Journal Evidence Of Law
Volume 1 Nomor 1
Januari 2022
DOI : 12345

ANALISA YURIDIS DALAM KASUS KEJAHATAN SIBER TERHADAP INTERNET BANKING DI INDONESIA

JURIDICAL ANALYSIS IN CYBER CRIME CASES ON INTERNET BANKING IN INDONESIA

Delvyan Putri Surya Ningrum
Sekolah Tinggi Ilmu Hukum IBLAM
devlyanputri@gmail.com

Jamiatur Robekha
Sekolah Tinggi Ilmu Hukum IBLAM
Jamiaturrobekha@iblam.ac.id

Abstrak: *Internet banking atau mobile banking merupakan bukti perkembangan di dunia teknologi yang bersangkutan dengan dunia perbankan. Perkembangan teknologi tersebut menjadi salah satu hasil dari semakin pesatnya dunia teknologi informasi sehingga memudahkan masyarakat terutama nasabah untuk melakukan transaksi melalui internet. Fitur internet banking menjadi salah satu pemanfaatan melalui media internet serta informasi guna mempromosikan dan juga memberikan kemudahan dalam melakukan transaksi. Baik yang bersifat konvensional maupun dengan fitur-fitur terbaru. Perkembangan teknologi tersebut tentu saja memiliki dampak buruk terutama di sisi kejahatan dunia siber. Kejahatan ini merupakan bentuk kejahatan yang memanfaatkan dunia teknologi informasi dan perkembangannya dengan memanfaatkan internet. Kasus yang baru-baru saja terjadi yaitu pencurian data nasabah milik Bank Syariah Indonesia menjadi salah satu bukti bagaimana kejahatan dunia siber masih terus menghantui. Kasus kejahatan siber kembali terjadi terutama di sektor perbankan setelah sebelumnya Bank Rakyat Indonesia yang juga merupakan bank pemerintah harus mengalami kasus yang sama pada salah satu layanan BRI yaitu BRI Life tahun 2021 lalu. Pada penelitian yang menggunakan metode kualitatif ini ditujuan untuk menguji analisa yuridiksi mengenai kejahatan dunia siber terhadap internet banking atau mobile banking di Indonesia.*

Kata Kunci: internet banking, kejahatan siber, yuridiksi

Abstract: *Internet banking or mobile banking is evidence of developments in the world of technology concerned with the world of banking. The development of this technology is one of the results of the increasingly rapid world of information technology, making it easier for people, especially customers, to make transactions via the internet. The internet banking feature is one of the uses through internet media and information to promote and also provide convenience in making transactions. Both conventional and with the latest features. The development of this technology certainly has a bad impact, especially on the cybercrime side. This crime is a form of crime that takes advantage of the world of information technology and its development by utilizing the internet. The case that recently occurred, namely the theft of customer data belonging to Bank Syariah Indonesia, is one proof of how cyber crime still continues to haunt us. Cybercrime cases have reoccurred, especially in the banking sector after previously Bank Rakyat Indonesia, which is also a state-owned bank, had to experience the same case in one of BRI's services, namely BRI Life, in 2021. This research using qualitative methods aims to test jurisdictional analysis regarding cyber crimes against internet banking or mobile banking in Indonesia.*

Keywords: internet banking, cyber crime, jurisdiction

PENDAHULUAN

Perkembangan dunia teknologi informasi sekarang ini semakin maju dan sangat pesat. Hal ini tentu saja memberikan kemudahan bagi masyarakat dalam berurusan dengan dunia perbankan. Dunia internet sendiri sudah mulai ditemukan sejak tahun 1969. Dan mulai menjadi primadona sejak tahun 90-an di Indonesia meski belum sangat cepat sekarang ini. Baru di tahun 2010-an, Indonesia mendapatkan perkembangan internet yang sangat cepat dan memberikan kemudahan kepada masyarakat.

Internet menyajikan sebuah dampak yang signifikan dalam kehidupan masyarakat. Dan bukan hanya dari segi komunikasi dengan basis komputer semata, namun perkembangan di sektor lain juga didapatkan oleh masyarakat. Perkembangan dunia internet memiliki salah satu kemudahan yang diterima oleh masyarakat dimana salah satunya adalah transaksi bisnis melalui internet. Bahkan seluruh perbankan dan juga perusahaan di dunia sudah memaksimalkan dan memanfaatkan fasilitas internet tersebut. perkembangan internet juga membuat perkembangan di sisi negatif. Meski ada sisi positif yang bisa didapatkan oleh

masyarakat, namun tidak dipungkiri ada pula sisi negatif yang harus mendapatkan perhatian [1].

Transaksi bisnis, pemindahan dana dan juga transaksi konvensional pada pelayanan bank menjadi salah satu dampak positif yang bisa digunakan oleh masyarakat. Kegiatan transaksi perbankan melalui fitur internet banking atau mobile banking merupakan kegiatan yang sekarang ini sudah menjadi agenda penting bagi masyarakat. Dengan internet banking dan mobile banking, masyarakat bisa melakukan transaksi jual beli melalui aplikasi banking yang mereka miliki. Hal ini tentu saja sangat efisien dan juga efektif bagi masyarakat yang ingin bergerak cepat dan juga tidak ingin membuang-buang waktu pergi ke ATM atau ke kantor cabang dari bank yang digunakan.

Manfaat dari perkembangan teknologi tersebut tentu bukan hanya kepada masyarakat yang menggunakannya untuk kegiatan positif. Di sisi lain manfaat tersebut juga dirasakan oleh para penjahat yang menggunakan teknologi informasi untuk kegiatan negatif. Hal ini terlihat dengan semakin meningkat pula praktik kejahatan di dunia baru yaitu cyber crime atau kejahatan siber. Kejahatan siber atau cyber crime ini adalah sebuah tindakan kriminal yang dilakukan oleh penjahat siber dengan memanfaatkan perkembangan teknologi informasi dimana komputer dan perangkat elektronik lainnya sebagai alat untuk melaksanakan kejahatan mereka.

