkan oleh beberapa bank, hal tersebut terlihat dari pelayanan yang memanfaatkan perkembangan teknologi yang ada, yaitu berupa penggunaan internet sebagai media transaksi, hal ini bertujuan untuk meningkatkan kenyamanan nasabah

¹Ramadhani Aditya, "Keamanan Informasi", Surabaya, *Journal of Information and Library Studies*, Vol. 1 No. 1, (2018), hlm. 39.

²G. J. Lewis and K. J. Thygerson, "Financial Institutions Internet Sourcebook". New York, USA: McGraw Hill, 1997.

³R. Annisya and M. N. Hastuti, "Security System Layanan Internet Banking PT Bank Mandiri (Persero) Tbk.," *J. Sist. Komput.*, vol. 2, no. 2, (2012) hlm. 55–60

⁴Indra Ava Dianta dan Edwin Zusrony. "Analisis Pengaruh Sistem Keamanan Informasi Perbankan Pada Nasabah Pengguna Internet Banking" *INTENSIF: Jurnal Ilmiah Penelitian dan Penerapan Teknologi Sistem Informasi*, (2019).

terkait transaksi yang semakin cepat dan mudah. Tetapi, penggunaan media internet tetap memiliki kekurangan yaitu rentan adanya *hacking* atau pembajakan yang akan merugikan nasabah. Permasalahan terkait keamanan tersebut selain menyangkut kepentingan nasabah, adapun menyangkut kepentingan pihak bank sebagai pemberi layanan *internet banking*, maupun ranah perbankan secara menyeluruh. Selain itu, permasalahan terkait keamanan dalam bertransaksi dan perlindungan nasabah menjadi fokus utama untuk memajukan *internet banking* ke depannya, terlebih karena belum hadir konstitusi khusus yang menjamin kepastian hukum guna memberi perlindungan bagi nasabah pengguna *internet banking* di Indonesia.⁵

Meski dewasa ini belum ada konstitusi hukum yang secara mengatur lebih jauh terkait perlindungan hukum bagi nasabah perbankan yang pengguna layanan *internet banking* Indonesia maupun peraturan perundang-undangan khusus mengatur tentang *internet banking* di Indonesia, tetapi dapat ditemui adanya beberapa peraturan yang cukup relevan dengan perlindungan nasabah *internet banking*. Sehingga dalam memberi perlindungan hukum terhadap nasabah pengguna *internet banking* melalui penafsiran atas peraturan-peraturan tersebut untuk turut memberi kepastian hukum terkait *internet banking* adapun dengan menghubungkan peraturan yang satu dengan peraturan yang lainnya. Sehingga pengaturan yang dirasa cukup relevan untuk memberi perlindungan bagi nasabah pengguna *internet banking* antara lain:

Undang-Undang Nomor 7 Tahun 1992 yang diubah menjadi Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan

UU No. 10 Tahun 1998 telah berubah menjadi UU No. 7 Tahun 1992 tentang Perbankan. Dimana UU No. 10 Tahun 1998 ini merupakan peraturan perundang-undangan yang mengubah dan/atau menggantikan dan/atau menambahkan beberapa pasal dari UU No. 7 Tahun 1992. Berdasarkan pada Pasal 1 Angka 1 UU No. 10 Tahun 1998 menentukan bahwa perbankan ialah segala hal yang terkait dengan bank, baik tentang kelembagaan, aktivitas usaha maupun prosedur dan alur pelaksanaan kegiatannya. Salah satu pelaksanaan kegiatan usaha perbankan adalah dengan memberikan pelayanan baik produk maupun jasa kepada nasabah, baik secara konvensional ataupun melalui pemanfaatan teknologi yaitu *Internet Banking*. Menggunakan media internet dalam bertransaksi merupakan suatu bentuk pemanfaatan teknologi oleh bank untuk memasarkan serta memudahkan nasabah untuk bertransaksi dalam jaringan, baik itu merupakan produk dan/jasa yang sudah ada maupun inovasi terbaru.⁶ Berkaitan dengan *internet banking*, ada hal yang perlu mendapat perhatian lebih yaitu terkait kerahasiaan atas data seorang nasabah. Karena ciri dari layanan *internet banking* yang rentan akan kebocoran data pribadi nasabahnya. Peraturan yang dapat menjadi landasan atau dasar untuk memberi kepastian hukum sebagai upaya perlindungan hukum atas data pribadi nasabah pengguna *internet banking* terdapat di dalam Pasal 29 Ayat (4) UU Perbankan yang menyatakan bahwa untuk kepentingan nasabah, bank wajib menyediakan informasi mengenai kemungkinan risiko yang menimbulkan kerugian bagi nasabah yang melakukan transaksi perbankan. Hal tersebut diatur mengingat masyarakat menyimpan dana di bank didasarkan rasa percaya (*Confidence*).⁷

Jika dihubungkan dengan permasalahan terkait perlindungan hukum atas data pribadi nasabah, maka Pasal tersebut dapat turut diterapkan dalam *internet banking*. Penerapan atas suatu aturan pada dasarnya harus dilakukan tanpa diminta, karena bank harus lebih *aware* kepada nasabah dengan memberikan informasi-informasi penting terkait risiko yang rentan timbul karena pemanfaatan layanan *internet banking*, guna menghindari adanya kerugian yang dialami nasabah, serta guna memberikan kenyamanan dan keamanan kepada nasabah.⁸ Selanjutnya ketentuan lain dalam UU Perbankan adalah ketentuan Pasal 40 Ayat (1) dan (2), mengenai kewajiban bank dalam menjaga rahasia terkait nasabah dan tabungannya, terkecuali dalam suatu keadaan tertentu, sebagaimana dimaksud dalam Pasal 41, Pasal 41A, Pasal 42 Pasal 43, Pasal 44 dan Pasal 44A. Sehingga prinsip kerahasiaan bank guna memberi perlindungan kepada nasabah apabila terkait ketentuan tersebut tidak dapat dilakukan secara optimal. Karena perlindungan hukum terkait data pribadi nasabah yang terdapat dalam ketentuan tersebut hanya terhadap data yang disimpan dan dikumpul oleh bank, sedangkan data nasabah pengguna layanan *internet banking* tidak terbatas hanya pada data yang disimpan dan dikumpulkan, tetapi juga data terkait transaksi yang dilakukan oleh nasabah berasal dari komputer mana.

Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen

Peraturan perundang-undangan terkait perlindungan konsumen sangat relevan untuk turut memberikan perlindungan bagi nasabah perbankan, termasuk nasabah pengguna layanan *internet banking*, hal ini karena nasabah perbankan termasuk sebagai kategori konsumen, yaitu yang memakai/menggunakan/menikmati produk dan/atau jasa yang dikeluarkan oleh bank selaku pelaku usaha. Diperlukan seperangkat aturan hukum untuk melindungi konsumen

⁵Nasser Atorf., et.al, *Jurnal Manajemen Teknologi, Vol I*, (Juni 2002)

⁶Budi AgusRiswandi, *Aspek Hukum Internet Banking*, (Jakarta : Raja Grafindo Persada, 2005), hlm. 21.

⁷Pasal 29 ayat 3, Undang-undang Nomor 10 tahun 1998,

⁸Ibid., Pasal 29 ayat 4.

karena konsumen merupakan pihak yang rentan mengalami kerugian, hal ini karena konsumen berada di posisi yang lebih lemah dibandingkan dengan pelaku usaha. Selain itu, pembentukan Undang-undang Perlindungan Konsumen bertujuan untuk melindungi dan kepastian hukum bagi konsumen sebagaimana disebutkan dalam Pasal 1 angka 1 UUPK, yang menentukan bahwa UUPK adalah segala upaya untuk menjamin kepastian hukum serta untuk memberikan perlindungan kepada konsumen. Dari ketentuan tersebut dapat diketahui bahwa perlindungan terhadap konsumen tidak hanya dilakukan untuk memberi perlindungan kepada konsumen, tetapi untuk dapat menempatkan konsumen dalam posisi sejajar dengan pelaku usaha.