Kejahatan siber merupakan bentuk kejahatan dimana memiliki definisi sebagai perbuatan pelanggaran hukum dengan memanfaatkan teknologi komputer dengan basis dunia internet yang sekarang ini sudah sangat canggih dan juga cepat. Di media-media internet sekarang ini sudah banyak kejahatan yang kerap terjadi. Mulai dari penipuan yang mengatas namakan pihak bank hingga proses penipuan pada transaksi jual beli. Dan yang baru-baru ini kembali terjadi adalah pencurian data para nasabah yang menyimpan dana atau uang mereka di bank pemerintah yaitu Bank Syariah Indonesia [2].

Kejahatan siber yang mencuri data nasabah ini biasanya meminta tebusan dari pemerintah untuk mengembalikan dana mereka. Bahkan tidak jarang nilai rekening para nasabah akan hilang dan hangus tanpa ada jejak. Selain itu data-data dari para nasabah ini masuk ke dalam penyimpanan para penjahat untuk digunakan di kemudian hari. Kejahatan yang sama terjadi pada BRI melalui salah satu layanan mereka yaitu BRI Life dimana semua data para nasabah diambil dan dicuri [3].

---

[1] Dharma, Adhi Aryyaguna, "Tinjauan Kriminologis Terhadap Kejahatan Penipuan Berbasis Online (Studi Kasus Unit Cyber Crime Reskrimsus Polda Sulsel)" Skripsi Departemen Hukum Pidana Fakultas Hukum Universitas Hasanuddin Makassar, 2017.

[2] Aisah, Siti. "Penegakan Hukum Tindak Pidana Penipuan Online Di Kabupaten Sleman Yogyakarta Secara Integratif", Skripsi Program Studi Ilmu Hukum Fakultas Hukum Universitas Ahmad Dahlan 2019

[3] Ali, Zainuddin. Hukum Pidana Islam. Jakarta: Sinar Grafika, 2012.

Kejahatan dunia siber menjadi salah satu bukti dari dampak negatif yang tentu saja harus mendapatkan antisipasi dan juga ditanggulangi dengan payung hukum yang memiliki keterkaitan dengan dunia teknologi informasi serta komunikasi. Landasan hukum untuk dunia ini adalah Undang-Undang No. 11 Tahun 2008 mengenai dunia informasi dan juga Transaksi Elektronik atau disebut juga dengan UU ITE. Payung hukum tersebut menjadi sebuah pemikiran yang komprehensif dari pemerintah sebagai salah satu cara untuk menjamin sebuah perlindungan hukum bagi masyarakat yang menggunakan teknologi informasi tersebut.

Perlindungan hukum ini tentu saja bukan hanya ditujukan kepada pengguna teknologi informasi yang dipakai secara positif semata. Namun Undang-Undang ini dimaksudkan bisa memberikan pencegahan serta mengungkap semua bentuk kejahatan terutama penipan melalui transaksi perbankan dan juga dunia elektronik.

Kemudahan yang didapatkan oleh masyarakat melalui layanan internet banking dan mobile banking, tentu saja ada resiko dan ancaman besar yang mengintai para pengguna jasa teknologi informasi tersebut. Resiko dan ancaman tersebut berhubungan dengan kejahatan siber dan juga pelanggaran hukum. Para penjahat siber ini akan mencuri data-data dari para nasabah. Resiko yang berhubungan dengan data pribadi dan finansial memang bukan barang baru. Data yang didapatkan ini nantinya akan digunakan sebagai alat pencucian uang serta berhubungan dengan terorisme. Indonesia sendiri masuk ke dalam 10 besar serangan kejahatan dunia siber dan memiliki tingkat resiko yang sangat besar terhadap keamanan siber. Hal ini menjadi bukti belum ada payung hukum dan juga fitur keamanan yang hebat dalam menjaga data-data nasabah di bank pemerintah.

Kejahatan dunia siber atau cyber crime adalah sebuah kejahatan di dunia maya yang menyerang sisi keamanan dalam jaringan komputer dan juga informasi teknologi telekomunikasi. Di era globalisasi sekarang ini tentu saja kemajuan teknologi dan informasi. Dampak negatif dari sisi perkembangan tersebut tentu saja kejahatan di dunia siber atau cyber crime yang bisa memberikan kerugian kepada masyarakat. Sedangkan kejahatan tersebut memiliki kaitan yang erat dengan hasil dari budaya bangsa tersebut. Semakin tinggi tingkat budaya yang dianut oleh sebuah bangsa dan juga semakin modern serta berkembangnya sebuah bangsa, maka akan berbanding lurus dengan tingkat kejahatan yang hadir pada bangsa tersebut. Baik dalam bentuk, sifat dan juga cara pelaksanaan kejahatan tersebut [4].

Perkembangan di dunia teknologi komputer dan juga informasi serta komunikasi, memberikan kemungkinan muncul dan berkembangnya tindak kejahatan yang menyajikan karakteristik yang jauh berbeda dengan tindakan kejahatan konvensional yang sudah cukup marak terjadi di tengah masyarakat. Penyalahgunaan teknologi informasi seperti jaringan internet dan juga komputer menjadi dampak yang muncul dari berkembangnya teknologi di era modern. Dan hal ini tidak terlepas dari sifat yang mempunyai ciri tersendiri dimana membawa

[4] Amaliah, Dista Arifah. "Kasus Cybercrime Di Indonesia", Jurnal Bisnis dan Ekonomi (JBE) 18:2 September 2011.

permasalahan yang akan dipecahkan berhubungan dengan permasalahan penanggulangan menurut pemikiran dari (Edmon Makarim,2005).