Konsumen dalam Pasal 1 Ayat (2) UUPK menentukan bahwa konsumen merupakan seseorang yang membeli, menggunakan, atau memakai barang/jasa untuk dipergunakan sendiri, untuk keluarga, untuk orang sekitar, dan tidak untuk diperjualbelikan kembali.⁷ Selain itu, dalam UUD 1945 Pasal 28D Ayat (1) menentukan bahwa semua orang memiliki hak atas pengakuan, jaminan, perlindungan dan kepastian hukum yang adil, serta mendapat perlakuan yang sama di hadapan hukum. berdasarkan hal tersebut maka Pasal tersebut turut memberikan dasar hukum dalam melindungi konsumen di Indonesia, karena berdasarkan aturan tersebut secara tegas disebutkan bahwa keamanan dan perlindungan atas barang dan/atau jasa yang digunakan atau dikonsumsi adalah hak setiap orang. Sehingga peraturan perundang-undangan mengenai perlindungan konsumen dapat turut menjadi payung hukum untuk melindungi nasabah pengguna layanan *Internet Banking*, terkait berada pada tempat yang sejajar yang disebutkan di dalam Pasal 2 bahwa menentukan asas dalam melindungi konsumen adalah manfaat, adil, seimbang, aman dan keselamatan, serta kepastian hukum.⁹ Oleh karena itu, diberlakukannya pengaturan yang melindungi kepentingan konsumen, maka memberi batasan bagi bank sebagai pemberi pelayanan produk dan/atau jasa perbankan, oleh karenanya bank selaku pelaku usaha dalam memberi pelayanan kepada nasabah berkewajiban diantaranya memiliki itikad baik ketika melaksanakan kegiatan usahanya, informasi yang diberikan benar dan jelas, serta jujur mengenai kondisi dan jaminan atas jasa yang diberikan, memberi perlakuan dan pelayanan kepada konsumen secara benar dan jujur serta tidak diskriminatif, menjamin usaha perbankannya telah sesuai dengan ketentuan atau standar perbankan yang berlaku dan beberapa aspek lainnya.

Selain itu, UUPK turut mengatur hak daripada konsumen, diantaranya untuk mendapatkan rasa aman, nyaman dan jaminan selamat ketika menggunakan barang/jasa, serta hak untuk mendapat kompensasi apabila terbukti apa yang dilakukan pihak bank merugikan nasabah. Dalam Pasal 4 huruf a¹⁰, UUPK menyebutkan tentang hak konsumen atas rasa nyaman, aman dan barang/jasa yang dikonsumsi tidak membahayakan, hal tersebut menjadi tanggungjawab daripada bank sebagai pemberi jasa, sehingga bank wajib melakukan yang terbaik dalam melayani nasabah sebagai konsumen pengguna jasa pelayanan perbankan, karena nasabah berhak mendapat pelayanan terbaik, khususnya menyangkut keamanan dan kenyamanan nasabah itu sendiri. Bank selaku pelaku usaha dalam memenuhi kewajibannya berusaha mematuhi dalam hal memberi pelayanan terbaik, salah satunya dengan menerapkan sistem yang terdiri dari beberapa keamanan seperti yang telah disebutkan pada poin sebelumnya, namun pengamanan yang ada tetap memiliki kekurangan, sehingga masih adanya *cybercrime* yang mengakibatkan kerugian yang dialami oleh nasabah. Undang-undang telah dibentuk sedemikian rupa dan sebaik mungkin untuk memberikan kepastian hukum dan melindungi hak konsumen, namun masih adanya satu dan lain hal yang menjadi penyebab tidak dapat terlaksananya aturan di atas secara optimal. Pasal-pasal yang telah disebutkan di atas merupakan bentuk melindungi melalui pencegahan, yaitu upaya untuk terhindar dari kerugian bagi konsumen.

Melalui pengetahuan atas kepentingan yang dimiliki oleh konsumen, maka meminimalisir terjadinya penipuan dan kerugian. Pasal 4 huruf d¹¹ menentukan bahwa konsumen memiliki hak untuk didengarkan keluhan-kesah atas barang/jasa yang dikonsumsi. pengaturan ini memberi kesempatan bagi nasabah sebagai pengguna jasa pelayanan perbankan untuk dapat menyampaikan baik buruk yang ada pada pelayanan dalam transaksi melalui internet. Lalu bank memberikan *feedback* yakni mendengarkan dan melakukan evaluasi atas pemikiran dan kekurangan yang disampaikan oleh nasabah. Sekalipun mayoritas bank telah melaksanakannya melalui layanan pada *customer service* (CS), tetapi bank tetap perlu meningkatkan sistem terkait keamanan daripada bank dan meningkatkan *Risk Technology* yang dimiliki secara berkesinambungan.

Undang-Undang Nomor 11 Tahun 2008 yang diubah menjadi Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik

Selain itu, terdapat penerapan peraturan perundang-undangan lainnya dalam upaya memberikan kepastian hukum atas tindak pidana siber berdasarkan, yaitu melalui UU ITE. Undang-Undang ini dibuat secara khusus untuk menjadi aturan yang harus ditaati masyarakat Indonesia dalam aktivitas yang berkaitan dengan teknologi, informasi serta komunikasi serta tindak kejahatan yang termasuk tindakan pidana siber. Namun selain UU ITE, adapun

⁹Pasal 2 Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen

¹⁰Sembiring Sentosa, *HimpunantentangPerlindunganKonsumendanPeraturan Lain yang terkait*, (Bandung :NuansaAulia, 2010), hlm12.

¹¹Pasal 4 huruf d, Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen.

peraturan perundang-undangan lain yang turut mengatur tentang tindak pidana siber, baik mengatur secara khusus maupun umum, yang mana memerlukan penafsiran atau menghubungkan terlebih dahulu antara satu dan lain konstitusi ada.

Dalam konstitusi Indonesia, kriminalisasi tindak pidana terkait teknologi memiliki pengaruh atas upaya untuk mementaskan tindak pidana terkait teknologi di Indonesia, baik di Indonesia itu sendiri secara khusus maupun di dunia secara umum.¹² UU ITE kemudian diubah menjadi UU ITE, setelah perubahan tersebut, UU ITE dirasa telah layak untuk turut menjadi aturan terkait masalah-masalah yang terdapat dalam transaksi *Internet banking*, yang mana merupakan produk layanan perbankan yang berkaitan erat dengan transaksi yang memanfaatkan teknologi. Hambatan yang terdapat pada teknologi serta hukum tidak sepenuhnya akan menghambat jalannya *internet banking*, sekalipun tidak ada pengaturan khusus yang mengatur, hal ini karena terdapat berbagai pengaturan lain yang turut mengatur transaksi dalam *internet banking*.

Setiap pelaksanaan yang memanfaatkan elektronik wajib untuk mengadakan pola penggunaan elektronik secara cakap, aman dan bertanggungjawab terhadap sistem elektronik yang beroperasi atau berjalan sesuai ketentuannya.¹³ **Cakap** memiliki arti bahwa pola dalam pemanfaatan elektronik tersebut memiliki kemampuan yang tepat dengan yang dibutuhkan oleh klien. **Aman** memiliki arti bahwa pola pemanfaatan elektronik dilindungi baik fisik maupun nonfisik. **Beroperasi sesuai ketentuan** memiliki arti bahwa pola pemanfaatan elektronik memiliki kemampuan yang tepat dengan spesifikasi atau sesuai kegunaannya. Selain itu, pelaksana sistem elektronik¹⁴ **Bertanggungjawab**, yang memiliki arti adanya orang atau badan hukum yang memiliki tanggungjawab yang berkaitan dengan hukum terhadap pelaksanaan pola pemanfaatan elektronik tersebut. Namun ketentuan tersebut tidak berlaku apabila terbukti adanya unsur memaksa dalam pelaksanaan tersebut, adanya kekeliruan dari pihak pengguna pola pemanfaatan elektronik¹⁵. Undang-undang ITE juga menentukan bahwa sepanjang belum diatur oleh konstitusi tersendiri, setiap penyelenggara pola pemanfaatan elektronik wajib mengoperasikan pola pemanfaatan elektronik dengan tunduk pada persyaratan sebagai berikut¹⁶, yaitu menampilkan informasi elektronik dan dokumen elektronik secara lengkap dan waktu yang sepadan dengan jumlah pembayaran yang telah diatur dalam pengaturan yang berlaku, mampu memberikan perlindungan atas informasi yang utuh, otentik, rahasia, dan tidak ada hambatan dalam mengakses, pelaksanaannya yang sebagaimana mestinya, mempunyai suatu proses yang berkesinambungan untuk terus memelihara informasi elektronik tetap baru, jelas dan bertanggungjawab secara alur maupun barang.