Dari pendapat dan penuturan tersebut, bisa disebut pula bahwa kemajuan teknologi dan informasi bagaikan pedang bermata dua yang bisa memberikan dampak positif sekaligus negatif. Dampak negatif dengan penyalahgunaan teknologi ini bisa memberikan tindakan pidana yang disebut kejahatan dunia siber atau cyber crime. Dan tindakan kejahatan tersebut mempunyai sifat dan karakteristik yang berbeda dimana kejahatan tersebut memiliki hubungan dengan jaringan internet dan teknologi. Praktis penanganan kasus kejahatan tersebut berbeda dengan tindakan kejahatan konvensional [5].

Kejahatan siber tentu saja sangat berbeda dengan dunia kejatan konvensional atau disebut sebagai street crime. Kejahatan tersebut memang muncul berbarengan dengan lahirnya perkembangan teknolgi informasi yang diharapkan bisa membantu manusia dalam perkembangannya. Ciri lain dari revolusi teknologi menurut pemikiran Nitibaskara bahwa interaksi sosial yang meminimalisir interaksi secara fisik, menjadi salah satu cirinya. Dan penyimpangan di bidang sosial akan beradaptasi dan membentuk karakter baru di dalam dunia kejahatan [6].

Kejahatan di dunia maya menurut peraturan perundang-undangan kerap dihubungkan dengan kejahatan tindak pidana yang memiliki hubungan erat dengan teknologi informasi. Dan kejahatan dunia siber merupakan kejahatan dan tindak pidana yang menggunakan jaringan informasi serta teknologi demi mendapatkan keuntungan atau data secara ilegal dan tidak sah demi kepentingan pribadi atau kelompok yang memberikan kerugian kepada masyarakat.

Dasar hukum serta landasan untuk menindak kejahatan dunia siber ini adalah Undang-Undang No. 36 Tahun 1999 yang mengatur dunia Telekomunikasi. Pada peraturan Undang-Undang tersebut dibuat guna melakukan akomodir mengenai sanksi pidana dari kejahatan pidana dunia siber. Kemudian tahun 2008 pemerintah mengeluarkan Undang-Undang No. 11 Tahun 2008 mengenai Informasi dan Transaski Elektronik. Pada peraturan Undang-Undang No.11 Tahun 2008 ini sudah mengatur mengenai tindak pidana kejahatan dunia siber. Ada beberapa pasal yang mengatur permasalahan tersebut yang terdiri dari:

1. Pasal 22

   Pasal ini menyatakan bahwa setiap warga negara atau masyarakat yang berada di wilayah hukum Indonesia dilarang melakukan tanpa adanya hak dan juga sah serta melakukan manipulasi ke jaringan telekomunikasi dan atau jasa komunikasi serta akses ke jaringan

[5] Hamzah, Andi. Asas-Asas Hukum Pidana, Jakarta: Rineka Cipta, 1994.

[6] Ayu, Gusti Shabaina Jayantari & Dewa Gede Dana Sugama, "Kekuatan ALat Bukti Dokumen Elektronik dalam Tindak Pidana Berbasis Teknologi dan Informasi (Cyber Crime)", Program Kekhususan Peradilan Fakultas Hukum Universitas Udayana.

telekomunikasi khusus.

2. Pasal 38

   Pasal ini menyatakan bahwa dilarang menimbulkan gangguan fisik dan juga elektromagnetik kepada penyedia jasa atau operator dari telekomunikasi tersebut.

3. Pasal 40

   Pasal ini menyebutkan bahwa dilarang melakukan penyadapan dalam bentuk apapun dan juga menyalurkannya.

Undang-Undang No. 11 Tahun 2008 yang mengatur tentang Informasi dan juga Transaksi Elektronik ditujukan untuk melakukan akomodir mengenai pengelolaan informasi dan juga transaksi secara elektronik sebagai landasan hukum atau payung hukum jika terjadi penyalah gunaan teknologi informasi dan transaksi elektronik tersebut. Pastinya penyalah gunaan ini bisa memberikan kerugian kepada pribadi, masyarakat dan juga negara. Hal ini termasuk ke dalam tindak pidana kejahatan siber.

Peraturan Perundang-undangan tersebut menetapkan dan mengatur mengenai perbuatan yang temasuk ke dalam kejahatan dunia siber dan juga menentukan unsur tindak pidana kepada kepentingan hukum. Dan ada beberapa pasal yang mengatur mengenai kejahatan dunia siber yang terdiri dari:

1. Pasal 27
   a. Ayat 1

      Pasal dan ayat ini menetapkan bahwa setiap orang yang dengan sengaja melakukan distribusi dan atau transmisi akan akses informasi elektronik atau dokumen yang memiliki muatan dimana melanggar kesusilaan atau pornografi.

   b. Ayat 2

      Sementara pada ayat 2 diatur mengenai penetapan bentuk kejahatan dunia siber dimana setiap orang yang dengan sengaja melakukan distribusi dan atau transmisi ke dunia elektronik dan informasi dengan muatan perjudian. Hal ini termasuk ke dalam kejahatan dunia siber.

   c. Ayat 3

      Pada ayat 3 disebutkan bahwa setiap orang yang menggunakan dan atau mendistribusikan data melalui dunia informasi elektronik yang mempunyai muatan pencemaran nama baik atau penghinaan. Hal ini masuk ke dalam kateogri kejahatan dunia siber.

   d. Ayat 4

      Sementara ayat ke-4 pada Pasal 27 mengatur jenis kejahatan siber yang memiliki sangkut paut akan pemerasan dan pengancaman melalui jaringan internet atau informasi teknologi.

2. Pasal 28

a. Ayat 1
   Ayat ini menyebutkan salah satu jenis kejahatan dunia siber yaitu penyebaran hoax atau berita bohong yang membuat kerugian pihak tertentu.
b. Ayat 2
   Pada ayat ini disebutkan bahwa seseorang yang menyebarkan rasa kebencian dan mengandung SARA atau Suku, Agama, Ras dan Antar Golongan, termasuk ke dalam kejahatan dunia siber.