Selain itu, perlindungan hukum yang diberikan oleh UU ITE terkait melindungi data pribadi, berkaitan dengan kepentingan pribadi klien (*privacy*), dalam Pasal 26 menyebutkan bahwa kecuali ditentukan lain oleh suatu konstitusi tersendiri, apabila menyangkut informasi pribadi orang lain maka harus mendapat persetujuan dari orang yang bersangkutan. Perkembangan teknologi informasi saat ini sangat rentan terhadap keamanan atas kerahasiaan data daripada nasabah pengguna *internet banking*. Salah satunya karena masih adanya kekurangan atas upaya pencegahan dari berbagai pihak terhadap kejahatan dan penyalahgunaan media internet, sehingga mengakibatkan kerugian, terutama kepada nasabah sebagai pihak yang paling rentan mengalami kerugian.

Undang-undang Nomor 36 Tahun 1999 Tentang Telekomunikasi

Selain pengaturan hukum yang telah disebutkan sebelumnya, ada pun pengaturan hukum lainnya, dalam hal ini mengatur mengenai data pribadi nasabah, yang termaktub dalam Pasal 22 UU Telekomunikasi yang menentukan semua orang yang tidak memiliki hak, tidak diperbolehkan masuk, serta masuk secara ilegal dilarang mengakses jasa, jaringan khusus, dan jaringan telekomunikasi. Ketentuan ini dapat dikaitkan pada dengan permasalahan data pribadi nasabah dalam pelaksanaan layanan *internet banking*, terlihat adanya perbedaan dimana informasi yang dilindungi dalam ketentuan ini lebih fokus terhadap data yang ada dalam jaringan, bukan pada data yang sedang ditransfer.¹⁷ Aturan terkait hukuman bagi pihak yang melanggar Pasal 22 UU Telekomunikasi termaktub di dalam Pasal 50 dengan ketentuan akan mendapat hukuman penjara maksimal enam tahun dan/atau denda maksimal 600 juta rupiah. Ketentuan yang ada pada peraturan di atas dapat diterapkan terhadap kasus mengenai kerahasiaan nasabah terkait data dan hak yang diperoleh oleh nasabah terjadi hal yang merugikan pada saat menggunakan *Internet Banking*, tetapi kembali lagi pada jenis kasusnya. Aturan yang ada dalam perundang-undangan perbankan tidak berlaku untuk kasus kerugian akibat *Typosquatting*, dimana nasabah mengakses web plesetan, karena data nasabah yang mengalami kebocoran bukanlah kesalahan dari pihak bank, melainkan kekurangtelitian nasabah yang mengakibatkan terjadinya

¹²SigidSuseno, "Yuridiksi Tindak Pidana Siber", (Bandung : Refika Aditama, 2012) hlm. 165.

¹³Pasal 15 Ayat (1), Undang-undang Nomor 11 Tahun 2008 yang diubah menjadi Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik

¹⁴Ibid, Pasal 15 Ayat (2).

¹⁵Ibid, Pasal 15 Ayat (3).

¹⁶Ibid, Pasal 16.

¹⁷Budi AgusRiswandi, op.cit.,hlm. 223.

tindak kejahatan.

Dari yang telah dijelaskan di atas, perlindungan hukum bagi nasabah pengguna layanan *Internet Banking* dilakukan melalui cara, baik *selfregulation* maupun *government regulation*¹⁸ maka dapat disimpulkan bahwasannya upaya terkait perlindungan hukum yang ada saat ini belum sepenuhnya menjamin keamanan serta mewujudkan asas keseimbangan. Sehingga masih diperlukan adanya peraturan khusus atau konstitusi yang merefleksikan terkait hak dan kewajiban secara seimbang antara pihak bank sebagai pemberi layanan *Internet Banking* dan nasabah sebagai pengguna layanan *internet banking*.

Tanggungjawab yang diberikan oleh pihak bank terhadap nasabah yang mengalami kerugian dalam penggunaan *Internet Banking*

Dewasa ini tidak dapat dipungkiri bahwa teknologi mengalami kemajuan yang sangat pesat, pemanfaatan teknologi hampir terjadi di segala aktivitas masyarakat, baik itu untuk informasi maupun transaksi, tidak terkecuali dalam sektor perbankan. Saat ini, aktivitas terkait perbankan dapat dijalankan dengan menggunakan teknologi elektronik, yakni menggunakan internet sebagai media. Dari inovasi tersebut memunculkan istilah *Internet Banking*, dimana adanya pelayanan dari perbankan yang dilakukan melalui internet, antara lain membuka akun rekening atau tabungan, mengirim uang dan pembayaran secara daring. Namun ada yang perlu diperhatikan oleh nasabah, yaitu dalam menjalankan kegiatan elektronik banking penting untuk mengimplementasikan manajemen atas risiko yang mungkin terjadi dalam aktivitas *internet banking* secara terarah dan berkelanjutan. Dengan adanya risiko dalam aktivitas *internet banking*, maka sebagai upaya meningkatkan rasa kepercayaan nasabah, bank sebagai pemberi layanan *internet banking* perlu meningkatkan perlindungan dan memberi kepastian hukum. selain untuk mendapat kepercayaan nasabah, bank juga perlu memperhatikan keamanan dan kenyamanan, karena risiko yang ditimbulkan dalam layanan *internet banking* rentan terjadi, beberapa kemungkinan kerugian yang akan dialami nasabah adalah karena telah diintervensi oleh *hacker/cracker* sehingga dapat memasuki *firewall*¹⁹ atau dapat mengakses *website* dengan nama domain yang sangat mirip karena telah di plesetkan oleh pelaku kejahatan untuk mengecoh nasabah (*typosquatting*). Berikut adalah hal-hal penting yang dilakukan oleh bank yang bertujuan untuk memberi perlindungan terhadap nasabah, antara lain :

Pemberian rasa aman oleh bank kepada nasabah pengguna layanan *internet banking* telah dilaksanakan secara baik dan juga meliputi aspek-aspek yang harus ada dalam suatu keamanan, yaitu meliputi kerahasiaan, integritas, autentikasi atau keaslian, ketersediaan, pengaturan dalam mengakses dan tidak adanya penolakan saat yang memiliki wewenang mengakses, karena dewasa ini hampir semua bank apabila nasabah melakukan transaksi lewat *internet banking* menggunakan token PIN sebagai pengamanan tambahan, hal ini sebagai upaya perlindungan terhadap nasabah, karena token PIN dirasa dapat memberi perlindungan yang mumpuni dengan fungsinya yaitu untuk memunculkan password dinamis atau berbeda-beda tiap kali melakukan transaksi atau disebut juga dengan one time password (OTP). Dengan fungsi token PIN tersebut, dapat meminimalisir disalahgunakannya rekening nasabah, sekalipun informasi yang nasabah masukkan terbaca oleh *keylogger*. Dalam mendapatkan akses masuk ke dalam sistem *Internet Banking*, pengguna *internet banking* hanya perlu memasukkan ID pengguna atau nasabah dan PIN *Internet Banking* (PIN tetap) yang telah nasabah buat ketika mendaftarkan diri untuk menggunakan layanan *internet banking*. Token PIN memiliki karakteristik sama seperti kalkulator yaitu berukuran kurang lebih 3 x 5 centimeter. Dengan fasilitas Token PIN diharapkan mampu memberi rasa aman terhadap nasabah, dikarenakan dari token PIN tersebut memunculkan Password yang terus berganti apabila melakukan transaksi, hal ini akan membuat orang lain kesulitan untuk mengetahui informasi nasabah. Selain itu, token PIN nasabah yang satu dengan yang lain pasti berbeda, serta tidak dapat digunakan pada rekening lainnya.²⁰

Adapun upaya lain dari bank dalam menjaga privasi nasabah serta informasi dalam jenis apapun terkait keuangan nasabah yang menggunakan layanan *internet banking*. Untuk berkomitmen dalam menjamin rasa aman dan privasi nasabah, baik dalam hal keuangan, maupun transaksi, maka terdapat beberapa sistem dalam *Internet Banking* yang berfungsi untuk memberi perlindungan terhadap informasi dan data nasabah, antara lain:

1. **ID Pengguna dan PIN (Personal Identification Number)**, merupakan *code* yang bersifat rahasia dan hanya nasabah yang berwenang atang ID Pengguna serta PIN tersebut, apabila nasabah hendak mengakses atau masuk ke dalam *Internet banking* maka harus input ID Pengguna dan PIN yang telah dibuat saat mendaftar akun *internet banking*, apabila melakukan transaksi finansial, nasabah akan diarahkan untuk kembali memasukkan PIN, hal tersebut bertujuan untuk terhindar dari kejahatan ketika komputer yang masih terhubung dengan *internet banking* ditinggalkan.