3. Pasal 29
   Pasal 29 menyebutkan jika seseorang tanpa hak mengirim informasi yang berisi ancaman serta menakut-nakuti pihak lain atau personal maka termasuk ke dalam tindakan kejahatan siber
4. Pasal 30
   a. Ayat 1
      Disebutkan pada pasal ini bahwa jika seseorang mengakses informasi atau komputer milik orang lain tanpa adanya hak, maka dianggap sebagai kejahatan siber
   b. Ayat 2
      Jika seseorang tanpa hak dan melawan hukum dengan mencoba mengakses komputer atau sistem elektronik tanpa ijin dan dengan cara apapun yang bertujuan mendapatkan data secara ilegal, maka akan ditindak.
   c. Ayat 3
      Jika seseorang tanpa hak dan ijin melampaui, melanggar dan juga menjebol sistem pengamanan termasuk ke dalam kejahatan dunia siber atau cyber crime.
5. Pasal 31
   a. Ayat 1
      Pada ayat ini disebutkan jika seseorang tanpa ijin dan hak serta melanggar hukum melakukan penyadapan pada komputer atau sistem elektronik milik orang lain, termasuk ke dalam tindak pidana cyber crime.
   b. Ayat 2
      Perbuatan tanpa hak dan melawan hukum melakuan intersepsi mengenai transmisi di bidang informasi elektronik terhadap dokumen yang sifatnya privat dan bukan publik meski tidak melakukan perubahan pada data dan dokumen tersebut, maka termasuk ke dalam klasifikasi kejahatan siber.
   c. Ayat 3
      Pada ayat 3 ini merupakan pengecualian dari ayat 1 dan 2 dimana intersepsi atau penyadapan bisa dilakukan dalam rangka penegakan hukum. Namun harus mendapatkan persetujuan atau

permintaan dari Polisi, Kejasakaan dan juga penegak hukum lainnya.

6. Pasal 32
   a. Ayat 1
      Seseorang yang melakukan tindakan tanpa hak dan melawan hukum merusak hingga menyembunyikan informasi elektronik baik milik pihak pribadi atau data milik publik.
   b. Ayat 2
      Jika seseorang tanpa ijin mentransfer atau memindahkan data elektronik tanpa berhak, maka termasuk ke dalam tindakan kejahatan siber
   c. Ayat 3
      Jika seseorang melakukan perbuatan pada ayat 1 dan 2 kemudian data tersebut bersifat rahasia, maka mendapatkan hukuman yang cukup berat diakibatkan melakukan tindakan kejahatan siber.
7. Pasal 33
   Pada pasal 33 disebutkan bahwa seseorang yang melakukan gangguan kepada sistem informasi elektronik maka masuk ke dalam klasifikasi kejahatan siber. Dan hal ini biasanya menyerang dunia perbankan demi mendapatkan data nasabah serta mencuri dana dari nasabah tersebut.
8. Pasal 34
   a. Ayat 1
      Seseorang yang memproduksi, mengimpor hingga menjual perangkat keras dan lunak tanpa ijin hingga sandi serta kode akses maka termasuk ke dalam indikasi kejahatan siber.
   b. Ayat 2
      Isi dari ayat 2 ini mengenai seseorang yang melakukan perbuatan pada Ayat 1 dan sudah mendapatkan ijin untuk kegiatan penelitian hingga sistem elektronik, maka sah dan diperbolehkan di dalam ranah hukum.
9. Pasal 35
   Jika seseorang melakukan manipulasi, perubahan dan juga perusakan informasi elektronik, maka dianggap melakukan tindakan pidana kejahatan siber
10. Pasal 36
    Pasal 36 berisi mengenai tindakan yang dilakukan seseorang dari pasal 27 hingga pasal 34 yang memberikan akibat kerugian bagi pihak lain, masuk ke dalam ranah kejahatan siber.
11. Pasal 37
    Berisi bagi seseorang yang melakukan pelanggaran dari Pasal 27 hingga Pasal 36 yang berada di luar wilayah Indonesia namun

melakukan pelanggaran tersebut terhadap sistem elektronik di Indonesia, maka termasuk ke dalam kejahatan siber sesuai dengan Undang-Undang tersebut.

Dari ketentuan dan juga landasan hukum yaitu Undang-Undang No. 11 Tahun 2008 ini maka bisa dilihat ada beberapa bentuk kejahatan siber atau cyber crime tersebut [7]. Dan bentuk dari kejahatan dunia siber ini adalah:

1. Kejahatan siber yang menggunakan teknologi informasi seperti komputer sebagai alat utama dalam tindak kejahatan. Seperti penyebaran pornografi, perjudian hingga pencemaran melalui sosial media hingga penipuan. Begitu pula dengan pemalsuan serta pemerasan hingga pengancaman. Tidak lupa pula hoax yang disebar melalui media sosial tersebut.
2. Sementara kejahatan siber yang memiliki kaitan dengan dunia informasi elektronik dan berhubungan dengan komputer serta jaringan sebagai sasaran utama. Seperti mengakses data yang tidak legal, mengganggu sistem komputer dan data yang ada di dalamnya hingga penyadapan. Dan hal ini biasa terjadi pada sistem keamanan siber perbankan di Indonesia.

Transaksi di dunia perbankan menjadi salah satu kegiatan yang kerap mendapatkan incaran dari pihak-pihak yang hendak melakukan kejahatan. Data dari nasabah akan disadap dan semua perincian data akan didapatkan hingga digunakan untuk kegiatan yang negatif. Seperti pencucian uang hingga pendanaan teroris.

Penyidikan akan dilakukan jika terindikasi ada perbuatan kejahatan siber yang dilaporkan oleh para korban. Penyedidikan sendiri memiliki definisi sebagai rangkaian dari penyidin guna mengumpulkan bukti yang kuat agar pelaku bisa ditangkap dan dihukum sesuai dengan ketentuan perundang-undangan yang berlaku.

Menurut pemikiran dari M. Yahya (2006) bahwa kegiatan penyidikan merupakan tindakan lanjutan dari terjadinya tindak pidana dimana persyaratan dan juga pembatasannya cukup ketat dalam upaya mengumpulkan bukti agar tindak pidana tersebut bisa teratasi dan menemukan titik terang dengan tertangkapnya pelaku atau tersangka.

Pihak kepolisian menjadi salah satu aspek penyidik yang ada di bawah payung hukum UU No. 2 Tahun 2002 Pasal 1 ayat 1 mengenai Kepolisian Negara Republik Indonesia dimana menyatakan bahwa Kepolisian memiliki fungsi sebagai lembaga yang berkaitan erat dengan tindak pidana dan juga berhak melakukan penyidikan. Praktis pihak kepolisian memiliki wewenang dan tugas untuk melakukan penyelidikan jika terjadi kasus kejahatan siber tersebut.

[7] Partodihardjo, Soemarno. Tanya Jawab Sekitar Undang-undang No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, Jakarta: Gramedia Pustaka Utama, 2008.

Menurut pemikiran dari Riduan Syahrani (2004) bahwa teori efektifitas hukum ini ditentukan oleh beberapa faktor untuk melihat apakah teori tersebut efektif atau tidak. Dan ke-5 faktor tersebut adalah:

1. Undang-undang
   Hukum akan disebut efektif jika berdasarkan kepada isi dari peraturan tersebut. Dan hal ini berlaku kepada yuridis, sosiologis dan juga filosofis
2. Penegak hukum
   Pihak yang akan menerapkan hukum dan melakukan penyidikan atas terjadinya sebuah tindakan pidana. Para penegak hukum yang dimaksud adalah kepolisian, pengadilan, hakim dan juga pengacara serta masyarakat.
3. Sarana
   Sarana yang dimaksud adalah tenaga manusia yang terampil dan berpendidikan dengan peralatan yang memadai dan juga keuangan yang cukup.
4. Masyarakat
   Masyarakat menjadi salah satu penegak hukum yang bisa membantu tugas kepolisian dalam menginformasikan adanya tindakan kejahatan di lingkungan mereka.
5. Kebudayaan
   Kebudayaan sendiri memiliki cakupan nilai yang menjadi dasar akan hukum yang berlaku. Nilai tersebut merupakan konsepsi abstrak akan hal yang dianggap baik atau buruk.

METODE PENELITIAN

Pada penelitian ini digunakan metode penelitian kualitatif dimana metode tersebut akan mengharuskan para peneliti melakukan penelitian dengan terjun langsung ke lapangan serta ke obyek penelitian [8]. Metode penelitian kualitatif deskriptif ini berisi penelitian yang melakukan pendekatan kepada studi kasus atau case study yang berhubungan dengan penelitian yang sedang dilakukan [9].

Pendekatan studi kasus atau case study menjadi salah satu bagian dari metode kualitatif yang bisa mendalami sebuah kasus dengan lebih detail dan mendalam dengan melakukan pengumpulan data berupa informasi dari berbagai macam sumber [10]. Studi kasus ini memiliki definisi sebagai eksplorasi dari

[8] Raco, J.R. Metode Penelitian Kualitatif Jenis, Karakteristik, dan Keunggulannya. Jakarta: PT. Grasindo, 2010.

[9] Sugiyono. Memahami Penelitian Kualitatif. Bandung: Alfabeta, 2014. Sumadi, Hendy. "Kendala Dalam Menanggulangi Tindak Pidana Penipuan Transaksi Elektronik Di Indonesia" Jurnal Wawasan Hukum, 33:2 September 2015.

[10] Gunawan, Imam. Metode Penelitian Kualitatif: Teori dan Praktik. Jakarta: Bumi Aksara, 2015.

berbagai macam sistem yang saling berkaitan atau disebut pula dengan bounded system dari kasus tersebut. Sebuah kasus akan menarik untuk diteliti dengan alasan corak atau kekhasan dari kasus yang mempunyai peranan penting di dalamnya [11].

Pada penelitian kali ini akan diteliti mengenai kejahatan dunia siber terhadap internet banking atau mbanking pada kasus Bank Syariah Indonesia serta BRI Life yang teradi beberapa waktu lalu. Sumber data yang diperlukan pada penelitian ini yaitu sumber data primer berupa wawancara langsung kepada beberapa informan atau responden. Lalu sumber data sekunder berupa data dari buku, jurnal dan juga penelitian terdahulu sebagai acuan.

HASIL PENELITIAN DAN PEMBAHASAN

Dunia perbankan menjadi salah satu area yang mendapatkan keuntungan dengan perkembangan dunia teknologi dan informasi sekarang ini. Bank-bank di Indonesia memberikan kemudahan kepada para nasabah mereka dengan mengeluarkan jenis layanan-layanan baru agar para nasabah semakin mudah bertransaksi di dunia perbankan. Layanan konvensional berubah ke arah layanan modern dengan adanya layanan internet banking dan mobile banking. Layanan ini menjadi salah satu bukti perkembangan dunia teknologi tersebut.

Internet banking dan mobile banking menjadi salah satu inovasi pengembangan dari media internet yang terus pesat. Sehingga para nasabah tidak perlu repot lagi untuk datang ke kantor cabang atau kantor pusat dari bank yang digunakan untuk melakukan transaksi perbankan. Hanya kala keperluan tertentu saja nasabah harus datang ke kantor. Bahkan sekarang ini membuka rekening sudah bisa dilakukan melalui internet banking. Begitu juga dengan transaksi di e-commerce yang juga sudah bisa terkoneksi melalui aplikasi mobile banking. Tidak perlu lagi membuka aplikasi jual beli online.

Tentu saja pihak perbankan harus memperhatikan sisi keamanan atau privasi dari para nasabah mereka. Hal ini sesuai dengan Pasal 28G ayat 1 dari UUD 1945 yang menyatakan bahwasanya setiap warga negara berhak mendapatkan perlindungan diri terhadap pribadi, keluarga dan juga kehormatan serta martabat yang berada di bawah kendali kekuasaannya termasuk harta benda. Dan berhak mendapatkan rasa aman dan perlindungan dari ancaman yang mengganggu hak asasi.

Sementara pada Pasal 29 ayat 4 UU Perbankan disebutkan bahwasanya demi kepentingan nasabah, maka pihak perbankan wajib memberikan informasi bahwa adanya resiko kerugian yang bisa saja terjadi dengan transaksi nasabah melalui bank. Hal ini disebabkan bank mendapatkan dana dari masyarakat yang memberikan kepercayaan kepada mereka. Dan penerapan peraturan tersebut tentu saja penting untuk diterapkan di dunia perbankan sebagai bentuk perlindungan hukum bagi nasabah.

[11] Ahmadi, Rulam. Metodologi Penelitian Kualitatif. Yogyakarta: Ar-Ruzz Media, 2014.

Pihak perbankan selain melakukan sosialisasi kepada penyedia jasa layanan aplikasi internet banking dan juga mobile banking kepada nasabah, harus memberikan jaminan keamanan yang terjadi. Apalagi di dalam pemakaian internet banking tersebut, ada berbagai ancaman yang bisa didapatkan oleh masyarakat termasuk kepada penyedia layanan. Aspek perlindungan kepada data dan juga dana nasabah harus menjadi perhatian oleh pihak perbankan.

Perlindungan hukum kepada nasabah yang memakai aplikasi internet banking yang berhubungan dengan teknologi keamanan harus memenuhi beberapa aspek yang terdiri dari:

1. Sifat rahasia
2. Integritas
3. Autentikasi
4. Ketersediaan layanan
5. Kontrol akses
6. Non-repudiation.

Pihak bank harus memberikan keamanan bagi nasabah agar meminimalisir kejahatan dunia siber di dalam proses transaksi melalui internet banking. Seperti penipuan mendapatkan hadiah dimana nasabah diminta untuk pergi ke ATM untuk memasukkan kode atau dengan membuka aplikasi yang mirip seperti aplikasi internet banking sehingga semua data dari nasabah bisa tersedot oleh pelaku kejahatan. Sehingga semua data dan juga dana akan secara otomatis bisa dikontrol oleh pihak yang tidak bertanggung jawab tersebut. Hal ini menjadi salah satu kerja keras dari pihak bank memberikan edukasi kepada nasabah [12].

Berdasarkan penelitian yang pernah dilakukan oleh Rahmah (2018) bahwa pemakaian internet banking dan juga mobile banking memiliki pengaruh yang cukup besar kepada kejahatan dunia siber. Hal ini menunjukkan kejahatan siber sekarang ini sudah mulai cangging serta mengancam para nasabah di dunia perbankan. Layanan dan transaksi konvensional mulai ditinggalkan dimana para nasabah sekarang kerap melakukan transaksi menggunakan internet banking serta Qris yang terhubung dengan aplikasi mobile banking. Belum lagi dengan e wallet yang juga terkoneksi dengan mobile banking [13].

Sayangnya layanan yang mulai berkembang dan juga mendukung kebutuhan para nasabah, tidak dilengkapi dengan keamanan siber yang canggih. Hal ini terlihat dari kasus yang terjadi pada Bank Jatim dan juga BRI Life pada tahun 2021 serta di tahun 2022 Bank Indonesia mengeluarkan statemen bahwa mereka

---

[12] Gunawan, Hendra. "Tindak Pidana Penipuan Dalam Persfektif Fikih Jinayah", Jurnal El-Qanuny: Jurnal Ilmu-Ilmu Kesyariatan dan Pranata Sosial 4:2 Desember 2018.

[13] Rahmah, Y . N. (2018). *Pengaruh Penggunaan Internet Banking Dan Perlindungan Nasabah Pengguna Fasilitas Internet Banking Terhadap Cyber Crime Di Daerah 'Istimewa Y ogyakarta.* Jurnal Pendidikan dan Ekonomi, *Banking* di Era Millenium III, Jakarta: Majalah Bank dan Manajemen. Vol. 7, HAl579-588.

mendapatkan serangan ransomware. Dalam kurun waktu 1 tahun, bank sentral Indonesia dan juga 2 bank milik pemerintah mendapatkan tindakan kejahatan di dunia siber.

Sebuah kejadian yang sebenarnya mencoreng dunia perbankan Indonesia. Apalagi Bank Indonesia menggalahkan digitalisasi untuk semua layanan perbankan. Bahwa masyarakat bisa melakukan semua transaksi tanpa uang kertas alias cashless. Bank Indonesia ingin menciptakan cashless society. Hal ini untuk memberikan kemudahan bagi nasabah. Namun kejadian peretasan data-data para nasabah dari sistem perbankan seolah memberi bukti bahwa Indonesia belum terlalu siap untuk menuju ke dunia digital.

Setahun dari serangan ransomware yang diterima Bank Indonesia, kembali bank pemerintah yaitu Bank Syariah Indonesia mengalami hal yang sama. Beberapa nasabah mengalami permasalahan tidak bisa mengakses aplikasi BSI Mobile yang awalnya disebabkan proses maintenance yang dilakukan oleh BSI. Namun nasabah tidak bisa mengakses selama beberapa hari yang menimbulkan kecurigaan bagi para nasabah.

Dan pakar keamanan dunia siber baru kemudian mengungkapkan bahwasanya BSI terkena serangan ransomware dan disetujui oleh pihak BSI melalui akun media sosial mereka bahwa aplikasi BSI Mobile terkena ransomware. Yang mengejutkan adalah data sebesar 1,5 TB dimana terdapat 15 juta data pengguna dan juga password milik nasabah diambil oleh peretas yang menutup akses internal dan juga layanan dari bank BSI. Data tersebut bisa saja langsung digunakan oleh peretas. Namun pihak peretas meminta tebusan untuk semua data dari Bank Syariah Indonesia tersebut.

Disebutkan ransomware Lockbit menyerang keamanan siber dari Bank Syariah Indonesia tersebut. Dan 15 juta data nasabah sudah masuk ke kantong para peretas. Sewaktu-waktu mereka bisa menggunakan data dan dana dari para nasabah dengan bebas tanpa ada ijin. Kejadian kejahatan dunia siber di perbankan membuat para nasabah mendapatkan kerugian. Sebagian warga Aceh yang menggunakan Bank Syariah Indonesia menyatakan bahwa mereka menginginkan bank konvensional kembali dibuka di Aceh. Rata-rata responden dan juga informan di Aceh menyatakan bahwa BSI tidak bisa menjawab kepercayaan nasabah dan publik mengenai data-data dan dana yang diberikan oleh para nasabah [14].

Usai tidak bisa diaksesnya aplikasi internet banking milik BSI, beberapa waktu lalu aplikasi BCA Mobile juga tidak bisa diakses selama beberapa menit. Hal ini mengundang rasa khawatir dari banyak nasabah. Apalagi BCA menjadi salah satu bank swasta yang cukup canggih tingkat keamanannya dan juga salah satu bank dengan nasabah yang cukup besar di Indonesia. Bahkan errornya aplikasi BCA Mobile langsung menjadi trending topic di media sosial twitter. Hal ini membuat nasabah khawatir jika BCA akan mengalami hal yang sama seperti BSI. Jika Bank Central Asia yang memiliki sistem keamanan yang cukup canggih bisa

[14] Monica, Melisa Sumenge "Penipuan Menggunakan Media Internet Berupa Jual-Beli Online" Lex Crimen 2:4 Agustus 201

dibobol oleh peretas, tentu membuat nasabah mulai berpikir kembali guna menyimpan uang mereka di bank.

Apalagi sekarang sudah banyak pihak perbankan yang mengeluarkan bank digital demi memudahkan para nasabah untuk bertransaksi. Bank digital seperti Jenius milik BTPN, Jago dari Bank Jago serta blu dari bang BCA dan juga Digibank dari Bank DBS Indonesia ini memang dibangun dan diciptakan untuk memberikan kemudahan dalam bertransaksi. Akan tetapi dengan kejadian terhadap Bank Jatim, Bank BRI terhadap akun nsabah dan juga BRI Life hingga Bank Indonesia dan BSI, tentu membuat masyarakat harus memikirkan kembali untuk meletakkan uang mereka di bank digital [15].

Sementara dari sisi yuridiksi perlindungan hukum mengenai kejahatan dunia siber, pemerintah sudah memiliki landasan hukum mengenai cyber crime tersebut yang terdapat pada Undang-Undang No. 11 Tahun 2008 pada Pasal 33. Akan tetapi pemerintah belum menyediakan payung hukum untuk nasabah mengenai permasalahan keamanan siber yang cenderung mudah untuk diretas. Landasan hukum bagi penyedia jasa dan perbankan yang teledor dalam menjaga data dan dana nasabah belum ada payung hukum yang jelas. Landasan hukum yang berlaku di Indonesia hanya mengatur kepada pihak pelaku. Sedangkan peraturan kepada pihak layanan jasa terkait kewajiban mereka dan juga kelalaian yang terjadi masih belum ada aturan yang jelas.

KESIMPULAN

Kemudahan di dalam dunia perbankan memang memberikan kemudahan layanan kepada para nasabah dalam melakukan transaksi perbankan tersebut. Perkembangan dunia digital dan juga teknologi informasi, memberikan kemudahan bagi para bank-bank baik milik pemerintah dan swasta untuk menyajikan layanan yang bisa memudahkan dalam proses transaksi dan mulai mengurangi layanan konvensional. Praktis memberikan kemudahan kepada semua nasabah.

Akan tetapi perkembangan di dunia perbankan ini tidak dibarengi dengan sistem keamanan siber yang masih sangat mudah untuk diretas. Dalam kurun waktu 3 tahun terakhir mulai dari tahun 2021 hingga 2023 ini, sudah ada 4 bank yang mengalami peretasan pada sistem layanan dan keamanan siber. Bank Jatim dan BRI seperti layanan BRI mobile serta BRI Life harus terkena serangan ransomware. Sementara tahun 2022, Bank Indonesia mendapatkan serangan tersebut. Dan beberapa waktu lalu Bank Syariah Indonesia harus kecolongan 15 juta data para nasabah berupa data pribadi yang digunakan untuk kontrol akses serta password.

Hal ini memberikan bukti bahwa keamanan siber di Indonesia masih sangat rendah. Para peretas dengan mudah melakukan pembobolan data pribadi dari para

[15] Maskun. Kejahatan Siber (Cyber Crime) Suatu Pengantar. Jakarta: Kencana, 2014.

nasabah. Dan data ini bisa digunakan untuk memindahkan dana ke rekening lain tanpa perlu persetujuan dari nasabah. Dan ini tentu memberikan kerugian bagi dunia perbankan termasuk pihak bank dan juga kepercayaan dari nasabah kepada layanan perbankan. Bisa saja para nasabah mulai memikirkan untuk menyimpan uang mereka dengan cara konvensional .

Pemerintah sudah menyiapkan payung hukum untuk melindungi tindak kejahatan dunia siber terutama di sisi perbankan. Sementara pihak kepolisian sebagai penyidik juga sudah siap untuk bergerak mengatasi permasalahan tersebut. Hanya saja belum ada landasan hukum terhadap data dan dana milik nasabah yang dicuri oleh pihak peretas diakibatkan sistem keamanan siber milik perbankan yang lemah. Dalam kurun waktu beberapa hari para nasabah tidak bisa mengakses dan memiliki peluang besar dana mereka akan hangus dalam sekejap. Jika hal tersebu terjadi, belum ada ketegasan dari pemerintah melalui peraturan dan perlindungan dari aspek yuridiksi hukum guna memberikan kenyamanan kepada para nasabah tersebut.

DAFTAR PUSTAKA

Ahmadi, Rulam. Metodologi Penelitian Kualitatif. Yogyakarta: Ar-Ruzz Media, 2014.

Aisah, Siti. "Penegakan Hukum Tindak Pidana Penipuan Online Di Kabupaten Sleman Yogyakarta Secara Integratif", Skripsi Program Studi Ilmu Hukum Fakultas Hukum Universitas Ahmad Dahlan 2019

Ali, Zainuddin. Hukum Pidana Islam. Jakarta: Sinar Grafika, 2012.

Amaliah, Dista Arifah. "Kasus Cybercrime Di Indonesia", Jurnal Bisnis dan Ekonomi (JBE) 18:2 September 2011.

Ayu, Gusti Shabaina Jayantari & Dewa Gede Dana Sugama, "Kekuatan ALat Bukti Dokumen Elektronik dalam Tindak Pidana Berbasis Teknologi dan Informasi (Cyber Crime)", Program Kekhususan Peradilan Fakultas Hukum Universitas Udayana.

Dharma, Adhi Aryyaguna, "Tinjauan Kriminologis Terhadap Kejahatan Penipuan Berbasis Online (Studi Kasus Unit Cyber Crime Reskrimsus Polda Sulsel)" Skripsi Departemen Hukum Pidana Fakultas Hukum Universitas Hasanuddin Makassar, 2017.

Gunawan, Hendra. "Tindak Pidana Penipuan Dalam Persfektif Fikih Jinayah", Jurnal El-Qanuny: Jurnal Ilmu-Ilmu Kesyariatan dan Pranata Sosial 4:2 Desember 2018.

Gunawan, Imam. Metode Penelitian Kualitatif: Teori dan Praktik. Jakarta: Bumi Aksara, 2015.

Hamzah, Andi. Asas-Asas Hukum Pidana, Jakarta: Rineka Cipta, 1994.

Ilyas, Amir. Asas-asas Hukum Pidana. Yogyakarta: Rangkang Education, 2012

Iqbal, Muhammad. "Media Sosial sebagai Sarana Tindak Pidana Penipuan", Fakultas Ilmu Sosial, Universitas Islam Kuantan Singingi.

Jannah, Sofwan & M. Naufal. "Penegakan Hukum Cyber Crime Ditinjau Dari Hukum Positif Dan Hukum Islam" Al-Mawarid 12:1 Feb-Agust 2012
Janwari, Yadi. Asuransi Syari'ah. Bandung: Pustaka Bani Quraisy, 2005
Kurniawan, Gahfuur Pangku Alam. "Analisis Yuridis Penegakan Hukum Pidana Terhadap Tindak Pidana Penipuan Bisnis Online" Skripsi Program Studi Hukum Fakultas Hukum Universitas Muhammadiyah Palembang, 2020.
Lamintang, P.A.F. Dasar-dasar Hukum Pidana Indonesia. Bandung: Citra Aditya Bakti. 1997.
M. Arief, Dikdik Mansur, Elisatris Gultom. Cyber Law Aspek Hukum Teknologi Informasi. Bandung: PT. Refika Aditama, 2009.
M Yahya Hhrp. 2006. *Pembahasan Permasalahan Dan Penerapan KUHAP :Penyidikan Dan Penuntutan*. Jakarta : Sinar Grafika. Hal. 210.
Makarim, Edmon, 2005, *Pengantar Hukum Telematika (Suatu Kajian Kompilasi),* Jakarta PT Raja Grafindo Persada, hlm. 426.
Maskun. Kejahatan Siber (Cyber Crime) Suatu Pengantar. Jakarta: Kencana, 2014.
Miftah, Shabur Maulana, Heru Susilo & Riyad, "Implementasi E-Commerce Sebagai Mediapenjualan Online", Jurnal Administrasi Bisnis (Jab) 29:1 Desember 2015
Moeljatno. Asas-Asas Hukum Pidana. Jakarta: PT Rineka Cipta, 2015
Monica, Melisa Sumenge "Penipuan Menggunakan Media Internet Berupa Jual-Beli Online" Lex Crimen 2:4 Agustus 201
Nitibaskara, Ronni R dalam Didik M. Arief Mansur dan Elisatris Gultom, 2005, *Cyber Law Aspek Hukum Teknologi Informasi,* Bandung, PT Refika Aditama, hlm. 25.
Partodihardjo, Soemarno. Tanya Jawab Sekitar Undang-undang No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, Jakarta: Gramedia Pustaka Utama, 2008.
Pasal 5 ayat (1) dan (2) Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (ITE)
Raco, J.R. Metode Penelitian Kualitatif Jenis, Karakteristik, dan Keunggulannya. Jakarta: PT. Grasindo, 2010.
Rahmah, Y . N. (2018). *Pengaruh Penggunaan Internet Banking Dan Perlindungan Nasabah Pengguna Fasilitas Internet Banking Terhadap Cyber Crime Di Daerah 'Istimewa Y ogyakarta.* Jurnal Pendidikan dan Ekonomi, *Banking* di Era Millenium III, Jakarta: Majalah Bank dan Manajemen. Vol. 7, HAl579-588.
Rahmi, Nailul. "Hukuman Potong Tangan Perspektif Al-Qur`An Dan Hadis", Jurnal Ulunnuha 7:2, Desember 2018
Sugiyono. Memahami Penelitian Kualitatif. Bandung: Alfabeta, 2014. Sumadi, Hendy. "Kendala Dalam Menanggulangi Tindak Pidana Penipuan Transaksi Elektronik Di Indonesia" Jurnal Wawasan Hukum, 33:2 September 2015.
Syahrani, Riduan. 2004. *Rangkuman Intisari Ilmu Hukum*. Banjarmasin. PT. Citra Aditya Bakti. Hal. 184.