¹⁸Budi AgusRiswandi, *Aspek Hukum Internet Banking*, (Jakarta : Raja GrafindoPersada, 2005), hlm. 200.

¹⁹Ibid.

²⁰Dwi Ayu Astrini, "Perlindungan Hukum Terhadap Nasabah Pengguna Internet Banking Dari Ancaman *Cybercrime*", *Lex Privatum*, Vol. 3 No. 1, (2015), hlm. 158

2. Secara otomatis akan keluar dari akun (*automatically log out*), apabila dalam jangka waktu 10 menit tidak terdeksi adanya tindakan, maka secara otomatis *internet banking* akan berakhir dan akan keluar dan kembali pada halaman utama.
3. **SSL 128-bit encryption**, Standar dalam mengirim data rahasia, dimana data akan diubah menjadi kode rahasia oleh Protokol SSL dengan memakai dua pangkat seratus dua puluh delapan kombinasi password, namun hanya terdapat satu dari beberapa angka kombinasi tersebut yang benar dan dapat membuka kode rahasia tersebut.
4. **Firewall**, berfungsi untuk memberi batasan dan jaminan bahwa hanya nasabah yang dapat mengakses atau masuk ke dalam sistem *internet banking*.²¹

Dalam hal melindungi berdasarkan aspek hukum, yang paling tepat untuk menjamin kepastian hukum yakni terdapat di dalam "*policy and terms*" *internet banking*, karena dalam ketentuan tersebut turut memuat hak serta kewajiban pihak bank dan pihak nasabah. Namun ketentuan dalam kebijakan dan ketentuan tersebut bersifat perjanjian standar atau baku, yang dibuat oleh bank secara sepihak, sehingga nasabah tidak dapat menyampaikan keinginannya dalam ketentuan tersebut, sehingga perjanjian tersebut tidak memberikan posisi seimbang antara nasabah dan bank, karena dalam ketentuan tersebut lebih didomisasi kewajiban nasabah dan hak daripada bank. Kebijakan dan ketentuan tersebut dapat ditemui pada halaman menu di website *internet banking* serta buku panduan yang difasilitasi oleh bank. Dalam memberi perlindungan atas privasi nasabah baik yang menyangkut dengan transaksi perbankan, maupun informasi lainnya akan disimpan dengan kerahasiaan dan sesuai peraturan perundang-undangan di Indonesia, sehingga tidak ada seorang pun yang tanpa wewenang dapat mengaksesnya.

Serta dari aspek tanggungjawab bank sebagai pemberi layanan *internet banking* meminta nasabah untuk lebih berhati-hati dan memiliki tingkat kewaspadaan yang tinggi, serta cermat dalam mengakses layanan perbankan melalui internet. Apabila dirasa terjadi sesuatu yang janggal, indikasi kejahatan dan akan membahayakan akun nasabah pengguna *internet banking*, sebaiknya cepat melaporkan kepada pihak bank, pelaporan dapat dilakukan melalui *Call Center* maupun *Costumer Service Officer*.

Ketika terjadi kerugian yang diterima oleh nasabah pengguna *internet banking*, maka bank akan melakukan pengecekan terlebih dahulu, pengecekan tersebut meliputi aktivitas transaksi, catatan, rekaman, dan semua yang dikirimkan nasabah secara online kepada bank, apabila terbukti kerugian tersebut melibatkan pihak bank, dalam hal bank lalai atau terjadi kesalahan secara tidak sengaja, maka berdasarkan kesepakatan bersama, nasabah akan mendapatkan kompensasi dari bank sebagai ganti rugi, yang disesuaikan dengan kerugian materiil yang dialami oleh nasabah.²²

SIMPULAN

Berdasar pada yang telah dijelaskan pada pembahasan dapat disimpulkan bahwa:

1. Aspek-aspek yang harus diperhatikan dalam keamanan informasi perbankan diantaranya, **Kerahasiaan** yaitu terkait kerahasiaan informasi dan data nasabah serta yang memiliki akses hanyalah pihak yang memiliki wewenang. **Integritas** yaitu terkait jaminan bahwa tidak dapat mengubah data tanpa seizin pihak yang memiliki wewenang atas data tersebut serta mengamankan dan menjaga kelengkapan atas informasi dari ancaman dan kerusakan pada data dan informasi yang asli. **Ketersediaan** yaitu terkait jaminan atas data yang selalu tersedia ketika dibutuhkan dan nasabah mendapatkan informasi tanpa ada gangguan.
2. Perlindungan dalam aspek hukum bagi nasabah pengguna *internet banking* menjadi kepastian hukum guna menjamin keamanan dan kenyamanan nasabah, perlindungan hukum tersebut diantaranya:
 - a. Undang-undang Nomor 7 Tahun 1992 yang diubah menjadi Undang-undang Nomor 10 tahun 1998 tentang Perbankan
 - b. Undang-undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen
 - c. Undang-undang Nomor 11 Tahun 2008 yang diubah menjadi Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik
 - d. Undang-undang Nomor 36 Tahun 1999 Tentang Telekomunikasi
3. Pertanggungjawaban pihak bank terhadap kerugian yang dialami oleh nasabah pengguna *internet banking* yaitu berupa pertanggungjawab bank sebagai pemberi layanan *internet banking* dengan mengingatkan nasabah agar lebih hati-hati, memiliki tingkat kewaspadaan yang tinggi dan cermat pada saat menggunakan layanan *internet banking*. Apabila ada hal yang terasa yang janggal, ada indikasi kejahatan dan membahayakan, maka nasabah diminta untuk segera melapor kepada *Call Center* dan *Costumer Service Officer* pada bank terkait. Adapun terkait kompensasi

²¹Budi AgusRiswandi, *Aspek Hukum Internet Banking*, (Jakarta : Raja GrafindoPersada, 2005), hlm. 200.

²²Bank BCA, *BukuPanduanKemudahanDalamSatuKlik*, hlm 15.

apabila kerugian yang dialami oleh nasabah terbukti karena kelalaian atau ketidaksengajaan pihak bank, maka bank akan memberikan ganti rugi secara materiil sesuai kesepakatan antara nasabah dan bank.

DAFTAR PUSTAKA

Buku

Bank Central Asia, Buku Panduan Kemudahan Dalam Satu Klik.

G. J. Lewis, K. J. Thygerson, *Financial Institutions Internet Sourcebook*. New York, USA: Mc Graw Hill, 1997.

Riswandi, Budi, *Aspek Hukum Internet banking*, Yogyakarta : PT Raja Grafindo Persada, 2005.

Sentosa, Sembiring, *Himpunan tentang Perlindungan Konsumen dan Peraturan Lain Yang Terkait*, Bandung : NuansaAulia, 2010.

Suseno, Sigid, *Yuridiksi Tindak Pidana Siber*, Bandung :RefikaAditama, 2012.

Whitman, Michael. E dan Herbert J. Mattord, *Principles of Information Security*, 6th Edition, 2018

Jurnal Hukum

Atorf, et.al., *Jurnal Manajemen Teknologi, Vol I*, (Juni 2002).

Annisya dan M. N. Hastuti, "Security System Layanan *Internet banking* PT Bank Mandiri (Persero) Tbk.", *J. Sist. Komput*, vol. 2, (2012).

Astrini, Dwi Ayu, "Perlindungan Hukum Terhadap Nasabah Pengguna *Internet banking* Dari Ancaman *Cybercrime*", *Lex Privatum*, Vol. 3 No. 1, (2015)

Ramadhani, Aditya, "Keamanan Informasi", Surabaya, *Journal of Information and Library Studies*, Vol. 1 No. 1, (2018).

Indra Ava Dianta, Edwin Zusrony. "Analisis Pengaruh Sistem Keamanan Informasi Perbankan Pada Nasabah Pengguna Internet Banking" , *INTENSIF: Jurnal Ilmiah Penelitian dan Penerapan Teknologi Sistem Informasi*, (2019).

Peraturan Perundang-undangan

Undang-undang Nomor 7 Tahun 1992 yang diubah menjadi Undang-undang Nomor 10 tahun 1998 tentang Perbankan

Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen

Undang-undang Nomor 36 Tahun 1999 Tentang Telekomunikasi

Undang-Undang Nomor 11 Tahun 2008 yang diubah menjadi Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik