HASANATUL MUNAWARAH, S.E., M.H.
DR. MAHMUD YUSUF, M.S.I

Editor: Parman Komarudin, S.H.I., M.H.I.

BANK DIGITAL SYARIAH

ANALISIS CYBER SECURITY MENURUT HUKUM POSITIF DI INDONESIA DAN HUKUM EKONOMI SYARIAH

BANK DIGITAL SYARIAH
ANALISIS CYBER SECURITY MENURUT HUKUM POSITIF DI INDONESIA DAN HUKUM EKONOMI SYARIAH

HASANATUL MUNAWARAH, S.E., M.H.
Dr. MAHMUD YUSUF, M.S.I

PT.BDProject

PT. BORNEO DEVELOPMENT PROJECT

BANK DIGITAL SYARIAH
ANALISIS CYBER SECURITY MENURUT HUKUM POSITIF DI INDONESIA DAN HUKUM EKONOMI SYARIAH

HASANATUL MUNAWARAH, S.E., M.H.
Dr. MAHMUD YUSUF, M.S.I

Editor:
Parman Komarudin, S.HI., M.HI.

BANK DIGITAL SYARIAH: ANALISIS CYBER SECURITY MENURUT HUKUM POSITIF DI INDONESIA DAN HUKUM EKONOMI SYARIAH

Penulis :
Hasanatul Munawarah, S.E., M.H.
Dr. Mahmud Yusuf, M.S.I

Editor :
Parman Komarudin, S.HI., M.HI.

Hak cipta dilindungi oleh Undang-undang. All Rights Reserved
Dilarang mengutip atau memperbanyak sebagian atau seluruh isi buku ini tanpa izin tertulis dari penerbit

—Banjarmasin: 2022
vi+141 hal; 150x230 mm
ISBN : **978-623-98738-8-2**

Penyunting :
Syauqi Mahendra

Cetakan I: Oktober 2022
Diterbitkan oleh:
PT. Borneo Development Project
Anggota IKAPI: No. 005/KSL/2021

Kata Pengantar

Puji dan Syukur kepada Allah Yang Maha Pengasih dan lagi Maha Penyayang. Atas limpahan rahmat, taufiq dan hidayah-Nya, atas izin dan kehendak-Nyalah Buku ini dapat diselesaikan tepat pada waktunya. Shalawat dan Salam semoga selalu terlimpahkan kepada Rasulullah SAW, keluarga dan sahabatnya.

Buku yang berjudul "Analisis *Cyber Security* Pada Bank Digital Menurut Hukum Positif Di Indonesia dan Hukum Ekonomi Syariah" dimana buku ini berbicara tentang Bank digital syariah, alat keamanan, kebijakan, konsep, dan tindakan keamanan menurut hukum positif di Indonesia dan juga *Cyber Security* menurut hukum ekonomi syariah.

Buku ini berbicara mengenai kumpulan alat keamanan, kebijakan, konsep, tindakan keamanan, pedoman, pendekatan manajemen risiko, tindakan, pelatihan, praktik terbaik, jaminan, dan alat dalam pandangan hukum positif dan hukum ekonomi syariah. Teknologi yang dapat digunakan untuk melindungi lingkungan jaringan dan aset organisasi dan pengguna. Organisasi mengamankan jaringan dan aset pengguna termasuk perangkat komputerisasi yang terhubung, personel, infrastruktur, aplikasi, layanan, sistem telekomunikasi, dan semua informasi yang dikirimkan dan/atau disimpan di dunia maya.

Penulis menyadari bahwa penulisan buku ini jauh dari sempurna, terutama dibidang hukum yang dalam perkembangannya terus mengalami perubahan seiring dengan perubahan masyarakat dengan segala permasalahanya. namun penulis berharap buku ini bisa memberikan pengetahuan dalam bidang ilmu hukum cyber dan juga dalam pandangan hukum ekonomi syariah.

Ucapan terima kasih kami sampaikan kepada seluruh tim yang telah terlibat dalam penyusunan buku ini yang tidak bisa kami sebutkan satu persatu. Kami

menyadari masih terdapat kekurangan dalam buku ini untuk itu kritik dan saran terhadap penyempurnaan buku ini sangat diharapkan. Semoga buku ini dapat memberi manfaat bagi semua pihak yang membutuhkan.

Banjarmasin, Oktober 2022

Penulis

Daftar Isi

Kata Pengantar iv

Daftar Isi vi

BAB I PENDAHULUAN 1

BAB II DESKRIPSI UMUM 11

A. Definisi Istilah 11

B. Bank Digital 13

C. Cyber Security 37

D. Hukum Positif di Indonesia 63

E. Hukum Ekonomi Syariah 64

BAB III *CYBER SECURITY* MENURUT HUKUM POSITIF DI INDONESIA DAN HUKUM EKONOMI SYARIAH 70

A. Cyber Security Menurut Hukum Positif di Indonesia 70

B. Pengaturan Kejahatan Siber (Cybercrime) pada Perbankan 77

C. Cyber Security menurut Hukum Ekonomi Syariah 81

BAB IV ANALISIS *CYBER SECURITY* PADA BANK DIGITAL MENURUT HUKUM POSITIF DI INDONESIA DAN HUKUM EKONOMI SYARIAH 86

A. *Cyber Security* Pada Bank Digital PT Bank Aladin Syariah Tbk. 86

B. Analisis Cyber Security pada Bank Digital Menurut Hukum Positif di Indonesia 96

C. Analisis Cyber Security pada Bank Digital menurut Hukum Ekonomi Syariah 114

Daftar Pustaka 132

BAB I
PENDAHULUAN

Perkembangan zaman telah menyebabkan terjadinya perubahan sistem teknologi informasi di berbagai strata masyarakat, sehingga memudahkan masyarakat dalam melakukan aktivitas sehari-hari. Perkembangan teknologi dan kecepatan pengumpulan informasi tidak hanya membantu untuk memenuhi kebutuhan dunia pendidikan, tetapi juga sangat membantu kegiatan dunia ekonomi.

Pertumbuhan teknologi pula sudah bawa sesuatu pergantian kebutuhan oleh warga atas sesuatu perlengkapan pembayaran yang bisa penuhi kecepatan, ketepatan, serta keamanan dalam tiap transaksi elektronik. Sejarah meyakinkan pertumbuhan perlengkapan pembayaran terus berubah-ubah wujudnya, mulai dari wujud logam, duit kertas konvensional, sampai perlengkapan pembayaran sudah berevolusi yang berbentuk informasi yang bisa ditempatkan pada sesuatu wadah ataupun diucap dengan perlengkapan pembayaran elektronik .[1]

Teknologi dan *financial* memiliki hubungan yang berkaitan. Saat ini telah hadir teknologi yang mengarah pada inovasi *financial* dengan sentuhan teknologi modern di bidang jasa yang bernama *Financial Technology*. Di sisi lain, perkembangan *e-commerce* juga telah mendorong berkembangnya alat pembayaran dari yang

[1] Adiyanti, Arsita Ika, *Pengaruh Pendapatan, Manfaat, Kemudahan Penggunaan, Daya Tarik Promosi, dan Kepercayaan Terhadap Minat Menggunakan Layanan E-Money*, 2015.

awalnya *cash based instruments* (alat pembayaran tunai) kini bertambah alat pembayaran baru yang dikenal *non cash based instruments* (alat pembayaran non tunai) yang mana *non cash based instruments* ini pun telah berkembang sehingga tidak lagi berbasis kertas melainkan juga *paperless* (tidak berbasis kertas).[2]

Pemanfaatan pertumbuhan teknologi data secara lebih maksimal ialah ketentuan dalam menunjang inovasi layanan bank. Inovasi layanan serta penyelenggaraan strategi dalam penggunaan teknologi data mendesak perbankan buat merambah masa layanan perbankan digital. "Layanan ini bertujuan meningkatkan efisiensi kegiatan operasional dan mutu pelayanan bank kepada nasabahnya. Untuk itu, bank perlu mengembangkan "strategi bisnis" menuju layanan perbankan digital.

Peraturan OJK No.12/POJK.03/2018 Tentang Penyelenggaraan Layanan Perbankan Digital Oleh Bank Umum, "layanan perbankan digital adalah layanan perbankan elektronik yang dikembangkan dengan mengoptimalkan pemanfaatan data nasabah dalam rangka melayani nasabah secara lebih cepat, mudah dan sesuai dengan kebutuhan (*customer experience*) serta dapat dilakukan secara mandiri sepenuhnya oleh nasabah, dengan memperhatikan aspek pengamanan".

Adopsi perbankan digital di Indonesia dibuktikan dengan adanya berbagai layanan yang dapat memudahkan nasabah, antara lain: Pertama, adanya Internet Banking. Kedua, adanya Phone Banking. Ketiga, ada SMS

[2] Bank Indonesia, *Laporan Sistem Pembayaran dan Pengedaran Uang*, 2008.

Banking. Keempat, adanya Mobile Banking. Bank dapat bekerja sama dengan operator seluler, sehingga kartu SIM (kartu pintar seluler) *Global for Mobile Communication* (GSM) memiliki program khusus yang dipasang untuk memungkinkan transaksi perbankan. Proses transaksi nasabah di mobile banking akan lebih mudah dibandingkan SMS banking.

Peraturan OJK Nomor 12/POJK.03/2018 tentang Penyelenggaraan Layanan Perbankan Digital oleh Bank Umum menyebutkan bahwa bank yang mampu memberikan layanan perbankan digital diatur dalam Undang-Undang Nomor 10 Tahun 1998 tentang Bank dan Bank Umum Syariah. bahwa itu adalah bank komersial. Undang-Undang Nomor 21 Tahun 2008 tentang Perbankan Syariah. Perbedaan umum antara bank syariah dan bank tradisional adalah pengoperasian bank syariah berdasarkan prinsip syariah. Selain itu, dijelaskan bahwa bank dapat memberikan layanan perbankan digital sebagaimana dijelaskan dalam Pasal 2 POJK No. 12/POJK.03/2018. Ini menjelaskan hal berikut:

1. Bank dapat menyediakan layanan perbankan elektronik atau digital.
2. Bank yang menyediakan layanan perbankan elektronik atau digital wajib menerapkan prinsip-prinsip manajemen risiko dan kesehatan serta mematuhi ketentuan Peraturan Organisasi Jasa Keuangan ini.[3]

[3] Pasal 2 ayat (1) dan (2) Peraturan Otoritas Jasa Keuangan Nomor 12/POJK.03/2018 Tentang Penyelenggaraan Layanan Perbankan Digital Oleh Bank Umum.

Peraturan Otoritas Jasa Keuangan (OJK) nomor 12/POJK.03/2018 Tentang Penyelenggaraan Pelayanan Perbankan Digital oleh Bank Umum ini merupakan salah satu pendorong dan memperkuat lembaga perbankan bertransformasi atau membentuk sejak awal sebagai bank digital. Bank yang melakukan transformasi menjadi Bank Digital seperti Jenius milik Bank Tabungan Pensiunan Nasional (BTPN) bank digital yang beroperasi pertama kali di Indonesia pada tahun 2016. Disusul oleh Digibank (Bank DBS Indonesia), *Tyme* Digital (*Bank Commonwealth*), dan Wokee (Bank Bukopin) yang muncul tahun 2017. Tahun 2020 juga tercatat dua bank digital baru yaitu TMRW (UOB Indonesia) dan Nyala (OCBC NISP). Hingga pada tahun 2021 ini bank Digital baru dengan konsep membentuk sejak awal sebagai bank digital seperti Bank Digital BCA, Bank Jago dan Bank *Neo Commerce*.[4]

Bermunculannya bank digital yang telah beroperasi di Indonesia maka Otoritas Jasa Keuangan pada tanggal 30 Juli 2021 resmi merilis POJK Nomor 12/POJK.03/2021 tentang Bank Umum yang menjadi payung hukum legalnya Bank Digital di Indonesia dan mempertegas pengertian bank digital serta syarat-syarat untuk mendirikan bank digital.

Pengertian Bank Digital menurut POJK Nomor 12/POJK.03/2021 adalah Bank BHI (Berbadan Hukum Indonesia) yang menyediakan dan menjalankan kegiatan

[4]Chonnie Stephanie, *Daftar Bank Digital di Indonesia* (https://tekno.kompas.com/read/2021/04/22/10460097/daftar-bank-digital-di-indonesia?page=all) diakses tanggal 18 Oktober 2021 pukul 18:08 WIB.

usaha terutama melalui saluran elektronik tanpa kantor fisik selain KP (Kantor Pusat) atau menggunakan kantor fisik terbatas.[5]

Bank yang meningkatkan teknologi informasi dalam melayani nasabah secara tidak langsung membawa bank ke era baru yaitu era bank digital. [6] Era perbankan digital berorientasi pada layanan, jadi *fully* digital. Layanan digital bagi nasabah ini dapat diwujudkan dengan memulai hubungan bisnis antara nasabah dengan bank dengan membuka rekening, melakukan transaksi keuangan, dan menutup rekening menggunakan teknologi informasi. [7] Selain itu, jika bank digital menyediakan informasi dan transaksi non-perbankan lainnya, termasuk nasihat keuangan (financial *advice*), investasi, transaksi dengan sistem perdagangan elektronik (e-commerce), dan kebutuhan nasabah perbankan lainnya.

Mengembangkan strategi bisnis yang mengarah pada layanan perbankan digital membutuhkan infrastruktur yang tepat. Mendukung kenyamanan, keamanan, dan keandalan layanan perbankan digital dalam manajemen risiko, koordinasi TI, model bisnis, proses bisnis, pengendalian internal dan penyediaan informasi, komunikasi, pendaftaran, pembukaan rekening,

[5]Peraturan Otoritas Jasa Keuangan Nomor 12/POJK.03/2021 tentang Bank Umum.

[6]Catejan & Mbama, *Digital banking, customer experience and bank financial performance : UK customers perception*, International Journal of Bank Marketing, Vol. 36, No.2,2018. hlm. 230-255.

[7] Widi Aryo, Marlina, Asti & Bimo, , *Digitalisasi Bank Terhadap Peningkatan Pelayanan&Kepuasan Nasabah Bank*. Jurnal Ilmiah Inovator, Maret 2018. hlm.34.

pemrosesan transaksi, dan penutupan rekening. Termasuk sumber daya manusia.

Seiring dengan perkembangan teknologi, bank digital telah mewarnai aktivitas keuangan setiap nasabah. Layanan perbankan digital diharapkan dapat menghadirkan tingkat kenyamanan yang lebih tinggi dari layanan yang ada. Kenyamanan membuat nasabah merasa nyaman, namun di sisi lain layanan ini juga akan meningkatkan risiko yang dihadapi bank, terutama risiko operasional dan risiko reputasi jika terjadi masalah.[8]

Perbankan digital menimbulkan beberapa masalah, antara lain meningkatnya prevalensi kejahatan dunia maya dan berkembangnya teknik penyalahgunaan data oleh pihak-pihak yang tidak bertanggung jawab. Cybercrime telah menjadi kejahatan terbesar di industri perbankan, terutama di era digital.

Edwin Lim, Country Director Fortinet Indonesia, mengatakan transformasi digital sektor keuangan juga menjadi sangat rentan dalam hal keamanan siber. Faktanya, banyak kondisi yang dapat menyebabkan perusahaan kehilangan data dan menelan biaya sekitar $5,8 juta. Sepertiga dari transaksi yang dilakukan masuk ke ruang seluler, yang dapat terkena serangan *cyber*.[9] Senior Executive Analyst OJK Roberto Akyuwen juga mengatakan ada beberapa tantangan yang harus

[8] Kholis,N. Perbankan Dlam Era Baru Digital. Jurnal Economicus, Vol.9, (No.1), 2018. hlm.88.

[9] Yuni Astutik, *Awas Kejahatan Cyber Mengincar Sektor Keuangan* (https://www.cnbcindonesia.com/tech/20201116154457-37-202172/awas-kejahatan-cyber-mengincar-sektor-keuangan) diakses tanggal 18 Oktober 2021 pukul 18:15.

diperhatikan perbankan dalam melakukan transformasi digital seperti risiko perlindungan dan pertukaran data pribadi, risiko strategis investasi bidang IT dan risiko serangan siber.[10]

Pembatasan aktivitas masyarakat akibat pandemi Covid-19 yang telah terjadi ±2 tahun sejak tahun 2020 juga memberikan dampak pada meningkatnya tren penggunaan transaksi digital perbankan. Namun kondisi ini turut mendorong naiknya ancaman *cybercrime* di dunia perbankan, dari sisi nasabah maupun dari sisi bank seperti pencurian *database* bank, hingga pencurian ID dan password nasabah.

Contoh kasus pembobolan rekening digital dialami oleh salah satu nasabah PT Bank BTPN Tbk. yang menggunakan akun rekening Jenius. Perampokan dimulai pada 7 September dengan panggilan telepon dari penipu yang menyamar sebagai *call center* Genius. Menurut isi panggilan tersebut, ada pembaruan sistem dan perubahan kartu ATM. Korban memberikan informasi pribadi. Dalam hitungan menit, pelaku menyedot uang korban dan mengirimkannya ke rekening lain. Akun ini juga seorang jenius bernama Lutfi Putri Mardiana. Setelah dakwaan, diketahui bahwa pemilik akun tinggal di Lampung dan mengakui bahwa akunnya telah diretas oleh orang asing.

[10] Aldo Fernando, CNBC Indonesia, *Hati-hati! Ini Risiko Mengintai Bank Digital di Masa Depan* (https://www.cnbcindonesia.com/market/20211103113315-17-288645/hati-hati-ini-risiko-mengintai-bank-digital-di-masa-depan/2) diakses tanggal 3 Desember 2021, pukul 14.05.

Pada hari yang sama, uang yang dicuri dari rekening Jenius milik Anggita dialihkan ke dua rekening lainnya. [11]

Sektor keuangan 300 kali lebih rentan terhadap ancaman siber dibandingkan sektor lainnya. Hal ini menggambarkan kecenderungan bank digital untuk memperkuat diri dengan keamanan siber terpercaya untuk keamanan nasabah maupun bank digital. Hal ini menimbulkan pertanyaan apakah Pemerintah sudah memasukkan/mengcover di dalam peraturan perundang-undangan perihal perlindungan hukum terkait *Cyber Security* atau keamanan siber atas ancaman *cybercrime*. Mengingat bahwa saat ini pemerintah sedang gencar-gencarnya mensosialisasikan bahkan telah menerbitkan peraturan melalui Peraturan-peraturan OJK sejak tahun 2018 untuk percepatan digitalisasi perbankan, bahkan Pemerintah telah membuat *roadmap* pengembangan perbankan Indonesia tahun 2020-2025 yang tujuan akhirnya adalah migrasinya dari bank konvensional menuju bank digital.

Kebijakan yang dibuat oleh Pemerintah terkait digitalisasi perbankan memang akan membawa dampak positif terhadap kemajuan perbankan di Indonesia, namun Kebijakan/Peraturan pemerintah harus mempertimbangkan kemaslahatan bukan hanya dari sisi kelembagaan (bank) tetapi juga dari sisi Nasabah.

[11] M. Richard, *Ada Pembobolan Rekening Digital, Ini kata BTPN Soal Keamanan Akun Jenius* (https://finansial.bisnis.com/read/20200921/90/1294614/ada-pembobolan-rekening-digital-ini-kata-btpn-soal-keamanan-akun-jenius-indonesia) diakses tanggal 2 November 2021 pukul 12:10 WIB).

Sebagaimana Kaidah (Aturan) Fiqh yang yang erat kaitannya tentang Pemerintah yang berbunyi :

“Tindakan atau kebijakan seorang pemimpin terhadap orang-orang yang dipimpinnya harus dikaitkan dengan kemaslahatan. Sehingga kebijakan-kebijakan yang dikeluarkan oleh pemerintah selalu berorientasi terhadap perbaikan seluruh rakyatnya, mengingat tindakan dan kebijakan yang ditempuh dan diambil oleh seorang pemimpin atau penguasa harus sejalan dengan kepentingan bersama dan bukan untuk kepentingan golongan tertentu saja atau bahkan untuk kepentingan diri pribadinya”.[12]

Secara umum dari sisi Hukum Ekonomi Syariah, Muamalah pada dasarnya diperbolehkan. Jika ditinjau dari aspek Ekonomi Syariah, maka bank merupakan pihak yang diberikan amanah yang berkewajiban menjaga keamanan data maupun dana dari masyarakat. Sebagaimana dalam penggalan salah satu firman Allah SWT dalam Qur’an Surah Al-Baqarah/2: 283.

فَاِنْ اَمِنَ الَّذِى فَلْيُؤَدِّ بَعْضًا بَعْضُكُمْ اللّٰهَ وَلْيَتَّقِ اَمَانَتَهٗ اؤْتُمِنَ رَبَّهٗ

“.....jika sebagian kamu mempercayai sebagian yang lain, maka hendaklah yang dipercayai itu menunaikan amanatnya dan hendaklah ia bertakwa kepada Allah”.[13]

Dari ayat di atas dapat dipahami bahwa bank sebagai penerima amanat yang diberikan oleh masyarakat

[12] Abdul Mujib, Kaidah-Kaidah ‘Ilmu Fiqh, (Jakarta: Kalam Mulia, 2005), hlm 61.

[13] Kementerian Agama Republik Indonesia, *Quran Kemenag, (https://quran.kemenag.go.id/surah/2/283)* diakses tanggal 21 November 2021 Pukul 13.00.

(nasabah) harus menjaga data maupun dana masyarakat. Namun bagaimana jika ancaman *cybercrime* terjadi pada Bank Digital syariah. Dikarenakan mengutip dari laman Republika yang dirilis Februari 2022 bahwa saat ini Indonesia sudah mempunyai dua bank digital syariah yang benar-benar *fully* digital berbasis syariah yaitu PT Bank ALADIN Syariah Tbk. dan Jago Syariah yang merupakan Unit Usaha Syariah Bank Jago.[14] Apakah praktik *cybersecurity* pada bank Digital telah dikaji oleh DSN-MUI, mengingat Fatwa MUI tentang mekanisme pelaksanaan Bank Digital Syariah belum terbit saat munculnya Bank Digital Syariah.

Hal ini kembali menimbulkan pertanyaan apakah pada sistem perbankan Nasional dalam hal ini pemerintah dan pada sistem perbankan syariah sudah menyiapkan aturan akan keamanan siber (*Cyber Security*) terhadap ancaman dan serangan *cybercrime* pada Bank Digital.

[14] Nidia Zuraya, *Bagaimana Agar Bank Digital Syariah lebih Bisa Bersaing ? (*https://www.google.com/amp/s/m.republika.co.id/amp/r7rdzs383) diakses tanggal 11 April 2022, pukul 19:33.

BAB II
DESKRIPSI UMUM

A. Definisi Istilah

1. Cyber Security

Cyber security atau keamanan siber merupakan praktik untuk melindungi sistem, jaringan, program, data dan informasi dari ancaman atau serangan digital. Keamanan siber (*cybersecurity*) didefinisikan sebagai terjaganya kerahasiaan, keutuhan dan ketersediaan informasi dan/atau sistem informasi melalui media siber. Keamanan siber meliputi pula hal-hal antara lain keaslian (*authenticity*), akuntabilitas, non-penyangkalan (*non-repudiation*), dan keandalan.[15]

Cyber Security yang dimaksud dalam penelitian ini adalah upaya upaya perlindungan dan keamanan yang dilakukan mulai dari awal pendaftaran pembukaan rekening digital, saat bertransaksi maupun klausul-klausul terkait keamanan/*security* yang tercantum pada syarat dan ketentuan.

[15] Definisi cyber security berdasarkan FSB Cyber Lexicon (https://www.fsb.org/wp-content/uploads/P121118- 1.pdf). Diadaptasi dari International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27032:2012 – Guidelines for cybersecurity.

2. Bank Digital

Bank Digital menurut Peraturan OJK No. 12 /POJK.03 / 2021. Bab I Ketentuan Umum Pasal 1, ialah bank yang berbadan hukum Indonesia (BHI) yang menyediakan dan menjalankan kegiatan usaha terutama melalui saluran elektronik tanpa kantor fisik selain kantor pusat atau menggunakan kantor fisik terbatas. Bank bisa merupakan bank baru maupun bank lama yang bertransformasi menjadi bank digital.[16] Bank Digital yang dimaksud dalam penelitian ini mengambil sampel pada Bank Digital berbasis syariah yaitu PT. Bank Aladin Syariah Tbk.

3. Hukum Positif Indonesia

Hukum positif Indonesia adalah hukum yang saat ini berlaku baik tertulis maupun tidak tertulis, yang merupakan campuran dari sistem hukum Eropa, hukum agama dan hukum adat.[17] Hukum positif yang dimaksud dalam penelitian mengacu pada Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen dan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE).

[16] Peraturan Otoritas Jasa Keuangan Nomor 12 /POJK.03/ 2021 tentang Bank Umum

[17] Awinitya Paresti, *Pengaruh Hukum Masa Kolonial Terhadap Hukum Positif Indonesia*, UNAIR.

4. Hukum Ekonomi Syariah

Hukum Ekonomi syariah adalah hukum yang menjadi landasan pemikiran dan penentuan konsep ekonomi dalam Islam yang sumbernya dapat diambil dari Alquran, Hadits, Ijtihad maupun Kaidah Fiqh.[18]

B. Bank Digital

1. Pengertian Bank

Kata bank berasal dari bahasa Italia *banca* berarti tempat penukaran uang. Pengertian bank menurut Kamus Besar Bahasa Indonesia adalah badan usaha di bidang keuangan yang menarik dan mengeluarkan uang dalam masyarkat, terutama memberikan kredit dan jasa dalam lalu lintas pembayaran dan peredaran uang.[19]

Kasmir dalam bukunya Analisis laporan Keuangan mengartikan bank yaitu: "Bank adalah perusahaan yang bergerak dalam bidang keuangan, artinya aktivitas perbankan selalu berkaitan dalam bidang keuangan. Dimana kegiatan utamanya adalah menghimpun dana dari masyarakat dan menyalurkannya kembali dana tersebut ke masyarakat serta memberikan jasa bank lainnya".[20]

---

[18] Tim Dosen STAINU Tangerang, Modul Mata Kuliah Hukum Ekonomi Syariah, (PSP Nusantara : 2018) H 11.

[19] Kamus Besar Bahasa Indonesia (KBBI) Daring.

[20] Kasmir, Analisis Laporan Keuangan., Jakarta : PT. Raja Grafindo Persada, 2012.

Sedangkan menurut Undang-Undang (UU) Republik Indonesia Nomor 10 Tahun 1998 tentang Perbankan: "Bank adalah badan usaha yang menghimpun dana dari masyarakat dalam bentuk simpanan dan menyalurkannya kepada masyarakat dalam bentuk kredit dan/atau bentuk-bentuk lainnya dalam rangka meningkatkan taraf hidup rakyat banyak".[21]

Dari definisi di atas dapat disimpulkan bahwa Bank adalah organisasi komersial di bidang keuangan yang kegiatan utamanya adalah menghimpun dana masyarakat (*finance*), menyalurkannya dalam bentuk pinjaman (kredit) dan memberikan jasa pelayanan keuangan kepada masyarakat.

Perbankan adalah segala sesuatu yang menyangkut tentang Bank, mencakup kelembagaan, kegiatan usaha, serta cara dan proses melaksanakan usahanya. Perbankan Indonesia dalam menjalankan fungsinya berasaskan demokrasi ekonomi dan menggunakan prinsip kehati-hatian. Fungsi utama perbankan Indonesia adalah sebagai penghimpun dan penyalur dana masyarakat serta bertujuan untuk menunjang pelaksanaan pembangunan nasional dalam rangka meningkatkan pemerataan pembangunan dan hasil-hasilnya, pertumbuhan ekonomi dan stabilitas nasional, kearah peningkatan taraf

[21] Undang-Undang No. 10 Tahun 1998 tentang Perbankan

hidup rakyat banyak. Perbankan memiliki kedudukan yang strategis, yakni sebagai penunjang kelancaran sistem pembayaran, pelaksanaan kebijakan moneter dan pencapaian stabilitas sistem keuangan, sehingga diperlukan perbankan yang sehat, transparan dan dapat dipertanggungjawabkan.

2. Fungsi dan Tujuan

Bank sebagai lembaga keuangan memiliki fungsi utama yaitu sebagai penghimpun dana dalam bentuk pinjaman. Tetapi sebenarnya fungsi bank dapat dijelaskan dengan lebih spesifik seperti yang diungkapkan oleh Y. Sri Susilo, Sigit Triandaru, dan A. Totok Budi Santoso, yaitu sebagai berikut :[22]

a. *Agent of Trust*

Dasar utama kegiatan perbankan adalah kepercayaan (*trust*), baik dalam hal penghimpunan dana maupun penyaluran dana. Masyarakat percaya bahwa uangnya tidak akan disalahgunakan oleh bank, dan pihak bank percaya bahwa pihak debitur tidak akan menyalahgunakan pinjamannya

b. *Agent of Development*

Kegiatan perekonomian masyarakat di sektor moneter dan di sektor rill tidak dapat dipisahkan. Kedua sektor tersebut selalu

[22] Y. Sri Susilo, Sigit Triandaru, dan A. Totok Budi Santoso, *Bank dan Lembaga Keuangan Lain*" (Yogyakarta: Salemba Empat, 2006). hlm.36.

berinteraksi dan saling mempengaruhi. Sektor riil tidak akan dapat bekerja dengan baik apabila sektor moneter tidak bekerja dengan baik. Kegiatan bank berupa penghimpunan dan penyaluran dana sangat diperlukan bagi kelancaran kegiatan perekonomian di sektor riil.

c. *Agent of Service*
   Selain menghimpun dan menyalurkan dana, bank juga memberikan penawaran jasa-jasa perbankan yang lain kepada masyarakat. Jasa yang ditawarkan bank ini erat kaitannya dengan kegiatan perekonomian masyarakat. Jasa ini antara lain dapat berupa jasa transfer, *safe deposit box* (penitipan barang berharga), garansi bank, dan penyelesaian tagihan.

Menurut uraian Undang-Undang Perbankan No. 10 Tahun 1998, bank memiliki dua fungsi:

a. Pengumpul Dana Masyarakat dapat berupa deposito (deposito berjangka), giro, tabungan, dan lain-lain.
b. Menyalurkan Dana Masyarakat dapat disalurkan dalam bentuk pinjaman (kredit), atau yang dipersamakan dengan itu.

Menurut Kasmir Tugas Bank Umum adalah sebagai berikut:[23]

[23] Kasmir. *Analisis Laporan Keuangan*. (Jakarta: PT. Raja Grafindo Persada, 2012). hlm. 49

a. Bertindak sebagai perantara kredit sebagai peminjam atau dalam bentuk dana titipan masyarakat seperti tabungan, giro, dan deposito berjangka.

b. Sebagai badan yang memiliki tugas mengedarkan uang baik uang giral maupun uang kartal.
c. Pembiayaan sebagai perantara, yaitu perantara pihak yang kelebihan dana dengan pihak yang membutuhkan dana.

Tujuan utama bank adalah untuk mengunjungi pelaksanaan pembangunan nasional, meningkatkan keadilan, pertumbuhan ekonomi, stabilitas nasional dan meningkatkan kesejahteraan rakyat secara keseluruhan.

3. Kegiatan - Kegiatan Bank

Bank dibagi menjadi dua bidang kegiatan: Bank Umum dan Bank Perkreditan Rakyat. Bank umum lebih komprehensif daripada bank perkreditan rakyat. Ini berarti bahwa bank umum menawarkan lebih banyak variasi produk, karena bank umum bebas menentukan produk dan jasanya. Sedangkan bank perkreditan rakyat memiliki batasan tertentu, yang mempersempit aktivitasnya, tetapi menurut Kasmir, aktivitas perbankan dikategorikan sebagai berikut:[24]

[24] "*Bank dan Lembaga Keuangan Lainnya*" (Jakarta: Raja Grafindo Persada 2012). hlm.43.

a. Kegiatan Bank Umum

1) Menghimpun dana dari masyarakat (*funding*) dalam bentuk : Simpanan Giro (*Demand Deposit*), Simpanan Tabungan (*Saving Deposit*), Simpanan Deposito (*Time Deposit*) .

2) Menyalurkan dana ke masyarakat (*lending*) dalam bentuk : Kredit Investasi, Kredit Modal Kerja, Kredit Perdagangan

3) Memberikan jasa - jasa bank lainnya (*services)* dalam bentuk : Transfer (kiriman uang), Inkaso (*collection*), Kliring, *Safe Deposit Box*, Bank Card, Bank Note (valas), Bank Garansi, Referensi Bank, Bank Draft Letter of Credit (L/C), Cek Wisata (*Traveller's Cheque*), Jual beli surat berharga, Menerima setoran - setoran seperti : Pembayaran pajak, pembayaran telepon, pembayaran air, pembayaran listrik, dan pembayaran uang kuliah, Pembayaran - Pembayaran seperti : gaji/pensiunan/honorarium, pembayaran dividen, pembayaran kupon, pembayaran bonus/hadiah. Dalam pasar modal perbankan dapat memberikan atau menjadi : penjamin emisi (*underwriter*), penjamin (guarantor), wali amanat (*trustee*), perantara perdagangan efek (pialang/broker)

b. Kegiatan Bank Perkreditan Rakyat (BPD)

1) Penghimpunan dana dalam bentuk: Tabungan, Deposito Berjangka dan Giro.

2) Penyaluran dana dalam bentuk: kredit investasi, kredit modal kerja dan kredit usaha.

3) Hal-hal yang dilarang bagi Bank Perkreditan Rakyat adalah sebagai berikut: Menerima giro, kliring, melakukan transaksi valuta asing, serta melakukan transaksi asuransi.

4. Jenis–jenis Bank

Dalam perbankan Indonesia saat ini, terdapat beberapa jenis bank yang diatur oleh Undang-Undang Perbankan. Namun kegiatan pokok dan kegiatan pokok bank sebagai lembaga keuangan yang menghimpun dan menyalurkan dana masyarakat tidak berbeda satu sama lain. Menurut Lukman Dendawijaya, jenis bank dapat dilihat dari beberapa aspek, yaitu:

a. Dari segi Fungsi menurut Undang Undang No.10 tahun 1998 tentang Perbankan, yaitu sebagai berikut :

1) Bank Umum, yaitu bank yang melaksanakan kegiatan usaha secara umum (konvensional) dan/atau berdasarkan prinsip syariah serta menyediakan jasa transaksi pembayaran sebagai bagian dari usahanya.

2) Bank Perkreditan Rakyat (BPR), Artinya, bank yang beroperasi secara konvensional atau syariah dan tidak menyediakan jasa perdagangan pembayaran dalam kegiatannya. Jadi di sini, aktivitas BPR jauh lebih sempit daripada aktivitas bank umum.

b. Dari segi kepemilikan, jenis bank berdasarkan struktur kepemilikannya dapat dibedakan sebagai berikut :

1) Bank milik negara (pemerintah), merupakan bank yang akte pendiriannya maupun modal bank ini sepenuhnya dimiliki oleh pemerintah, sehingga keuntungannya dimiliki oleh pemerintah pula. Contoh bank milik pemerintah adalah : Bank Mandiri, Bank Negara Indonesia (BNI), Bank Rakyat Indonesia (BRI) dan Bank Tabungan Negara (BTN).

2) Bank Milik Pemerintah Daerah (BUMD), Bank yang akte pendirian maupun modal bank sepenuhnya dimiliki oleh Pemerintah Daerah, sehingga keuntungan bank dimiliki oleh Pemerintah Daerah. Contoh bank milik pemerintah daerah antara lain : Bank DKI, Bank Jawa Barat,Bank DIY, Bank Riau, Bank Sulawesi

Selatan, Bank Nusa Tenggara Barat, Bank Kalsel, Bank KalTeng.

3) Bank milik swasta nasional, merupakan bank yang seluruh atau sebagian besar sahamnya dimiliki oleh swasta nasional, sehingga keuntungannya menjadi milik swasta pula. Contoh bank milik swasta nasional antara lain : Bank Central Asia (BCA), Bank Lippo, Bank Mega, Bank Danamon, Bank Internasional Indonesia (BII)

4) Bank milik koperasi, merupakan bank yang kepemilikan saham sahamnya oleh perusahaan yang berbadan hukum koperasi. Contoh bank milik koperasi adalah Bank Umum Koperasi Indonesia (Bukopin).

5) Bank milik asing, merupakan cabang dari bank yang ada di luar negeri, atau seluruh sahamnya dimiliki oleh pihak asing (luar negeri). Contoh bank milik asing antara lain: ABN AMRO Bank, American Express Bank, Bank of Tokyo, Bangkok Bank, Deutsche Bank.

6) Bank milik campuran, merupakan bank yang sahamnya dimiliki oleh pihak asing dan pihak swasta nasional dan secara mayoritas sahamnya dipegang oleh warga Negara Indonesia. Contoh bank campuran adalah: Bank

Finconesia, Bank Merincorp, Bank PDFCI, Bank Sakura Swadarma, Mitsubishi Buana Bank.

c. Dilihat dari Segi Status Jenis bank dilihat dari segi status adalah sebagai berikut :

1) Bank Devisa, merupakan bank yang dapat melaksanakan transaksi ke luar negeri atau yang berhubungan dengan mata uang asing secara keseluruhan, misalnya transfer ke luar negeri, inkaso ke luar negeri, *travellers cheque*, dan pembayaran L/C. Persyaratan untuk menjadi bank devisa ditentukan oleh Bank Indonesia.

2) Bank non Devisa Bank non devisa merupakan bank yang belum mempunyai izin untuk melaksanakan transaksi sebagai bank devisa, sehingga tidak dapat melaksanakan transaksi yang berhubungan dengan luar negeri.

d. Dilihat dari Segi Cara Menentukan Harga, bank dapat dibedakan dalam dua jenis :

1) Bank yang berdasarkan prinsip konvensional (Barat), Bank konvensional mendapatkan untung dengan menetapkan bunga sebagai harga dari rekening giro dan tabungan dan deposito berjangka. Harga kredit (*loan*) juga ditentukan berdasarkan suku bunga. Keputusan pendapatan

untuk layanan perbankan lainnya, di sisi lain, ditetapkan pada biaya nominal atau persentase tertentu.

2) Bank berdasarkan prinsip Syariah (Islam). Perbedaan utama antara bank konvensional dan bank syariah terletak pada landasan filosofis yang dianut. Bank syariah tidak memiliki sistem suku bunga, tetapi bank konvensional memilikinya. Di bank syariah, penetapan harga atau pengejaran keuntungan didasarkan pada: a) pinjaman bagi hasil (Mudharabah) b) pinjaman bagi hasil (Musyarakah) c) pinjaman peralatan modal di bawah sewa murni tanpa pilihan d) atau Opsi pengalihan kepemilikan barang disewa dari bank oleh pihak lain (ijarah waigtina) e) Prinsip jual beli barang dengan keuntungan (murabahah).[25]

Dilihat dari segi berdasarkan *Impact* dari Transformasi Industry 4.0 dan *impact* transformasi digital, Bank dibedakan menjadi dua, yaitu: Bank Tradisional dan Bank Digital.

[25] Lukman Dendawijaya, *Manajemen Perbankan*, (Jakarta : Ghalia Indonesia, 2009) hlm.16-18.

5. Bank Digital

a. Sejarah singkat Bank Digital

James menjelaskan bentuk-bentuk paling awal dari perbankan digital yaitu munculnya mesin dan kartu ATM yang diluncurkan pada tahun 1960-an. Ketika internet muncul pada 1980-an dengan broadband awal, jaringan digital mulai menghubungkan pengecer dengan pemasok dan konsumen untuk mengembangkan kebutuhan untuk mengembangkan kebutuhan untuk katalog online awal dan sistem perangkat lunak inventaris.

Sejarah dibuat di India pada saat munculnya teknologi internet. Perbankan digital terbentuk pada akhir 1990-an ketika ICICI Bank pertama kali menawarkan layanan ini kepada pelanggan ritel.

Perbankan digital menjadi arus utama pada tahun 1999 karena biaya Internet berkurang dan kesadaran dan kepercayaan akan Internet meningkat. Sebelumnya, Bank Sumitomo meluncurkan layanan perbankan online pertama pada Januari 1997. Financial Brand, salah satu penanda utama dalam transformasi perbankan digital, dilaporkan setelah pengenalan iPhone

yang diproduksi oleh Steve Jobs oleh *Apple Computer Inc*. pada tahun 2007. Dengan Apple iPhone, industri perbankan berubah pada saat yang sama. Tidak butuh waktu lama bagi para inovator untuk menemukan bahwa smartphone dapat membuat perbankan digital lebih menarik dan mudah diakses.[26]

Di tahun 2007-2009 di Amerika Serikat, Lehman Brother menyatakan masa itu adalah kebangkrutan dan memicu krisis perbankan yang disebabkan oleh monopoli pinjaman dan pengambilan risiko yang berlebihan oleh keuangan global.[27] Situasi krisis ini, Regulator (Pemerintah) AS membuka kompetisi perbankan yang lebih besar dengan memanfaatkan digitalisasi.

Di era ini, bank yang berorientasi pada pelayanan yang lebih baik, transparan, aman, lebih murah, dan dorongan kelincahannya pertumbuhan dan kesuksesan yang belum pernah terjadi sebelumnya. Inilah bagaimana

[26] Daniel Deha, Banking Everywhere: *Neobank dan Sejarah Bank Digital* (https://www.trenasia.com/banking-everywhere-neobank-dan-sejarah-bank-digital-part-3-habis-indonesia diakses tanggal 13 Juni 2022 Pukul 05.00 WITA).

[27] Wirianto Widjaja, *Digital Bank Trends and Regulations in Indonesia* disampaikan pada pertemuan Alumni Gathering MMSI 2022, Jakarta 19 Maret 2022.

beberapa bank digital muncul di seluruh dunia. B. Simple, Neobank AS yang berbasis di Portland, Oregon pada tahun 2009 (bank yang awalnya hanya memiliki ekosistem digital). Simple harus diakui sebagai neobank pertama di dunia. Simple harus diakui sebagai neobank pertama di dunia. "*Neobanks: creating a digital bank from scratch among the FinTech firms, some aspire to become banks and to provide a purely digital alternative to traditional institutions*".[28] Tujuan pendiriannya adalah untuk menciptakan kolaborasi yang lancar dengan konsumen.

Bank digital terus bermunculan di tahun yang sama, termasuk Ally Bank di Amerika Serikat yang berkantor pusat di Detroit, Michigan. Kemudian, pada tahun 2010, Meven, sebuah bank digital di Amerika Serikat, muncul dan sekarang sudah ada ratusan di seluruh dunia hingga masuk ke Indonesia.

b. Definisi Bank Digital

Menurut POJK No.12/POJK.03/ 2021, bank digital adalah bank berbadan hukum Indonesia (BHI) yang

[28] BBVA Research, *Digital Economy Outlook*: January 2017. (https://www.bbvaresearch.com/wpcontent/uploads/2016/01/DEO_Jan16.pdf)

menyediakan dan menjalankan kegiatan usaha terutama melalui saluran elektronik tanpa kantor fisik selain kantor pusat atau menggunakan kantor fisik terbatas. Bank bisa merupakan bank baru maupun bank lama yang bertransformasi menjadi bank digital. Selanjutnya dalam Bab IV tentang Bank Digital, dijelaskan semua bank BHI dapat beroperasi sebagai bank digital. Bank yang memilih model bisnis *fully digital* bank tetap diwajibkan memiliki minimal satu kantor fisik berupa kantor pusat dan memenuhi persyaratan operasional sebagai bank digital.[29]

Dalam paper diskusi digital bank untuk India mendefinisikan "Bank Digital" berarti Bank dalam Perbankan Regulasi Act, 1949 (B R Act). Dengan kata lain, entitas ini akan menerbitkan deposito, membuat pinjaman dan menawarkan rangkaian layanan lengkap. Seperti namanya Bank Digital pada prinsipnya akan bergantung pada internet dan saluran terdekat lainnya, untuk menawarkan layanan mereka dan bukan cabang fisik. *"Digital Banks" or DBs referred in this Paper means Banks as defined in the Banking Regulation Act, 1949 (B R Act). In other words, these*

[29] Peraturan Otoritas Jasa Keuangan nomor 12/POJK.03/2021 tentang Bank Umum

entities will issue deposits, make loans and offer the full suite of services that the B R Act empowers them to. As the name suggests however, DBs will principally rely on the internet and other proximate channels to offer their services and not physical branches.[30]

Menurut Chris bank digital melacak inovasi dalam perbankan dan bagaimana internet seluler mengubah dinamika hubungan konsumen dan perusahaan dengan bank mereka. Alasan perbankan digital lebih dari sekadar platform seluler atau online adalah karena ia menyertakan solusi *middleware*. *Middleware* adalah perangkat lunak yang menjembatani sistem operasi atau basis data dengan aplikasi lain.[31]

Ada tiga faktor utama dalam agenda transformasi perbankan digital : Pertama, secara perlahan tumpukan kertas akan ditinggalkan sebagai proses utama perbankan dan mengadopsi cara-cara baru

[30] Niti Aayog, *Digital Banks A Proposal for Licensing & Regulatory Regime for India*, Discussion Paper, November 2021, page. 12

[31] Razatul Janna, *Faktor-Faktor Yang Mempengaruhi Nasabah Dalam Menggunakan Layanan Digital Banking Dengan Menggunakan Model Unified Theory Of Acceptance And Use Of Technology (UTAUT) pada PT. Bank Syariah mandiri cabang banda aceh*, 2019

yang lebih cerdas, yang dulunya melakukan transaksi yang menghabiskan banyak kertas kini transformasi digital akan merubah pola kerja bank yang lebih simple dan mudah. Kedua, perbankan perlu memperhatikan keinginan dari diri nasabah dan mengubah pengalaman nasabah agar menjadi lebih dari otomasi. Ketiga, menanamkan budaya baru dalam perusahaan.[32]

c. Regulasi Bank Digital di Indonesia

Regulasi yang berhubungan terhadap Bank Digital di Indonesia yaitu sebagai berikut:

1. Peraturan Otoritas Jasa Keuangan Republik Indonesia Nomor 12 /POJK.03/2021 Tentang Bank Umum
2. Peraturan Otoritas Jasa Keuangan Nomor 12 /POJK.03/2018 Tentang Penyelenggaraan Layanan Perbankan Digital Oleh Bank Umum

[32] Aulia Febriana. *Pengaruh Penggunaan Modul Pada Model Pembelajaran Kooperatif Tipe Student Team Achievement Divisions terhadap Hasil Belajar Siswa Pada Mata Pelajaran Keterampilan Komputer dan Pengelolaan Informasi di SMK Negeri 2 Bukittinggi*. Jurnal, Program Studi Pendidikan teknik Informatika, Fakultas Teknik: Universitas negeri Padang, 2014.

d. Perbedaan Bank Tradisional dengan Bank Digital

Perbedaan Bank Tradisional dengan Bank Digital dapat dilihat dalam tabel berikut:

Aspek	Bank Tradisional	Bank Digital
Jam Layanan	Terbatas	Sepanjang Waktu
Kecepatan Layanan	Tergantung kualifikasi dan pengalaman pegawai bank	Segera
Saluran Layanan	Fleksibel tetapi terbatas	Fleksibel dengan lebih banyak pilihan
Biaya Pemeliharaan	Tinggi, tergantung keseringan diberikan layanan	Rendah, sebagian besar layanan gratis
Cakupan Layanan	Terbatas tergantung pada jenis layanan	Tidak terbatas, diluar geografis dan batas lokasi
Status Operator	Dilakukan oleh pegawai bank	Dilaukan oleh klien bank
Pembelajaran dan sifat promosi	Relatif membutuhkan lebih banyak waktu dan biaya	Dapat dilakukan dengan cepat melalui pemberitahuan SMS/Email

Biaya	Staf dan aset fisik pemeliharaan	Server dan paket perangkat lunak
Orientasi Bisnis	Produk dan Layanan	Kebutuhan Pelanggan

(Sumber : Data *Digital Bank Trends and Regulations in Indonesia)*

e. Perbedaan Bank Digital dengan Layanan *Digital Banking*

Aspek	Layanan *Digital Banking*	Bank Digital
Istilah/ Pengertian	Layanan perbankan yang bisa dilakukan nasabah melalui daring seperti *mobile banking* dan *internet banking*	suatu produk dari sebuah instansi bank konvensional yang mengeluarkan layanan perbankan dalam bentuk aplikasi
Kantor Fisik	bank konvensional yang menyediakan *digital banking* masih mempunyai banyak kantor fisik.	mempunyai kantor fisik dengan jumlah sangat terbatas bahkan boleh tidak sama sekali

Produk dan Layanan	bagian dari layanan atau fasilitas tambahan bank konvensional (nasabah tidak dapat menggunakannya jika tidak mempunyai rekening di bank tersebut)	satu produk atau lembaga keuangan tersendiri
Cakupan Layanan	Online tapi terbatas dan tetap harus datang ke kantor fisik, seperti verifikasi identitas, penggantian kartu ATM, pendaftaran/pembuatan kartu kredit, dan lain-lain	Semuanya online mulai dari pendaftaran, pembukaan rekening, pemrosesan transaksi, dan penutupan rekening serta kartu debit yang berbentuk digital.
Segmentasi Pasar	segmentasi nasabah yang lebih luas mulai dari *payroll, mass, emerging affluent, premier* bahkan *private* dengan kebutuhan dan karakteristik yang berbeda bagi setiap segmentasi	Segmen pasar bank digital juga lebih luas dibandingkan bank konvensional, terlebih karena

		menyasar generasi milenilal. Mulai dari registrasi nasabah, transaksi, bahkan pengisian saldo dapat dilakukan dari jarak jauh
Biaya	potongan atau biaya administrasi bulanan flat bahkan besar setiap bulan	potongan atau biaya administrasi bulanan murah bahkan gratis

(Sumber : Data Diolah oleh Penulis)

f. Manfaat Bank Digital

Manfaat digitalisasi bank dapat dikemukakan sebagai berikut:

1) Menurunkan biaya operasional, digitalisasi perbankan merupakan investasi jangka panjang. Pihak perbankan dapat menjangkau pasar lebih luas dengan menurunkan anggaran investasi pembukaan cabang

pembantu dan kantor kas kecil.[33]

2) Transformasi perbankan digital, ketika teknologi sudah memenuhi sistem keuangan yang akan menghemat waktu.[34]

3) Proses sederhana, nyaman digunakan tanpa harus pergi ke kantor cabang. Nasabah dapat membuka akun dalam waktu kurang dari 10 menit dan antarmuka pengguna aplikasi membuat navigasi menjadi cepat dan sederhana.

4) *Anywhere, anytime is a new way of busy lives neobanks tap into. Thus, they are all pro the utmost comfort of a customer and offer 24✕7 access to banking services*. Dapat diakses dimana saja dan kapan saja yang mengutamakan aspek kenyamanan maksimal untuk nasabah, dan menawarkan akses 24x7 dalam layanan perbankan.[35]

---

[33] Marlina Asti, Bimo.Widhi Aryo. *Digitalisasi Bank Terhadap Peningkatan Pelayanan Dan Kepuasan Nasabah Bank*. Jurnal Ilmiah Inovator Edisi Maret 2018.

[34] Quesada, V. *When Tech Meets Finance: A Roadmap for Digital Banking Transformation. Massachusetts: CreateSpace Independent Publishing Platform*. Edisis kedua, 2017.

[35] Hopkinson, G., Klarova, D., Turcan, R. V., & Gulieva, V. *How Neobanks' Business Models challenge Traditional Banks. International Business Centre at Aalborg University*, August, 3, 2019.

5) Tersedia reward hingga promo, yang berupa cashback, poin yang bisa ditukarkan dengan voucher diskon, penawaran suku bunga yang lebih besar.

g. Tantangan Bank Digital

Menurut catatan OJK, ada beberapa tantangan bagi upaya transformasi digital perbankan ke depan, yaitu sebagai berikut:

1) Risiko penyalahgunaan teknologi kecerdasan buatan (*artificial intelligence*). Di sektor perbankan, kecerdasan buatan telah digunakan di beberapa bidang, termasuk otomatisasi beberapa tugas (deteksi penipuan/*fraud*, transaksi pencucian uang, atau mesin pengambilan keputusan dalam proses aplikasi kartu kredit). Risiko yang diidentifikasi di bidang kecerdasan buatan termasuk bias algoritmik, deepfake, dan kemampuan untuk menentukan keputusan sendiri.

2) Perlindungan data pribadi dan risiko kehilangan data pelanggan. Menurut OJK, perlindungan data pribadi nasabah akan berdampak signifikan terhadap perkembangan layanan perbankan digital ke depan. Dalam

hal ini, proteksi menjadi faktor penting bagi kepercayaan online dan penting untuk transaksi digital. Untuk alasan ini, ancaman-ancaman yang timbul dari lemahnya perlindungan data pribadi nasabah tersebut akan sangat berdampak pada perkembangan layanan perbankan digital. Belum tersedianya payung hukum yang mengatur terkait perlindungan data pribadi menjadi alasan utama mengapa perusahaan lokal belum selaras dengan aturan perlindungan data.

3) Literasi keuangan masih rendah. Menurut OJK, tingkat literasi keuangan digital konsumen bank yang rendah bisa menjadi salah satu faktor pemicu kejahatan siber. Berdasarkan data Direktorat Tindak Pidana Siber Bareskrim Polri yang disitir OJK, terdapat 2.259 laporan masyarakat tentang kejahatan digital pada Januari-September 2020. Sebanyak 18 aduan di antaranya tentang peretasan sistem elektronik, 649 penipuan daring, 39 pencurian data atau identitas, dan 71 manipulasi data (CISSREc, 2020). Berdasarkan laporan tersebut terlihat bahwa penipuan daring menjadi aduan

tertinggi dan hal ini menunjukkan rendahnya pemahaman masyarakat atas risiko transaksi digital.

4) Risiko ancaman siber (*cyber crime*). Ancaman siber merupakan salah satu ancaman yang perlu diwaspadai di era industri 4.0 ini. Data dari Pusat Operasi Keamanan Siber Nasional BSSN yang disitir OJK menunjukkan bahwa sepanjang tahun 2020 terjadi 495 juta serangan siber atau naik 5 kali lipat dibanding tahun sebelumnya sejumlah 228 juta serangan siber.[36] Sehingga hal inilah yang menyebabkan pada Bank Digital penting adanya *cybersecurity*.

C. Cyber Security

1. Sejarah singkat *Cyber Security*

Dalam 20 tahun abad ke-21, awalan "cyber" ditambahkan ke istilah-istilah seperti "cyberculture," "cybersex," dan "cyberwar." Semua ini berhubungan dengan bidang media digital, virtual reality dan internet. Sejak munculnya internet, kata "*network*" telah menjadi metafora menonjol dan telah mengambil perhatian

[36] Aldo Fernando, CNBC Indonesia, *Hati-hati! Ini Risiko Mengintai Bank Digital di Masa Depan* (https://www.cnbcindonesia .com/market/20211103113315-17-288645/hati-hati-ini-risiko-mengintai-bank-digital-di-masa-depan diakses tanggal 13 Juni pukul 10:00WITA)

di hampir setiap disiplin ilmu kontemporer dan institusi besar. Seperti pada tahun 1948, prefix "*cyber*" ditemukan dalam istilah "*cybernetics*" yang digambarkan sebagai "studi tentang pesan sebagai sarana yang mengendalikan mesin dan masyarakat". Namun, pada dasarnya, tujuan *cybernetics* adalah untuk mengembangkan bahasa dan teknik menyerang terkait dengan masalah kontrol dan komunikasi pada umumnya dan kemudian menjadi dasar untuk komputasi setelah Perang Dunia II. Seperti halnya istilah "*cyber*", istilah "*network*" sejak pertengahan abad kedua puluh juga telah ada, dan dalam era globalisasi di mana orang yang terhubung satu sama lain melalui infrastruktur transportasi dan komunikasi, jaringan atau jaringan adalah realitas fisik dan metaforis**.**[37]

Kata jaringan banyak digunakan untuk menggambarkan realitas media baru. Konsep media baru sendiri awalnya diperkenalkan dalam novel fiksi ilmiah True Name karya Vernor, seorang novelis dan matematikawan 1981. Vernor menggunakan istilah "The Other Plane" untuk menggambarkan keberadaan sebuah jaringan. Selanjutnya, konsep dimensi lain dipopulerkan oleh William Gibson pada tahun 1984 dalam novelnya Neuromancer, yang muncul dengan ide setelah mengamati fenomena kepercayaan yang

[37] Patrick Jagoda,*"Speculative Security", Dalam Reveron, Derek S., Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, (Washington, DC: Georgetown University Press, 2012), hlm. 22.

muncul pada anak-anak setelah bermain video game. Anak-anak percaya bahwa permainan itu nyata dan bahwa semua bangunan, ruang, interaksi, dan objek dalam permainan itu nyata atau ada; bahkan jika mereka tidak dapat mencapainya. [38]

Sementara itu, sejarah keamanan siber sebagai konsep keamanan berawal dari disiplin ilmu komputer dan ilmu informasi, di mana keamanan siber pertama kali digunakan dalam *Computer Council Report and Telecommunications* (CSTB) pada tahun 1991, di mana keamanan di era informasi. dalam istilah "Keamanan" didefinisikan sebagai tindakan perlindungan terhadap pengungkapan yang tidak disengaja, modifikasi atau korupsi data dalam sistem dan juga untuk keamanan sistem itu sendiri. Dalam hal ini, ancaman dalam keamanan siber tidak hanya disebabkan oleh beberapa aktor atau agen, tetapi Nissenbaum menunjukkan bahwa sebagian besar ilmuwan komputer mengadopsi wacana teknis yang berfokus pada pengembangan program yang baik dengan beberapa bug dan sistem yang sulit ditembus oleh penyerang luar. , dengan demikian "keamanan komputer matic" beralih ke "keamanan siber" di mana keamanan jaringan dapat dianggap sebagai "keamanan

[38] Rulli Nasrullah, *Teori dan Riset Media Siber (Cybermedia*), (Jakarta: Prenada Media Group, 2014). hlm. 17-18.

komputer" dan "keamanan". ".[39] Keamanan (*security*) secara umum dapat diartikan sebagai kemampuan mempertahan diri (*survival*) dalam menghadapi ancaman yang nyata (*existential threat*).[40]

Kemudian konsep cyber security berkembang, dimana menurut Saco dan Deibert, ancaman *cyber security* juga telah merambah batas negara sehingga menjadi ancaman internasional. Hal ini disebabkan semakin banyaknya interaksi publik di dunia maya akibat kemajuan teknologi dan era informasi.

2. finisi Cyber Security

Cyber security atau keamanan siber merupakan praktik untuk melindungi sistem, jaringan, program, data dan informasi dari ancaman atau serangan digital. Keamanan siber (*cybersecurity*) didefinisikan sebagai menjaga kerahasiaan, integritas, dan ketersediaan informasi dan/atau sistem informasi melalui media jaringan. Keamanan siber juga mencakup isu-isu seperti

[39] Lene Hansen and Helen Nissenbaum, "*Digital Disaster, Cyber Security, and the Copenhagen School*", International Studies Quarterly, Vol. 53, No. 4, 2009. Hlm. 1160.

[40] Dewi Triwahyuni, *Security Pengertian Dasar&Jenisnya* disampaikan pada paparan mata kuliah studi Keamanan Internasional, 2017.

keaslian, akuntabilitas, non-penyangkalan, dan keandalan.[41]

Cybersecurity adalah kumpulan alat keamanan, kebijakan, konsep, tindakan keamanan, pedoman, pendekatan manajemen risiko, tindakan, pelatihan, praktik terbaik, jaminan, dan alat. Teknologi dapat digunakan untuk melindungi lingkungan jaringan dan aset organisasi dan pengguna. Organisasi mengamankan jaringan dan aset pengguna termasuk perangkat komputasi yang terhubung, personel, infrastruktur, aplikasi, layanan, sistem telekomunikasi, dan semua informasi yang dikirimkan dan/atau disimpan di dunia maya.

Cybersecurity adalah upaya untuk memastikan bahwa atribut keamanan organisasi dan penggunanya dicapai dan dipelihara terhadap risiko keamanan terkait dalam lingkungan jaringan. Tujuan keamanan umum meliputi: ketersediaan; Integritas mencakup keaslian dan kemampuan untuk meminimalkan penolakan dan akhirnya kerahasiaan.

Keamanan siber global didasarkan pada lima bidang pekerjaan: Jaminan Hukum (hukum kejahatan siber); tindakan dan prosedur teknis (pengguna akhir dan perusahaan (akses langsung

[41] Definisi cyber security berdasarkan *FSB Cyber Lexicon (https://www.fsb.org/wp-content/uploads/P121118- 1.pdf). Diadaptasi dari International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27032:2012 – Guidelines for cybersecurity.*

dan penyedia layanan dan penyedia perangkat lunak); struktur organisasi (struktur organisasi yang sangat berkembang, menghindari tumpang tindih); pengembangan kapasitas dan pendidikan pengguna (kampanye publisitas dan komunikasi terbuka tentang ancaman kejahatan dunia maya terbaru) ; Kerjasama internasional (termasuk didalamnya kerjasama timbal balik dalam upaya mengatasi ancaman *cyber*) (undang-undang cyber crime); teknis dan tindakan prosedural (pengguna akhir dan bisnis (pendekatan langsung dan penyedia layanan dan perusahaan perangkat lunak); struktur organisasi (struktur organisasi sangat berkembang, menghindari tumpang tindih); capacity building dan pendidikan Pengguna (kampanye publik dan komunikasi terbuka dari ancaman *cyber crime* terbaru); Kerjasama Internasional (termasuk didalamnya kerjasama timbal balik dalam upaya mengatasi ancaman *cyber*).

Keamanan siber juga didefinisikan sebagai seperangkat mekanisme yang diterapkan untuk melindungi dan meminimalkan gangguan terhadap kerahasiaan, integritas, dan ketersediaan informasi. Mekanisme ini harus mampu melindungi informasi dari serangan fisik dan *cyber*. Keamanan siber adalah upaya untuk melindungi informasi dari serangan siber, sedangkan elemen kunci dari keamanan siber adalah:

a. Dokumen kebijakan privasi (*security* policy) merupakan dokumen standar sebagai acuan dalam

pelaksanaan semua proses yang berkaitan dengan keamanan informasi.

b. Infrastruktur informasi (*Information infrastructure*) adalah sarana untuk menyediakan kelangsungan operasi informasi, termasuk perangkat keras dan perangkat lunak. Contohnya termasuk router, switch, server, sistem operasi, database, dan situs web.

c. Perimeter Pertahanan (*Perimeter Defense*) adalah sarana bertindak sebagai elemen defensif dalam infrastruktur informasi seperti IDS, IPS dan firewall.

d. Sistem pemantauan jaringan (*Network Monitoring System*) adalah sarana untuk memantau kelayakan, penggunaan, dan pengoperasian suatu infrastruktur informasi.

e. Sistem Informasi dan Manajemen Peristiwa (*system Information and Event Managemen*t) adalah sarana untuk memantau berbagai peristiwa di jaringan, termasuk yang terkait dengan insiden keamanan.

f. Peringkat keamanan siber (*Network Security Assessment*) adalah elemen keamanan siber yang bertindak sebagai mekanisme kontrol dan memberikan ukuran keamanan informasi.

g. Kesadaran sumber daya manusia dan keamanan (*Human resource and security awareness*) terkait

dengan sumber daya manusia dan kesadaran keamanan informasinya.[42]

3. Jenis-Jenis Cyber

Menurut Prof. Richardus Eko Indrajit dalam bukunya Konsep dan Strategi keamanan Informasi di Dunia Cyber bagian Fenomena keamanan Informasi dalam Dunia Cyber terdapat 6 Jenis cyber yaitu sebagai berikut:[43]

a) Cyber Space

Pengertian *cyberspace* menurut William Gibson *"A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts...A graphical representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the non-space of the mind, clusters and constellations of data. Like city lights, receding."*[44]

Gibson menciptakan istilah dunia maya untuk menjelaskan bahwa ada tempat-tempat yang tidak nyata tetapi keberadaannya dapat dirasakan atau bahkan menjadi kenyataan dalam pikiran. *Cyberspace* telah dijelaskan jauh sebelum munculnya teknologi internet dan

[42] Handrini Ardiyanti, *Cybersecurity Dan Tantangan Pengembangannya Di Indonesia*, Politica Vol. 5, No.1 Juni 2014, hlm.98-99

[43] Richardus Eko Indrajit, *Konsep dan Strategi Keamanan Informasi di Dunia Cyber*, Yogyakarta : Graha Ilmu, 2014, hlm. 1.

[44] William Gibson, *Neuromancer* (New York: Berkley Publishing Group, 1989), pp. 128.

menjelaskan "ilusi konsensus" atau seolah-olah ada ruang atau sesuatu.

Cyberspace atau dunia maya ini merupakan integrasi dari berbagai peralatan teknologi komunikasi dan jaringan komputer (sensor, tranduser, koneksi, transmisi, prosesor, signal, kontroler) yang dapat menghubungkan peralatan komunikasi (computer,telepon genggam,instrumentasi,elektronik dan lain-lain) yang tersebar diseluruh penjuru dunia secara interaktif yang termediasi oleh internet.

Dibandingkan dengan penetrasi teknologi lainnya dalam sejarah manusia, penetrasi Internet adalah yang tercepat karena dikatakan bahwa miliaran transaksi terjadi setiap hari dengan nilai transaksi miliaran dolar AS per detik tanpa henti selama 24 jam. Singkatnya, Internet adalah entitas yang tak ternilai, seiring waktu harga dan nilainya akan meningkat karena semakin banyak aktivita**s**.[45]

b) *Cyber Threat*

Semakin besar nilai dunia maya, semakin banyak ancaman yang menyertainya. Ancaman pertama adalah keinginan beberapa kelompok atau pihak untuk mencuri barang dan barang berharga yang dapat diperjualbelikan melalui internet. Ancaman kedua adalah niat pelaku jahat untuk membuat Internet tidak berfungsi dengan baik, atau dengan kata lain, mencoba membuat Internet tidak berfungsi dengan baik. Ancaman ketiga datang dalam bentuk upaya untuk mengubah data atau

[45] Richardus Eko Indrajit, *Konsep dan Strategi Keamanan Informasi di Dunia Cyber*, hlm.2

informasi yang beredar di Internet dengan tujuan merusak. Ancaman keempat adalah keinginan individu untuk menyebarkan hal-hal buruk ke seluruh populasi dunia. Ancaman kelima adalah penyebaran dan penggarapan program jahat di komputer yang terhubung ke Internet. Semua ancaman ini normal karena tingginya nilai internet.[46]

Singkatnya Ancaman siber (*cyber threat*) mengacu pada kemungkinan keberhasilan serangan siber yang bertujuan untuk mendapatkan akses yang tidak sah, merusak, mengganggu, atau mencuri aset teknologi informasi, jaringan komputer, kekayaan intelektual, atau segala bentuk data sensitif lainnya. Ancaman siber dapat datang dari dalam suatu organisasi oleh pengguna terpercaya atau dari lokasi yang jauh oleh pihak yang tidak dikenal.

c) *Cyber Attack*

Potensi ancaman tersebut akan benar-benar menjadi masalah jika berhasil dimanfaatkan oleh pihak jahat dalam bentuk serangan. Dalam hal ini perlu dibedakan pengertian "ancaman" dan "serangan", dimana suatu kejadian baru dapat dianggap sebagai serangan jika penjahat memanfaatkan kelemahan sistem teknologi sehingga ancaman yang menakutkan benar-benar terjadi.

Berdasarkan Konvensi Budapest, serangan cyber dapat diklasifikasikan menjadi tiga kategori, yaitu:

- Jenis serangan pertama adalah kumpulan serangan dimana teknologi informasi dan

[46] Richardus Eko Indrajit, hlm.3-4.

komunikasi menjadi alat atau senjata utama untuk melakukan kejahatan. Misalnya, ponsel digunakan untuk mengirim pesan teks untuk mengelabui calon korban.

- Serangan dalam kategori kedua adalah serangkaian peristiwa di mana komputer atau teknologi informasi menjadi sasaran serangan penjahat. Seperti melakukan transaksi keuangan fiktif dalam sistem perbankan berbasis internet.
- serangan ketiga yang menargetkan peristiwa yang tujuan utamanya adalah untuk menghancurkan (termasuk memodifikasi dan membuat) data atau informasi yang disimpan di media komputer. Serangan yang dimaksud adalah modifikasi isi sebuah website tanpa sepengetahuan pemiliknya. [47]

d) *Cyber crime*

Menurut Gregory (2005) Cybercrime adalah suatu bentuk kejahatan virtual dengan memanfaatkan media komputer yang terhubung ke internet, dan mengeksploitasi komputer lain yang terhubung dengan internet juga. Serangan terhadap sistem keamanan teknologi informasi suatu organisasi tergolong pidana (*criminal*), baik pidana maupun perdata. Meskipun sebagian besar jenis kejahatan berkaitan erat dengan masalah keuangan, tidak jarang serangan tersebut mengakibatkan sejumlah nyawa melayang karena

[47] Richardus Eko Indrajit, hlm. 6-7.

menyerang sistem yang sangat sensitif, penting bagi kehidupan manusia.

Pada prinsipnya ada (empat) jenis kegiatan yang dianggap tindak pidana dalam dunia teknologi informasi, yaitu::

- Intersepsi (*Interception*) adalah tindakan mendengarkan transmisi yang terjadi antara satu pihak dengan pihak lain. Sebagai contoh, di Indonesia, hanya beberapa lembaga yang memiliki kewenangan untuk melakukan penyadapan/pemblokiran telepon, seperti Kepolisian Negara Republik Indonesia, Badan Intelijen Negara, dan Komisi Pemberantasan Korupsi. Perorangan atau organisasi yang tidak memiliki kewenangan untuk itu dapat dituntut jika melakukan tindakan yang berkaitan dengan penyadapan.
- *Interruption*, yaitu tindakan yang mengakibatkan terjadinya pemutusan komunikasi antara dua belah pihak yang seharusnya berinteraksi. Fenomena *Denial of Services* (*DoS*) atau *Distributed Denial of Services* (*DDoS*) merupakan salah satu serangan yang dapat mengakibatkan terjadinya kondisi interupsi pada sistem komputer.
- *Modification*, yaitu tindakan melakukan perubahan terhadap data atau informasi atau konten yang mengalir dalam sebuah

infrastruktur teknologi informasi tanpa sepengetahuan yang mengirimkan/ menerimanya. *Web defacement* salah satu jenis serangan yang bisa dikategorikan dalam kelas ini.

- *Fabrication*, yaitu tindakan mengelabui seolah-olah terjadi suatu permintaan interaksi dari seseorang seperti yang dikenal dengan istilah *phishing*. Tindakan kejahatan digital bertujuan untuk mencuri informasi dan data pribadi melalui email, telepon, pesan teks atau tautan yang mengaku sebagai instansi atau pihak-pihak tertentu.[48]

e) *Cyber Security*

Hal ini diperlukan untuk mencegah dan menghindari serangan siber yang merusak agar tidak merugikan banyak pihak. Oleh karena itu, beberapa tindakan pengamanan diperlukan. Pada prinsipnya, ada tiga cara utama untuk melindungi diri sendiri, yaitu:

- Memproteksi infrastruktur tempat mengalirnya data dan informasi mengalir saat transit. Infrastruktur fisik dan operasional darat, laut dan udara harus dilindungi dan dilindungi.
- Memproteksi data, nformasi atau konten yang ada dan/atau beredar dalam sistem komunikasi dan teknologi informasi. Metode seperti enkripsi atau kriptografi informasi adalah salah satu cara yang

[48] Richardus Eko Indrajit, hlm. 11-12.

populer dan kuat yang dipraktikkan oleh para pemain teknologi informasi.

- Melakukan proteksi terhadap komponen-komponen terkait dengan proses interaksi. Mulai dari pemilihan jenis media dan perangkat lunak komunikasi *email*, *chatting*, *browsing*, dan *blogging* hingga melakukan setting konfigurasi program. Khusus untuk Transaksi keuangan, misalnya, harus melengkapi mekanisme keamanan standar dan prosedur khusus untuk mencegah kebocoran dan pencurian data keuangan.[49]

Standar internasional BS7799/ISO17799 menekankan perlunya memperhatikan 10 (sepuluh) aspek utama agar memiliki sistem keamanan yang lengkap, holistik dan lengkap. Kesepuluh aspek keamanan dalam suatu organisasi atau instansi adalah:

1. Kebijakan privasi untuk memberikan panduan dan dukungan bagi manajemen keamanan informasi.
2. Organisasi keamanan untuk mengelola keamanan informasi dalam suatu organisasi. Pendekatan multi-disiplin terhadap keamanan informasi harus dikembangkan misalnya dengan melibatkan kerja sama dan kolaborasi di antara manajer, pengguna, administrator, perancang aplikasi, pemeriksa dan staf keamanan, serta keahlian di bidang asuransi dan manajemen risiko.
3. Klasifikasi dan kontrol aset untuk memelihara perlindungan yang tepat bagi pengorganisasian aset.

[49] Richardus Eko Indrajit, hlm. 8-9.

Akuntabilitas terhadap aset akan menjamin terdapatnya perlindungan yang tepat.

4. Pengamanan personil untuk mengurangi risiko kesalahan manusia, pencurian, penipuan, atau penyalahgunaan fasilitas. Seluruh pegawai dan pengguna pihak ketiga yang menggunakan fasilitas pemrosesan informasi harus menandatangani perjanjian kerahasiaan (*non-disclosure*).
5. Keamanan fisik dan lingkungan untuk mencegah akses yang tidak sah, kerusakan dan gangguan terhadap tempat dan informasi bisnis. Fasilitas pemrosesan informasi harus dilindungi secara fisik dari akses tanpa ijin, kerusakan dan gangguan. Perlindungan harus disesuaikan dengan identifikasi resiko.
6. Komunikasi dan Manajemen Informasi, keharusan ditetapkannya tanggung jawab dan prosedur untuk manajemen dan operasi seluruh fasilitas pemrosesan informasi. Hal ini mencakup pengembangan instruksi operasi yang tepat dan prosedur penanganan insiden.
7. Kontrol akses untuk mencegah akses tidak sah ke sistem informasi. Prosedur formal harus ada untuk mengontrol pemberian hak akses, mulai dari pendaftaran awal pengguna baru hingga pencabutan hak pengguna yang tidak lagi membutuhkan akses ke sistem dan layanan informasi.
8. Mengembangkan dan memelihara sistem untuk memastikan keamanan terintegrasi ke dalam sistem informasi. Persyaratan keamanan sistem, termasuk infrastruktur, harus ditetapkan selama fase persyaratan

proyek dan diputuskan, disetujui, dan didokumentasikan sebagai bagian dari sistem informasi secara keseluruhan.

9. Manajemen Kelangsungan Bisnis, prosesnya harus mencakup kontrol untuk mengidentifikasi dan mengurangi resiko, membatasi konsekuensi kesalahan yang merusak dan memastikan penyimpulan tahapan operasional yang penting.
10. Kesesuaian, untuk menghindari pelanggaran terhadap hukum pidana maupun perdata, maka desain operasional, penggunaan dan manajemen sistem informasi harus dicari penasihat hukum atau praktisi hukum yang berkualitas.[50]

f) *Cyber Law*

Lagi pula, keamanan siber saja tidak dapat mencegah munculnya motif kriminal di dunia maya, sehingga diperlukan perangkat yang lebih canggih dan efektif. Dalam kerangka inilah sejumlah negara mulai mengembangkan dan menegakkan hukum siber. Dalam undang-undang ini, berbagai klasifikasi dan ancaman hukuman untuk pelanggaran yang berkaitan dengan dunia komputer atau teknologi informasi. [51] Meski relatif tertinggal dari negara lain, Indonesia dalam Indonesia pada akhirnya memiliki undang-undang *cyber law* pertama yaitu Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Teknologi Elektronik (ITE) yang akhirnya direvisi pada beberapa bagian menjadi Undang-*Undang* (*UU*)

[50] Richardus Eko Indrajit, hlm. 89-92.
[51] Richardus Eko Indrajit, hlm. 13-14.

Nomor 19 Tahun 2016 tentang Perubahan atas *UU* Nomor 11 Tahun 2008.

4. *Cybercrime* (Kejahatan Siber) di Bidang Perbankan

Cyber Crime yang berkaitan dengan teknologi komputerisasi dan penggunaan jaringan telekomunikasi dapat dibagi menjadi beberapa kelompok. Menurut Golose (2006), sifat cybercrime dapat dibagi menjadi beberapa bentuk berdasarkan bentuknya, dengan fungsi sebagai berikut:

a. Akses tidak sah ke sistem dan layanan computer (*Unauthorized Access to Computer System and Service)* Kejahatan yang dilakukan dengan penyusupan atau penyusupan ke dalam sistem jaringan komputer adalah izin atau sepengetahuan pemilik sistem jaringan komputer di mana sistem itu diserang. Serangan yang terjadi biasanya dilakukan dengan cara mencuri untuk mendapatkan informasi yang sensitif dan sensitif. Selain itu, beberapa orang melakukan serangan hanya karena mereka merasa mencoba menguji keterampilan mereka melalui sistem .

b. Konten illegal (*Illegal Contents*) adalah kejahatan ketika data atau informasi yang salah dan tidak etis dan dapat dianggap ilegal atau ketertiban umum dan moral dimasukkan di Internet. Pembuatan berita palsu, tuduhan palsu yang dapat menghancurkan martabat dan harga diri orang lain, hal-hal yang berhubungan dengan pornografi, membaca informasi rahasia nasional,

ujaran kebencian, publisitas pemerintah yang sah, dll. Kejahatan yang terkandung dalam konten ilegal, dll.

c. Pemalsuan data (Data Forgery) adalah kejahatan pemalsuan data dokumen penting yang disimpan sebagai dokumen tanpa naskah di Internet. Kejahatan ini biasanya menyasar dokumen e-commerce dengan membuat seolah-olah ada "salah ketik" yang pada akhirnya menguntungkan pelakunya.

d. *Cyber Espionage* adalah kejahatan yang menggunakan internet untuk menyusup ke sistem jaringan komputer pihak yang dituju dan kemudian memata-matai pihak lain. Kejahatan ini biasanya menargetkan pesaing yang dokumen dan data penting disimpan di sistem komputer mereka.

e. *Cyber Sabotage and Extortion* adalah kejahatan yang dilakukan dengan cara mengganggu, merusak, atau menghancurkan data, program komputer, atau sistem jaringan komputer yang terhubung ke Internet. Biasanya, kejahatan ini tidak dapat ditanami dengan bom logika, virus komputer, atau program tertentu untuk digunakan, berfungsi dengan baik, atau dilakukan sebagaimana penjahat ingin menggunakan data, program komputer, atau sistem jaringan komputer. Contoh kejahatan biasanya penyebaran virus komputer ketika korban browsing internet.

f. Kejahatan kekayaan intelektual adalah kejahatan terhadap hak kekayaan intelektual yang dimiliki oleh pihak lain di Internet. Misalnya, secara ilegal meniru tampilan situs web orang lain di situs web tersebut, atau menyebarkan informasi yang ditemukan sebagai rahasia dagang orang lain di Internet.

g. Invasi privasi (*Infringements of Privacy*) adalah kejahatan yang ditujukan terhadap informasi yang sangat pribadi dan sensitif dari seorang individu. Kejahatan ini biasanya ditujukan terhadap informasi pribadi seseorang yang disimpan dalam bentuk informasi pribadi yang terkomputerisasi, dan jika diketahui orang lain, korbannya mungkin serius atau tidak serius, seperti: Dapat menyebabkan kerugian serius. B. Nomor kartu kredit, nomor PIN ATM, cacat tersembunyi dan penyakit, dll.

h. Pembobolan (*Cracking*) adalah kejahatan yang menggunakan teknologi komputer dan dilakukan untuk merusak sistem keamanan suatu sistem komputer, biasanya untuk mendapatkan akses dan melakukan tindakan pencurian dan kekacauan. Hal ini sering di salah faham antara hacker dan cracker. Hacker sendiri identik dengan aksi.

i. Carding adalah kejahatan yang menggunakan teknologi komputer untuk melakukan transaksi terhadap kartu kredit orang lain yang dapat

menimbulkan kerugian baik yang serius maupun tidak serius bagi orang tersebut.[52]

Dari hasil penelitian yang dikemukakan oleh Muhammad Khairul Faridi dengan judul "Kejahatan Siber dalam Bidang Perbankan" terdapat 3 metode yang sering digunakan pelaku tindak kejahatan (*cybercrime*) pada perbankan yaitu:[53]

a. *Skimming*, metode ini digunakan untuk mencuri informasi nasabah pada saat bertransaksi menggunakan ATM. Ada 3 komponen utama yang digunakan untuk melakukan metode skimming, yaitu skimmer, hidden camera dan keyboard. Skimmer digunakan untuk merekam aktivitas nasabah menggunakan mesin ATM, alat ini mampu merekam jejak elektromagnetik pada kartu korban saat kartu tersebut dimasukkan ke dalam ATM. Kamera tersembunyi dan keypad digunakan untuk merekam aktivitas korban saat memasukkan kode pin di ATM.

b. *Malware* merupakan singkatan dari *malicious software* yang artinya software yang tidak diinginkan pada sistem komputer, biasanya *malware* dibuat untuk mencuri informasi dan

[52] Maskun, *Kejahatan Siber Cyber Crime Suatu Pengantar* (Jakarta: Kencana Prenada Media Group, 2013). hlm.51-54.

[53] Muhammad Khairul Faridi, *Kejahatan Siber dalam Bidang Perbankan*, CyberSecurity dan Forensik Digital, Vol. 1, No. 2, November 2018, e-ISSN: 2615-8442, hlm. 59-60.

data, yang bahkan dapat merusak sistem komputer.[54] Malware sulit dideteksi oleh sistem komputer. Ada dua cara untuk mempengaruhi sistem komputer oleh malware, yaitu melalui drive USB dan melalui Internet. Sistem komputer yang terinfeksi malware melalui USB flash drive biasanya tidak memiliki keamanan seperti anti virus atau sejenisnya, sehingga malware yang diinstal pada USB flash drive dapat dengan mudah masuk ke sistem sistem komputer. Selain itu, infeksi sistem komputer melalui Internet terjadi ketika pengguna membuka email atau halaman web. Email berbahaya biasanya akan langsung difilter sebagai spam oleh sistem, namun beberapa dari email tersebut juga berhasil masuk ke kotak masuk. Malware ini dijalankan ketika objek yang terinfeksi dalam email diklik dan kemudian ketika sistem komputer terinfeksi malware, informasi pribadi termasuk data perbankan disimpan di komputer.

c. Hacking adalah aktivitas menyerang program komputer dan mengeksploitasi komputer yang dimiliki oleh individu atau bisnis dan dari waktu ke waktu peretasan umumnya dianggap sebagai kejahatan. Semua penjahat dunia maya

[54] Prayudi, Y dan Kurniawan, A, *Teknik Live Forensics Pada Aktivitas Zeus Malware Untuk Mendukung Investigasi Malware Forensics. HADFEX (Hacking and Digital Forensics Exposed),* 2014, hlm. 1-5.

diklasifikasikan sebagai serangan peretasan dan berikut adalah beberapa kemungkinan serangan peretasan dalam transaksi perbankan seperti *Distributed Denial of service* (DDOS). DDOS merupakan salah satu serangan yang sering dilakukan pada sistem server baik pada perusahaan maupun perbankan. Untuk dapat melakukan peretasan, hacker akan melakukan scan port yang terbuka kemudian mulai malukan menyerang pada jaringan bank.[55]

5. Sumber Risiko *Cyber Security* pada Bank

Sumber risiko keamanan siber dapat berasal dari pihak internal (sumber daya manusia, proses dan sistem) maupun faktor eksternal Bank, dengan penjelasan sebagai berikut:

a. Sumber Daya Manusia (SDM) SDM merupakan sumber risiko siber berupa ketidakmampuan SDM dalam menjalankan tugas terkait keamanan aset dan informasi Bank atau kurangnya kesadaran keamanan SDM dalam menjalankan tugas dan proses kerja sehari-hari serta sebagai faktor lain yang terkait dengan integritas sumber daya manusia bank.

b. Proses Desain dan implementasi proses operasional di Bank dapat menimbulkan risiko siber bagi Bank. Kelemahan dalam proses ini antara lain kurangnya proses saluran yang aman selama transmisi,

[55] Islam, S., *Systematic literature review: Security challenges of mobile banking and payments system. International Journal of u-and e-Service, Science and Technology*, 7(6), 2014, hlm.116.

pemeriksaan keamanan yang jarang, manajemen kata sandi yang buruk, dan penggunaan akses internet publik yang tidak aman.

c. sistem Kelemahan teknologi dan infrastruktur informasi Bank dapat menjadi sumber risiko cyber. Kurangnya pengujian keamanan, pengendalian dan pemantauan terhadap ancaman dan kerentanan keamanan, kelemahan sistem, seperti tidak adanya perangkat lunak anti-malware/anti-virus dan sistem yang tidak *up-to-dat*e merupakan penyebab risiko siber bagi Bank.

d. Faktor eksternal merupakan penyebab utama risiko siber bagi Bank karena kurangnya rasa aman nasabah. Selain itu, perkembangan taktik dan kecanggihan serangan siber juga menjadi faktor eksternal yang memunculkan ancaman siber.[56]

6. Upaya Pencegahan *Cybercrime* sebagai bentuk *Cyber security* pada Bank

Menurut Muhammad Khairul Faridi, dari menganalisis sejumlah penelitian sebelumnya tentang phishing dan malware, beberapa metode dapat diterapkan sebagai bagian dari upaya cybersecurity untuk memerangi kejahatan di bidang perbankan, terutama dengan menerapkan otentikasi tiga kali lipat menggunakan PIN/password, Token/OTP dan biometrik.[57]

Serangan oleh *cyber crime* menyulitkan

[56] Departemen Penelitian dan Pengaturan Perbankan OJK, *Consultative Paper Manajemen Risiko Keamanan Siber Bank Umum*, 2021, hlm. 9.

[57] Op.cit..., Muhammad Khairul Faridi, hlm.60.

banyak korban, terutama dari sudut pandang keamanan dan keuangan. Berdasarkan banyaknya serangan yang ditimbulkan oleh pelaku *cyber crime*, menurut Arifah, penanganan dan pencegahan dapat dilakukan dengan berbagai cara, seperti:

a. Edukasi Pengguna Edukasi pengguna (*Educate User Educate User*) merupakan upaya pemulihan yang dilakukan dengan memberikan pengetahuan baru tentang pelaku kejahatan siber dan dunia internet, bahwa tindakan yang dilakukan oleh pelaku adalah melawan hukum.

b. Menggunakan Perspektif Peretas (*Use Hacker's Perspective*) adalah perawatan yang menggunakan pemikiran peretas untuk melindungi sistem Anda.

c. Penambalan system (*patch system)* adalah perawatan yang melibatkan pengisian semua titik lemah dari suatu sistem.

d. Kebijakan (*Policy*) mendefinisikan kebijakan dan aturan yang melindungi sistem Anda dari orang yang tidak bertanggung jawab.

e. Firewall adalah sistem keamanan jaringan komputer yang digunakan untuk melindungi komputer dari berbagai jenis serangan dari luar komputer.

f. Anti Virus adalah software yang digunakan untuk mendeteksi, mengamankan dan menghapus virus

komputer seperti worm, Trojan horse, spyware dan sejenisnya dari sistem komputer.[58]

7. Standar Penerapan Manajemen Risiko Keamanan Siber (*Cyber Security*) pada Bank

Bank perlu menerapkan manajemen risiko keamanan siber yang efektif. Penerapan manajemen risiko keamanan siber perlu disesuaikan dengan tujuan bank, kebijakan bisnis, ukuran dan kompleksitas bisnis, teknologi informasi yang digunakan, dan kapabilitas.

Saat ini di Indonesia, seperti yang ditunjukkan dalam *Consultative Paper*, ada standar minimum yang harus dipenuhi bank dalam menerapkan manajemen risiko keamanan siber. Makalah penasihat ini memberikan laporan tentang konsep dasar keamanan siber, standar untuk menerapkan manajemen risiko keamanan siber, menilai kematangan manajemen risiko keamanan siber, menguji pertahanan keamanan siber, dan menerapkan manajemen risiko keamanan siber. [59]

Bank perlu secara proaktif menerapkan manajemen risiko keamanan siber untuk memastikan kelangsungan bisnis. Dalam hal ini, bank perlu mempertimbangkan risiko yang melekat pada keamanan siber dan aspek manajemen risiko keamanan siber.

---

[58] Dista Amalia Arifah, *Kasus Cybercrime di Indonesia*, Jurnal Bisnis dan Ekonomi (JBE), September 2011, Vol. 18, No. 2, ISSN: 1412-3126, hlm. 190.

[59] Departemen Penelitian dan Pengaturan Perbankan OJK, *Consultative Paper Manajemen Risiko Keamanan Siber Bank Umum*, 2021, hlm. 6.

Risiko bawaan mencakup risiko yang dapat diukur dan tidak dapat diukur yang dapat berdampak buruk pada bisnis kami. Karakteristik risiko bawaan terutama ditentukan oleh faktor internal dan eksternal seperti strategi bisnis, karakteristik bisnis, teknologi informasi yang digunakan bank, kompleksitas produk dan aktivitas bank, serta ancaman keamanan siber yang muncul. Penilaian risiko yang unik memperhitungkan setidaknya lima faktor penilaian: teknologi, saluran distribusi, produk dan aktivitas, karakter organisasi, dan kinerja ancaman *cyber*.

Bank perlu menerapkan aspek-aspek manajemen risiko keamanan siber, yang paling sedikit meliputi:

(a) Tata kelola risiko keamanan siber meliputi dewan dan komite, sumber daya manusia, struktur organisasi, budaya dan kesadaran, dan staf. Termasuk pemantauan aktif terhadap kemampuan Anda.

(b) Manajemen atau strategi risiko keamanan siber melibatkan penentuan tingkat risiko yang akan diambil dan toleransi risiko yang terkait dengan keamanan siber, dan penetapan strategi manajemen risiko keamanan siber . Dan kebijakan, prosedur, dan pengaturan pembatasan.

(c) Proses Identifikasi, Perlindungan, Ketanggapan, dan Ketahanan serta Sistem Informasi Manajemen Risiko Keamanan Siber

(d) Kecukupan sistem pengendalian internal.[60]

[60] Departemen Penelitian dan Pengaturan Perbankan OJK, hlm. 15.

8. Pentingnya Penerapan *Cyber Security* pada Bank Digital

Alasan pentingnya penerapan Cyber Security pada Bank Digital adalah sebagai berikut:

a. Upaya untuk mencegah, melindungi bahkan menghindari banyaknya serangan *cyber* atau ancaman cyber crime pada Bank Digital.

b. Meminimalisir kebocoran data yang terjadi yang dapat berakibat penipuan berkedok pinjaman online (Pinjol), atau juga peretasan akun media sosial untuk menipu keluarga dan kerabat dekat.

c. Agar transaksi keuangan yang dilakukan secara digital dapat dilakukan secara aman.

D. Hukum Positif di Indonesia

Sebelum mengulas tentang pengertian dari hukum positif, ada baiknya mengulas tentang yang dimaksud dengan hukum terlebih dahulu. Hukum adalah keseluruhan peraturan baik yang tertulis maupun tidak tertulis yang mengatur tata tertib dalam masyarakat dan terhadap pelanggarnya umumnya dikenakan sanksi. Tujuan dari hukum adalah untuk mengadakan keselamatan, kebahagiaan, dan ketertiban dalam masyarakat.

Adapun yang dimaksud dengan hukum positif adalah kumpulan asas dan kaidah hukum tertulis yang pada saat ini sedang berlaku dan mengikat secara umum atau khusus dan ditegakkan oleh atau melalui pemerintah atau pengadilan dalam negara Indonesia.

Hukum dapat diklasifikasi kedalam berbagai macam pengelompokan, yang antara lain dilihat dari segi sumbernya, bentuknya, isi materinya dan lain sebagainya. [61]

Berdasarkan isinya, hukum dapat dibagi menjadi 2, yaitu hukum privat dan hukum publik. Hukum privat adalah hukum yang mengatur hubungan orang perorang seperti halnya, perkawinan, perceraian, kematian, pewarisan, harta benda, kegiatan usaha dan tindakan-tindakan yang bersifat privat lainnya. Berbeda dengan hukum publik, hukum publik adalah hukum yang mengatur hubungan antara negara dengan warga negaranya.

E. Hukum Ekonomi Syariah

Hukum ekonomi syariah adalah kumpulan peraturan yang memiliki kaitannya tentang pemenuhan kebutuhan manusia baik itu bersifat umum maupun khusus berdasarkan ketentuan atau syariat Islam. Secara konseptual hukum ekonomi syariah ini memiliki hubungan yang erat dengan fiqih muamalat, karena kajian mengenai sumber hukum ekonomi syariah telah ada dalam pada fiqih muamalat. Hanya pengembangan dan perluasan gagasannya perlu penjabaran yang sesuai dengan konteks perkembangan zaman khusus dalam bidang ekonomi dan harta benda.

Hukum ekonomi syariah merupakan salah satu cabang ilmu yang muara adalah hukum Islam. Posisi

[61] Abdoel Djamali, *Pengantar Hukum Indonesia*, (Jakarta: PT. Raja Grafindo Persada, 2005), hal.3

hukum ekonomi syariah pada kedudukan konstitusi di Indonesia juga dilihat dari sumbernya. Ada 3 (tiga) elemen sumber hukum yang memiliki kedudukan yang seimbang di Indonesia yaitu, hukum adat (hukum kebiasaan), hukum dari Barat dan hukum Islam. Menurut Azizy positivisasi hukum di Indonesia adalah menjadikan hukum Islam sebagai sumber dari perarturan perundang-undangan termasuk didalamnya juga putusan hakim, kebiasaan dan doktrin.[62]

Sumber hukum ekonomi syariah ini merujuk pada muara dari sumbernya. Muara dari hukum ekonomi syariah ini adalah hukum Islam, maka otomatis dahwa sumber hukumnya terbagi menjadi 2 (dua) bagian, yaitu:

1. Sumber hukum primer yaitu sumber hukum yang telah menjadi hujah dan rujukan oleh para ulama untuk mengetahui hukum-hukum Islam yaitu:

a. Al-Qur'an sumber segala hukum yang diturunkan Allah SWT kepada Nabi . Muhammad SAW.

b. As-Sunnah yaitu segala perkataan, perbuatan, pengakuan yang berasal dari Nabi Muhammad SAW. Al-Qur'an dan As-Sunnah menjadi dasar hukum utama dalam Islam. hierarki kedudukannya As-Sunnah merupakan sumber hukum kedua setelah Al-Qur'an.

[62] A. Qodri Azizy, *Eklektisisme Hukum Nasional*, Cet. ke-1 (Yogyakarta: Gama Media, 2002). hlm. 177

2. Sumber hukum sekunder adalah hukum yang dikeluarkan melalui teknik berfikir dan penalaran oleh para ulama dengan menyaring kaidah-kaidah dari sumber hukum primer untuk menyelesaikan masalah baru dan belum disebutkan dalam nash. Adapun pembagian sumber hukum sekunder terdiri dari:

a. Ijma' Ulama yaitu hukum yang didapat dari kesepakatan dari para mujtahid setelah wafatnya Rasulullah ﷺ .Para mujtahid ini tentunya memiliki kualifikasi tertentu untuk mengeluarkan sebuah hukum yaitu: 1) Orang tersebut memiliki tingkatan tertentu dalam suatu bidang ilmu tertentu;

2) Orang tersebut memiliki tingkat penalaran yang tinggi dan kompleks untuk diuraikan terhadap kasus-kasus yang berkembang;

3) Usaha ijtihad dilakukan dengan metode istinbat (menggali dari sumber hukum tertentu); dan

4) Hasil dari ijtihad tersebut adalah dugaan kuat tentang hukum syara' yang bersifat amaliyah. Ijtihad terbagi menjadi 2 (dua) menurut tipenya, yaitu pertama ijtihad fardhi yaitu ijtihad yang dilakukan oleh satu orang ulama saja contohnya Yusuf Qardhawi. Dan kedua ijtihad jama'i yaitu ijtihad yang dilakukan para ulama secara berkelompok contohnya DSN-MUI dan Kompilasi Hukum Ekonomi Syariah (KHES).

b. Qiyas yaitu menjelaskan suatu hukum pada masalah-masalah yang tidak dijelaskan atau disebutkan tentang dasar hukumnya dalam nash,

dengan membandingkan masalah tersebut dengan masalah sejenis dengannya.[63] Contoh metode qiyas ini adalah tentang minuman khamar terdapat dalam Al-Qur'an Surah An-Nahl ayat 67 yang maknanya Para fuqaha menyadari bahwa selain air perasan anggur dan kurma, segala hal yang menyebabkan timbulnya rasa memabukkan maka jatuh hukumnya dengan khamer dan itu diharamkan.

c. Urf' merupakan kebiasaan-kebiasaan baik yang telah menjadi tradisi oleh manusia baik itu berupa perbuatan maupun perkataan. Istilah yang paling melekat dalam masyarakat Indonesia adalah kearifan lokal.[64]

d. Istihsan merupakan pengambilan hukum melalui teknik qiyas yaitu dengan mencari dasar hukum dari qiyas jalli yang satu guna mencari dan menjabarkan hukum dengan qiyas khafi dengan bersandarkan terhadap nash yang telah ada. Contohnya istihsan dengan hadits yaitu sahnya puasa bagi orang yang makan karena lupa.

e. Maslahah Mursalah merupakan penetapan hukum menurut akal manusia yang selaras dengan tujuan syara', tetapi nash tidak menyebutkan terhadap penolakannya dan tidak ada pula mengakuinya.[65]

---

[63] Ahmad Sarwat, Qiyas Sumber Hukum Syariah Keempat (Jakarta: Rumah Fiqh Publishing, 2019). hlm. 13

[64] Syamsuddin, Anita Marwin, dan Mohammad Tahmid Nur, *Realitas 'Urf Dalam Reaktualisasi Pembaharuan Hukum Islam Di Indonesia* (Madura: Duta Media Publishing, 2020). hlm. 10.

[65] Rusdaya Basri, Ushul fikih 1 (Pare pare: IAIN Parepare Nusantara Press, 2020). hlm. 18.

Contohnya yaitu mengenai kasus al-Laits Ibnu Sa'ad yang langsung menetapkan dengan hukuman berupa puasa dua bulan berturut-turut bagi seorang penguasa yang hubungan suami-isteri pada siang hari bulan Ramadhan. Pada kasus tersebut, para ulama memandang putusan Al-Laits tersebut bertentangan dengan hadits Rasullah. Karena menurut para ulama tersebut hukum dalam hadits tersebut harus diterapkan secara berurutan. Oleh sebab itu, ulama ushul fiqh memandang mendahulukan puasa dua bulan berturut-turut daripada memerdekakan seorang budak dengan dalil kemaslahatan hukum, merupakan kemaslahatan yang bertentangan dengan kehendak syara', sehingga dengan sendirinya putusan itu menjadi batal.

f. Sududz Dzariah adalah penetapan suatu hukum yang asalnya mubah menjadi makruh atau haram.[66] Contohnya larangan meminum minuman keras walau hanya seteguk. Apabila dipikirkan seteguk minuman tersebut tidak mungkin membuat seseorang menjadi mabuk. Akan tetapi konteks larangan ini dimaksudkan agar menjaga orang tersebut untuk tidak meminum lebih banyak lagi.

g. Istishab merupakan penetapan hukum yang telah ada pada masa lalu dan masih berlaku hingga ada hukum baru untuk memperbaharui hukum tersebut.[67]

[66] M. Syukri Azwar Lubis, *Materi Pendidikan Agama Islam* (Surabaya: Media Sahabat Cendekia, 2019). hlm. 92

[67] Moh Mufid, *Ushul Fiqh Ekonomi dan Keuangan Kontemporer: Dari Teori ke Aplikasi* (Jakarta: Kencana, 2018). hlm. 100

Contohnya yaitu ketika seseorang ragu-ragu apakah dia telah melakukan wudhu atau belum. Pada saat itu dia harus memiliki keyakinan bahwa dia belum melakukan wudhu dan harus segera berwudhu, karena sholat tidak akan sah jika tidak berwudhu.

BAB III
CYBER SECURITY MENURUT HUKUM POSITIF DI INDONESIA DAN HUKUM EKONOMI SYARIAH

A. *Cyber Security* Menurut Hukum Positif di Indonesia

Hukum adalah keseluruhan peraturan baik yang tertulis maupun tidak tertulis yang mengatur tata tertib dalam masyarakat dan terhadap pelanggarnya umumnya dikenakan sanksi. Adapun yang dimaksud dengan hukum positif adalah kumpulan asas dan kaidah hukum tertulis yang pada saat ini sedang berlaku dan mengikat secara umum atau khusus dan ditegakkan oleh atau melalui pemerintah atau pengadilan dalam negara Indonesia.

Hukum melekat pada masyarakat, karena hukum diciptakan untuk mengatur masyarakat, maka masyarakat harus ikut serta dalam pelaksanaan peraturan tersebut. Orang-orang diharuskan untuk mengikuti aturan untuk mendapatkan pesanan. [68] Peraturan yang dibuat untuk mengatur masyarakat biasanya berupa undang-undang yang dikeluarkan oleh pemerintah untuk memenuhi kebutuhan masyarakat.

Dasar hukum pengaturan keamanan siber di Indonesia adalah Undang-Undang Informasi dan Transaksi Elektronik (ITE) Nomor 11 Tahun

[68] Satjipto Rahardjo, *Sosiologi Hukum Esai-Esai Terpilih* (Yogyakarta: Genta Publishing, 2010). hlm. 99.

2008 dan Undang-Undang ITE Perubahan Nomor 19 Tahun 2016. Undang-undang ini memuat ketentuan sejumlah pelanggaran, seperti penyebaran konten ilegal. , pelanggaran perlindungan data, akses tidak sah ke sistem komputer untuk memperoleh informasi, perampasan ilegal dan tidak sah atau penyadapan sistem komputer komputer atau elektronik lainnya. UU ITE memberikan perlindungan hukum terhadap isi sistem elektronik dan transaksi elektronik. Namun, undang-undang tersebut tidak membahas aspek-aspek penting dari keamanan siber, seperti infrastruktur informasi dan jaringan, serta sumber daya manusia yang memiliki keahlian keamanan siber.

Berdasarkan UU ITE 2016, pemerintah telah mengeluarkan regulasi teknis, khususnya Peraturan Pemerintah (PP) Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. PP No 71 Tahun 2019 memuat pemutakhiran terkait penerapan keamanan siber dalam sistem dan transaksi elektronik. Selain sejumlah pasal terkait pelanggaran yang tercakup dalam UU ITE, PP No 71 Tahun 2019 memiliki ketentuan yang lebih ketat tentang perlindungan informasi dan informasi pribadi, serta otentikasi situs web untuk Menghindari situs web palsu atau scam. Selain itu, PP Nomor 71 Tahun 2019 menekankan perlunya pemerintah mencegah kerugian terhadap kepentingan umum melalui penyalahgunaan informasi dan transaksi elektronik

serta perlunya mengembangkan strategi keamanan jaringan nasional. Namun, PP No. 71 hanya mencakup kejahatan dunia maya yang terkait dengan transaksi elektronik, seperti penyalahgunaan informasi, tanda tangan elektronik yang tidak sah, dan penyebaran infeksi dan afiliasi. Terbatasnya cakupan UU ITE dan PP No. 71 Tahun 2019 tidak mampu menjawab ancaman siber yang terus berkembang, terutama terhadap infrastruktur kritis pemerintah..[69]

Selain UU ITE, selama ini *cybersecurity* Indonesia diawasi oleh Indonesia Internet Infrastructure Security Incident Response Team (IDSIRTII), Indonesia Internet Infrastructure Security Incident Response Team (IDSIRTII). Sub Komite Darurat Komputer (IDCERT) dan *cybercrime* Bareskrim Divisi Ekonomi Khusus dan Reserse Kriminal (Dit Tipideksus). Meskipun kebijakan keamanan siber telah diatur dalam UU ITE, Indonesia juga menghadapi masalah pembagian kekuasaan dan lembaga yang diperlukan untuk memerangi *cybercrime*, *cyber terrorism*, *cyber hacktivism*, dan *cyber warfare*.[70]

Undang-Undang yang mengatur untuk perlindungan terhadap keamanan data dan

[69] Noor Halimah Anjani, *Ringkasan Kebijakan No. 9 Perlindungan Keamanan Siber di Indonesia, Center For Indonesian Policy Studies (CIPS)*, Maret 2021. hlm.4.

[70] Hidayat Chusnul Chotimah, *Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara*, Politica Vol. 10 No. 2 November 2019. hlm.119.

transaksi yang dilakukan konsumen/pengguna jasa/nasabah di Indonesia dikaitkan dengan Undang-Undang Perlindungan Konsumen yang tertuang dalam Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen.

Sedangkan Undang-Undang tentang Informasi dan Teknologi Informasi (ITE) sangat erat kaitannya dengan digitalisasi di Indonesia termasuk perihal perbankan digital yang di dalamnya juga mengatur tentang pentingnya keamanan (*security*) pada transaksi-transaksi digital.

1. Cyber Security pada Bank Digital Menurut Undang-Undang Perlindungan Konsumen

   Di Indonesia Undang-Undang tentang Perlindungan Konsumen diatur dalam Undang-Undang No. 8 Tahun 1999. Perlindungan Konsumen merupakan istilah yang dipakai untuk menggambarkan adanya hukum yang memberikan perlindungan konsumen. Menurut Pasal 1 angka (1) "Perlindungan konsumen adalah segala upaya yang menjamin adanya kepastian hukum untuk memberikan perlindungan konsumen".

   Perlindungan konsumen mempunyai cakupan yang sangat luas meliputi perlindungan terhadap segala kerugian yang akan, sedang dan telah terjadi akibat penggunaan barang dan jasa.

   Dalam transaksi pada bank digital, aspek tanggung jawab berlaku untuk pelaku usaha

(bank digital). apabila konsumen (nasabah) menemui barang dan/atau jasa dalam hal ini layanan perbankan yang merugikan pihak nasabah. Aspek tanggung jawab terhadap keamanan/*security* kepada Nasabah dalam Undang-Undang Perlindungan Konsumen diatur dalam Pasal 2 yaitu "Perlindungan Konsumen berasaskan manfaat, keadilan, keseimbangan, keamanan, dan keselamatan konsumen serta kepastian hukum" . [71]

Dan diatur pula dalam pasal 4 bagian a. yaitu "Hak atas kenyamanan, keamanan dan keselamatan dalam mengkonsumsi barang dan/atau jasa".[72]

Aspek ini berlaku pada saat pelaku usaha melakukan perbuatan yang menyebabkan kerugian bagi konsumen (nasabah). Kerugian ini berupa kebocoran data nasabah karena kurangnya keamanan/*security* pada bank digital.

2. Cyber Security menurut Undang-Undang Informasi dan Teknologi Elektronik (ITE)

Pengenalan rezim hukum baru (UU ITE) yang dikenal sebagai undang-undang telekomunikasi dapat dilihat sebagai respon positif. Telekomunikasi atau hukum jaringan digunakan secara internasional untuk istilah

[71] Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen pasal 2

[72] Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen pasal 4

hukum yang berkaitan dengan penggunaan teknologi informasi dan komunikasi. Demikian pula hukum telekomunikasi merupakan ekspresi dari konvergensi hukum telekomunikasi, hukum telekomunikasi, hukum komunikasi, dan hukum komputer. Istilah lain yang juga digunakan adalah hukum teknologi informasi (information technology law), hukum siber (virtual world law) dan hukum siber. Istilah ini berasal dari pertimbangan kegiatan yang dilakukan melalui jaringan sistem komputer dan sistem komunikasi, baik lokal maupun global (Internet) dengan menggunakan teknologi informasi berdasarkan satu sistem.Komputer adalah sistem elektronik yang terlihat secara virtual. [73]

Kegiatan melalui media sistem elektronik, yang disebut juga ruang siber (*cyber space*), meskipun bersifat virtual dapat dikategorikan sebagai tindakan atau perbuatan hukum yang nyata. Kegiatan dalam ruang siber adalah kegiatan virtual yang berdampak sangat nyata meskipun alat buktinya bersifat elektronik. Secara yuridis kegiatan pada ruang siber tidak dapat didekati dengan ukuran dan kualifikasi hukum konvensional saja sebab jika cara ini yang ditempuh akan terlalu banyak kesulitan dan hal yang lolos dari pemberlakuan hukum.

[73] Maskun, *Kejahatan Siber (Cybercrime) Suatu Pengantar*, Kencana Prenada Media Group : Jakarta, 2013, hlm.29.

UU ITE diundangkan pada tahun 2008 dan kemudian direvisi secara terbatas pada tahun 2016, ruang lingkup undang-undang ini adalah "satu untuk semua" dalam hal mengatur segala hal yang berkaitan dengan penggunaan teknologi informasi dan komunikasi termasuk perihal *Cyber Security* namun hanya sedikit pasal yang membahas terkait dengan keharusan adanya *Cyber Security*. Sebagaimana tertuang dalam pasal pasal 15 ayat 1 Undang Undang ITE bahwa "Setiap Penyelenggara Sistem Elektronik harus menyelenggarakan Sistem Elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya Sistem Elektronik sebagaimana mestinya."

Dan tertuang pada pasal 16 ayat (1) point b. Pada Undang-Undang Nomor 11 Tahun 2008 jo. Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik yang berbunyi:

"Setiap penyelenggara Sistem Elektronik wajib mengoperasikan Sistem Elektronik yang memenuhi persyaratan minimum yaitu dapat melindungi ketersediaan, keutuhan, keotentikan, kerahasiaan, dan keteraksesan Informasi Elektronik dalam Penyelenggaraan Sistem Elektronik tersebut"

Cyber Security erat kaitannya dengan Cyber Law. Hukum siber adalah dasar hukum untuk proses penegakan hukum anti kejahatan kejahatan yang menggunakan teknologi digital, termasuk kejahatan pencucian uang dan kejahatan

teroris. Fakta bahwa Hukum Jaringan perlu diatasi Kejahatan dunia maya.

B. Pengaturan Kejahatan Siber (*Cybercrime*) pada Perbankan

Indonesia belum memiliki undang-undang/*cyber law* khusus yang mengatur tentang *cybercrime*. Namun, ada sejumlah hukum positif lainnya yang diterima secara umum dan dapat diterapkan pada penjahat dunia maya, terutama dalam kasus dimana komputer digunakan sebagai kendaraan, antara lain:[74]

1. Kitab Undang-Undang Hukum Pidana

   Ketentuan KUHP sering digunakan lebih dari satu karena berkaitan dengan banyak perbuatan serta ketentuan yang dapat diterapkan dalam KUHP tentang Cybercrime, yaitu:

   a) Pasal 362 KUHP berlaku untuk kasus pencurian kartu dimana pelaku mencuri nomor kartu kredit orang lain, bahkan tidak dalam kenyataan, karena nomor kartu hanya diperoleh dengan menggunakan perangkat lunak pembuatan kartu berbasis internet untuk melakukan transaksi e-commerce . Setelah menyelesaikan transaksi dan mengirimkan barang, merchant yang ingin menarik uang dari bank ditolak karena pemegang kartu bukanlah orang yang melakukan transaksi.

[74] Deris Setiawan, *Sistem Keamanan Komputer*, (Jakarta: PT Elex Media Komputindo, 2005).hlm. 40

b) Pasal 378 KUHP dapat dijerat dengan penipuan dengan berpura-pura menawarkan produk atau barang dengan memasang iklan di salah satu situs web agar orang yang berminat membelinya dan kemudian mengirimkan uang kepada Pengiklan. Tapi, pada kenyataannya, itu tidak ada. Hal ini diketahui setelah uang dikirim tetapi barang yang dipesan tidak sampai, sehingga pembeli tertipu.

c) Pasal 378 dan 262 KUHP dapat diterapkan pada kasus carding, karena pelaku melakukan penipuan seperti ingin membeli barang dan membayar dengan Nomor Kartu Kredit kartu kredit orang yang dicuri.

d) Pasal 406 KUHP dapat berlaku jika terjadi deface atau hacking yang membuat sistem orang lain, seperti situs web atau program, tidak dapat dioperasikan atau digunakan.

2. Undang-Undang No 36 Tahun 1999 tentang Telekomunikasi atau Undang- Undang Nomor 11 Tahun 2008 Tentang Internet & Transaksi Elektronik.

Menurut Pasal 1 angka (1) Undang - Undang No 36 Tahun 1999, Telekomunikasi adalah setiap pemancaran, pengiriman, dan/atau penerimaan dan setiap informasi dalam bentuk tanda-tanda, isyarat, tulisan, gambar, suara, dan bunyi melalui sistem kawat, optik, radio, atau sistem elektromagnetik lainnya. Dari definisi tersebut, maka Internet dan segala fasilitas yang

dimilikinya merupakan salah satu bentuk alat komunikasi karena dapat mengirimkan dan menerima setiap informasi dalam bentuk gambar, suara maupun film dengan sistem elektromagnetik. Penyalahgunaan Internet yang mengganggu ketertiban umum atau pribadi dapat dikenakan sanksi dengan menggunakan Undang- Undang ini, terutama bagi para hacker yang masuk ke jaringan orang lain menurut ketentuan Pasal 22, khususnya: Dilarang keras orang melakukan perbuatan tanpa hak, tidak sah, atau manipulatif:

1. Akses ke jaringan telekomunikasi
2. Akses ke layanan telekomunikasi
3. Akses ke jaringan telekomunikasi khusus

Apabila anda melakukan hal tersebut seperti yang pernah terjadi pada website KPU www.kpu.go.id, maka dapat dikenakan Pasal 50 yang berbunyi "Barangsiapa yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 22, dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp600.000.000,00 (enam ratus juta rupiah)".

3. Undang-Undang No.15 Tahun 2002 tentang Tindak Pidana Pencucian Uang

Undang-undang Nomor 15 Tahun 2002 merupakan undang-undang yang paling kuat yang memungkinkan penyidik memperoleh informasi tentang tersangka pelaku penipuan melalui internet, karena tidak memerlukan prosedur administrasi yang

panjang dan memakan waktu. Karena tindak pidana pencucian uang (Pasal 2 ayat (1) huruf q). Penyidik dapat meminta kepada bank penerima transfer untuk memberikan identitas tersangka dan rincian perbankan tanpa tunduk pada ketentuan. Dalam undang-undang perbankan, identitas dan data perbankan merupakan bagian dari rahasia perbankan, sehingga apabila penyidik membutuhkan informasi dan data tersebut, prosedurnya adalah dengan mengirimkan surat dari Kapolda kepada Kapolri dan diteruskan kepada gubernur. dari Bank Indonesia. Proses ini membutuhkan waktu yang lama untuk mendapatkan data dan informasi yang diinginkan.

Dalam UU Pencucian Uang proses lebih cepat karena Kapolda hanya perlu mengirimkan surat kepada pimpinan Bank Indonesia di daerah beserta tembusannya kepada Kapolri dan Gubernur Bank Indonesia, untuk data dan informasi yang diperlukan Dapat diperoleh lebih lanjut dengan cepat dan memudahkan penyidikan terhadap pelaku yang ditawarkan oleh pihak bank, berupa: formulir permohonan, nomor rekening kedatangan dan keberangkatan, tanggal dan lokasi transaksi, penyidik dapat menelusuri lokasi pelaku pada data tersebut. Undang-undang ini juga mengatur tentang barang bukti elektronik atau barang bukti digital berdasarkan Pasal 38 huruf b, khususnya alat bukti lain berupa informasi yang diucapkan, dikirim,

diterima atau disimpan secara elektronik dengan alat optik atau sejenisnya.[75]

C. Cyber Security menurut Hukum Ekonomi Syariah

Hukum ekonomi syariah adalah kumpulan peraturan yang memiliki kaitannya tentang pemenuhan kebutuhan manusia baik itu bersifat umum maupun khusus berdasarkan ketentuan atau syariat Islam. Secara konseptual hukum ekonomi syariah ini memiliki hubungan yang erat dengan fiqih muamalat, karena kajian mengenai sumber hukum ekonomi syariah telah ada pada fiqih muamalat. Hanya pengembangan dan perluasan gagasannya perlu penjabaran yang sesuai dengan konteks perkembangan zaman khusus dalam bidang ekonomi dan harta benda.

Sumber hukum ekonomi syariah ini merujuk pada muara dari sumbernya. Muara dari hukum ekonomi syariah ini adalah hukum Islam, maka otomatis bahwa sumber hukumnya terbagi menjadi 2 (dua) bagian, yaitu:

1. Sumber hukum primer yaitu sumber hukum yang telah menjadi hujah dan rujukan oleh para ulama untuk mengetahui hukum-hukum Islam yaitu:

    a. Al-Qur'an sumber segala hukum yang diturunkan Allah kepada Nabi Muhammad SAW.

[75] Sofwan Jannah dan M. Naufal, *Penegakan Hukum Cyber Crime Ditinjau dari Hukum Positif dan Hukum Islam,* AL-MAWARID, VOL. XII, NO 1, FEB-AUGUST 2012, hlm. 74-77.

b. As-Sunnah yaitu segala perkataan, perbuatan, pengakuan yang berasal dari Nabi Muhammad SAW. Al-Qur'an dan As-Sunnah menjadi dasar hukum utama dalam Islam. hierarki kedudukannya As-Sunnah merupakan sumber hukum kedua setelah Al-Qur'an.

2. Sumber hukum sekunder adalah hukum yang dikeluarkan melalui teknik berfikir dan penalaran oleh para ulama dengan menyaring kaidah-kaidah dari sumber hukum primer untuk menyelesaikan masalah baru dan belum disebutkan dalam nash yang biasa disebut dengan Usaha Ijtihad. ijtihad dilakukan dengan metode istinbat (menggali dari sumber hukum tertentu). Orang yang melakukan Ijtihad disebut dengan Mujtahid atau *faqih* (ahli fikih). Untuk memudahkan seorang Mujtahid dalam beristinbat hukum terhadap suatu masalah hukum maka diperlukan adanya kaidah fikih atau *qawaid al-fiqhiyah*. Abdullah bin Sa'id Muhammad "Abbadi al-Lahji al-Hadhrami mendefinisikan al-*qawa'id al-fiqhiyyah* sebagai ketentuan yang dapat digunakan untuk mengetahui hukum tentang kasus-kasus yang tidak ada aturan pastinya di dalam Alquran, Sunnah maupun Ijma'.[76] Definisi ini mengindikasikan bahwa al-Hadhrami secara tegas meletakkan kaidah fikih dalam fungsinya

[76] Abdullah bin Sa'id Muhammad al-Lahji al-Hadrami, *Idah al-Qawa'id al-Fiqhiyyah*, (Surabaya : Hidayah. 1410H) hlm. 10.

sebagai status hukum tentang kasus-kasus baru yang belum disikapi dengan pasti oleh ketiga sumber hukum yaitu Alquran, Sunnah maupun Ijma'.

Dalam Hukum Ekonomi Syariah yang kaitannya dengan dunia digitalisasi yakni yang berkaitan dengan *Cyber Security* dalam penggunaan internet untuk menangkal serangan dan ancaman dari dunia *Cyber* belum ada ayat Alquran, Sunnah dan Ijma' yang secara jelas menerangkan perihal tersebut. Sehingga untuk menjabarkan *Cyber Security* dalam perspektif Hukum Ekonomi Syariah diperlukan adanya Kaidah-kaidah Fiqh. Dari hasil penelusuran penulis Kaidah-Kaidah Fiqh adalah sebagai berikut :

الْأَصْلُ فِي الْمُعَامَلَاتِ الْإِبَاحَةِ اِلاَّ اَنْ يَدُلَّ دَلِيْلٌ عَلَى تَحْرِيْمِهَا

"Pada dasarnya segala bentuk muamalah adalah boleh, terkecuali ada dalil yang mengharamkannya".[77]

Kaidah ini menerangkan bahwa Bank Digital dan *Cyber security* merupakan salah satu bentuk kegiatan yang termasuk dalam kajian muamalah kontemporer dan boleh dilakukan. Namun praktik muamalah kontemporer ini bisa saja diharamkan apabila mengandung unsur kezaliman.

Tanpa adanya *cyber security* maka Bank Digital akan menghadapi sebuah bahaya atau ancaman dan serangan kejahatan siber. Maka penerapan *cyber security*

[77] Hendi Suhendi, *Fiqh Muamalah*, (Jakarta : PT Raja Grafindo Persada, 2011). hlm. 2.

harus lebih didahulukan dibanding mengoperasikan Bank Digital. Sebagaimana kaidah fiqh bahwa mencegah kemudaratan itu lebih utama daripada menarik datangnya kemaslahatan.

دَرْءُ الْمَفَاسِدِ أَوْلَى مِنْ جَلْبِ الْمَصَالِحِ

"Mencegah kemudharatan itu lebih utama daripada menarik datangnya kemaslahatan".[78]

Ancaman dan bahaya serangan dari *cybercrime* merupakan hal yang akan mendatangkan kemudharatan bagi kehidupan manusia yang harus dihilangkan. Dalam kaidah fiqh berkaitan dengan "kemudaratan harus dihilangkan" sebagaimana berbunyi:

الضرار يزال

Menurut Muhammad al-Zarqa dalam kitabnya *Syarh al-Qawa'id al-Fiqhiyyah*, kaidah fiqh "al-dhâraru yuzâlu" menunjukkan bahwa menghilangkan kemudharatan adalah wajib.[79]

اَلضَّرَرُ يُدْفَعُ عَلَى قَدرِ الْإِمْكَانِ

"Kemudaratan dihilangkan semaksimal mungkin meskipun tidak seluruhnya hilang".[80]

---

[78] Fathurrahman Azhari, *Qawaid Fiqhiyyah Muamalah* (Banjarmasin, LKPD, 2015) hlm. 109.

[79] Ade Dedi Rohayana, *Ilmu Qawa'id Fiqhiyyah Kaidah-Kaidah Hukum Islam* (Jakarta: Gaya Media Pratama, 2008) hlm. 215.

[80] A.Djazuli, *Kaidah-Kaidah Fikih Kaidah-Kaidah Hukum Islam dalam Menyelesaikan Masalah-Masalah yang Praktis* (Jakarta: Kencana, 2007). Hlm. 73.

BAB IV
ANALISIS *CYBER SECURITY* PADA BANK DIGITAL MENURUT HUKUM POSITIF DI INDONESIA DAN HUKUM EKONOMI SYARIAH

A. *Cyber Security* Pada Bank Digital PT Bank Aladin Syariah Tbk.

1. Sekilas tentang PT Bank Aladin Syariah Tbk

PT Bank Aladin Syariah Tbk (IDX: BANK) (sebelumnya bernama PT Bank Net Indonesia Syariah Tbk) merupakan perusahaan yang bergerak dalam bidang perbankan dan bermarkas di Jakarta, Indonesia. Perusahaan ini didirikan pada tahun 1994.

Pada awalnya, perusahaan bernama Maybank Nusa Internasional yang merupakan patungan usaha antara Maybank dan Bank Nusa Nasional. Kemudian, pada tahun 2000, nama perusahaan berubah menjadi Bank Maybank Indocorp karena pengalihan saham Bank Nusa kepada Menteri Keuangan Republik Indonesia dan Perusahaan Pengelola Aset (sebelumnya Badan Penyehatan Perbankan Nasional).

Pada tahun 2010, perusahaan mulai beroperasi dengan prinsip syariah dengan nama baru Bank Maybank Syariah Indonesia. Kemudian, pada tahun 2011, saham milik Menteri Keuangan Republik Indonesia dialihkan kepada PT Prosperindo.

Pada Mei 2019, Maybank dan Prosperindo menandatangani Perjanjian Pembelian Saham dengan Aladin Global Ventures (dahulu NTI Global Indonesia) dan Berkah Anugerah Abadi, dimana Aladin dan Berkah bertindak sebagai pembeli saham.

Setelahnya, pada Desember 2019 kepemilikan perusahaan oleh Aladin dan Berkah mulai resmi berjalan, ditandai dengan persetujuan akuisisi oleh OJK, dimana masing masing perusahaan memegang 70% dan 30% saham perusahaan, yang dilanjutkan dengan perubahan nama perusahaan pada akhir Desember 2019 dan penandatanganan akta akuisisi oleh kedua pihak pada Januari 2020.

Dalam pengumuman akuisisi yang ditampilkan di website, kedua investor baru ini memiliki niat untuk memperluas cakupan perbankan dengan sektor UMKM. Pada tahun 2021, bank ini mencatatkan di lantai bursa dengan kode BANK. Bank ini menjadi bank digital syariah full pertama di Indonesia, dimana aplikasi Aladin sendiri sudah di *launch* ke publik sejak 2022.[81]

Alamat Bank Aladin Syariah ini bertempat di Gedung Millenium Centennial Center, Lt 7, Jl. Jenderal Sudirman Kav. 25. Jakarta Selatan 12920 Indonesia.

Aladin Bank akan membuka dan mempermudah akses layanan perbankan syariah berbasis digital agar

[81] "Bank Aladin Syariah", (https://id.wikipedia.org/wiki/Bank_Aladin_Syariah diakses tanggal 20 Mei 2022, Pukul 14:00)

dapat melayani seluruh lapisan masyarakat, serta menjalin kerjasama dengan pelaku industri di berbagai sektor. Keamanan dan kenyamanan nasabah juga menjadi prioritas kami dalam memaksimalkan penggunaan teknologi informasi guna mengembangkan produk-produk pendanaan, pembiayaan dan jasa-jasa perbankan lainnya, seperti transfer dana, pembayaran, pembelian dan lain-lain.

Nilai-nilai utama PT. Bank Aladin Syariah Tbk :

a. Beretika dan Patuh Syariah, Dalam menjalankan kegiatannya, Aladin Bank memiliki identitas etika dan kepatuhan syariah. Hal ini diwujudkan dengan menerapkan nilai-nilai Islam, antara lain kepercayaan, keadilan, kejujuran, menghormati sesama, kebenaran, dan toleransi.

b. Mudah diakses, Aladin Bank menyediakan layanan dan produk perbankan bagi siapa saja. Teknologi digital memungkinkan masyarakat Indonesia mengakses layanan perbankan syariah di mana saja dengan mudahnya. Dukungan dan layanan pun tersedia bagi nasabah yang membutuhkan bantuan.

c. Kolaboratif, Senantiasa terbuka untuk berkolaborasi dengan mitra bisnis dan menyalurkan dananya pada sektor-sektor yang produktif untuk menciptakan sebuah ekosistem bisnis yang sehat, produktif, dan menguntungkan bagi nasabahnya.

d. Integritas dan Amanah, Kepercayaan yang diberikan menjadi bekal Aladin Bank untuk selalu menjaga integritasnya dan amanah dalam memberikan berbagai pilihan layanan dan produk yang bermanfaat bagi nasabah.

Visi PT. Bank Aladin Syariah Tbk yaitu "Menjadi Bank Syariah Digital Terdepan melalui Inovasi Berkelanjutan"

Misi PT. Bank Aladin Syariah Tbk adalah sebagai berikut:

a. Membuka akses layanan perbankan syariah terpercaya untuk seluruh lapisan masyarakat

b. Menjalin kolaborasi berbasis teknologi dengan pelaku industri di berbagai sektor

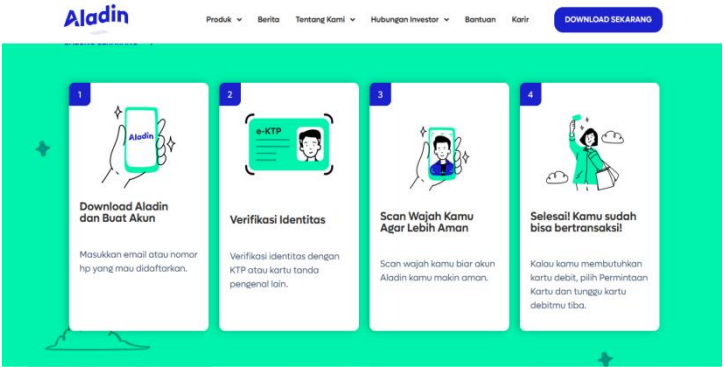
c. Pengembangan produk yang berkesinambungan dengan fokus pada kepentingan dan kepuasan pelanggan.[82]

2. Cyber Security pada Awal Pembuatan Rekening pada Bank Digital PT Bank Aladin Syariah Tbk

Pembuatan Rekening pada Bank Digital PT Bank Aladin Syariah Tbk dapat ditunjukkan pada gambar di bawah ini :

[82] "Tentang Aladin", (https://aladinbank.id/tentang-aladin/ diakses tanggal 22 Mei 2022, Pukul 23:40)

Gambar 4.1



Penjelasan :

a. Pada tahap awal setelah mendownload aplikasi Aladin di Playstore atau Appstore maka akan diarahkan untuk membuat Akun dengan memasukkan email aktif.

b. Setelah alamat email dimasukkan maka akan muncul pemberitahuan di pesan Gmail dengan judul "Verifikasi alamat email-mu" yang isi pesannya mengarahkan untuk mengklik tombol "Konfirmasi Email Saya" agar bisa melanjutkan proses buka rekening

c. Setelah Email terverifikasi, masukkan nomor ponsel aktif lalu tunggu sms dari Aladin Bank yang berisi Kode OTP dikirimkan ke nomor tersebut.

d. Setelah memasukkan Kode OTP yang dikirimkan melalui via sms dari Aladin Bank maka kita diwajibkan untuk pindai wajah mandiri, dengan syarat tidak ada yang

menghalangi wajah dan pencahayaan yang sesuai. Pemindaian wajah diambil secara dua kali dengan mulut terbuka dan mulut tertutup.

e. Jika posisi wajah sudah sesuai dengan permintaan aplikasi Tunggu beberapa menit bahkan sampai 2x24 jam untuk memverifikasi Informasi yang diberikan.

f. Setelah semua Proses Verifikasi berhasil maka akan diarahkan untuk memasukkan Identitas diri dengan memasukkan nomor NIK dan mengirimkan gambar e-ktp.

g. Setelah aplikasi Bank Aladin memverifikasi e-ktp atau identitas lain pengisian data pendapatan bulanan.

h. Setelah mengisi data pendapatan bulanan maka kita harus melakukan set up Ala PIN untuk keamanan transaksi.

i. Berhasil membuat PIN maka akan diarahkan pada form untuk menyetujui membuka tabungan dengan Akad Mudharabah dan Muthlaqah, yang akan dilanjutkan kepada syarat dan ketentuan (E-Statement).

j. Jika setuju maka klik centang pada kalimat "Saya setuju" lalu klik setuju dan lanjutkan. Jika tidak setuju, maka tidak dapat dilanjutkan ke proses selanjutnya.

k. Pembuatan Rekening Bank Digital pada PT Bank Aladin Syariah Tbk sudah selesai.

Kembali ke beranda masukkan email dan kata sandi untuk keamanan rekening.

(Gambar untuk Pembuatan Aplikasi Bank Digital tercantum di Lampiran)

Jika dilihat dari proses awal pembukaan Rekening pada PT Bank Aladin Syariah Tbk maka dapat dicermati beberapa point **upaya-upaya keamanan (*security*)** yaitu sebagai berikut :

a. Pada tahap awal pembukaan rekening Bank Digital pada PT Bank Aladin Syariah Tbk harus mendaftarkan email aktif dan harus memverifikasi melalui pesan yang dikirimkan melalui Email. Jika alamat email yang didaftarkan adalah fiktif maupun milik orang lain maka tidak akan bisa mengklik pesan verifikasi email yang dikirimkan pada Google Mail (G-Mail).

b. Memasukkan Nomor ponsel aktif yang akan dikirimkan kode OTP melewati Via SMS. Jika nomor ponsel yang digunakan adalah fiktif maupun milik orang lain maka akan kesulitan untuk memasukkan Kode OTP yang diminta pada aplikasi.

c. Mengirimkan foto E-KTP atau identitas lain sesuai dengan nama dan NIK yang didaftarkan. Jika foto E-KTP atau Identitas lain tidak bersesuaian dengan nama dan nomor NIK yang didaftarkan maka sistem akan otomatis menolak verifikasi Identitas.

d. Pemindaian Wajah (Scan Wajah) merupakan Sistem Pengenalan Wajah (Face Recognition) yang akan disesuaikan dengan database berkaitan data diri yang telah dikirimkan.

e. Proses Verifikasi Informasi/Identitas yang berlangsung bisa sampai 2 x 24 jam hari kerja. Ini merupakan proses keamanan dengan memperhatikan prinsip kehati-hatian.

f. Memasukkan Password setiap kali untuk membuka aplikasi dan Kode PIN setiap kali bertransaksi pada aplikasi rekening Bank Digital Aladin Syariah. Password/Kata Sandi yang dibuat harus mengandung minimal 8 karakter dan harus mengandung angka, huruf besar dan kecil serta karakter khusus jika tidak memenuhi syarat maka Password tidak bisa digunakan untuk membuka aplikasi Bank Digital pada PT Bank Aladin Syariah Tbk.

3. Cyber Security pada Klausul-Klausul yang tercantum pada Syarat dan Ketentuan

Pada saat membuka Rekening Bank Digital pada PT Bank Aladin Syariah Tbk maka diharuskan untuk menyetujui beberapa Syarat dan Ketentuan. Berkaitan dengan Cyber Security (keamanan) yang diupayakan Bank Digital PT Bank Aladin Syariah Tbk terhadap nasabah maka terdapat beberapa klausul-klausul yang

tercantum pada syarat dan ketentuan pada PT Bank Aladin Syariah Tbk yaitu sebagai berikut :

a. Point 3 Penyimpanan Data pribadi Anda bagian b. Terdapat klausul "kami menyimpan kerahasiaan dan keamanan data/informasi diri yang anda berikan. Penggunaan data Anda akan kami lakukan dengan mengacu pada bagian Kebijakan Privasi".

b. Point 9. Informasi Keamanan bagian a – e yang berbunyi sebagai berikut:

    1) Informasi keamanan berupa email Nasabah, kata sandi, One Time 1) 1) Password (OTP), dan Personal Identification Number (PIN) akan dibutuhkan untuk login, aktivasi perangkat, dan mengeksekusi setiap transaksi yang menurut Bank dibutuhkan sebagai tujuan otentikasi. Untuk tiap informasi keamanan yang akan ditentukan dan ditetapkan oleh Nasabah, Nasabah harus memastikan untuk menggunakan kata sandi yang kuat dan tidak memasukkan kata sandi yang mudah ditebak serta informasi diri seperti tanggal lahir dan alamat. Penggunaan informasi tersebut akan dianggap sebagai kelalaian Nasabah. Nasabah bertanggung jawab penuh terhadap keamanan dan kerahasiaan seluruh penggunaan Aplikasi Aladin miliknya.

    2) Bank tidak akan pernah meminta Nasabah memberitahukan kata sandi, OTP, dan PIN kepada Nasabah. Kelalaian Nasabah dalam

memenuhi ketentuan ini menjadi risiko dan tanggung jawab sepenuhnya Nasabah dan membebaskan Kami dari tanggung jawab apa pun.

3) Sesuai ketentuan yang berlaku, Bank wajib merahasiakan data penyimpan dan simpanannya kecuali diminta oleh pihak yang berwenang sesuai Peraturan Yang Berlaku.

4) Informasi keamanan akan menjadi rahasia di bawah tanggung jawab Nasabah, karena informasi tersebut memiliki keberlakuan setara dengan instruksi tertulis yang ditandatangani oleh Nasabah, dan akan diperlakukan sebagai otorisasi oleh Nasabah agar Bank melaksanakan transaksi melalui Aplikasi Aladin.

5) Bank akan mengajukan proses verifikasi yang memenuhi standar Bank untuk memungkinkan Nasabah melakukan transaksi keuangan dan/atau non-keuangan.[83]

[83] Tercantum pada syarat dan ketentuan dalam aplikasi Bank Digital Aladin Syariah

B. Analisis Cyber Security pada Bank Digital Menurut Hukum Positif di Indonesia

1. Analisis Cyber Security pada Awal Pembuatan Rekening hingga bertransaksi pada Bank Digital PT Bank Aladin Syariah Tbk

a. Mendaftarkan Email Aktif dan Verifikasi melalui Pesan EMail

Menurut Josua Sitompul, E-mail merupakan salah satu cara identifikasi keamanan yang paling lemah. Dalam banyak hal, kepercayaan, baik secara teknis maupun hukum, yang telah dibangun dalam dunia siber sulit untuk dilanjutkan atau dihubungkan dalam dunia nyata. Namun untuk membuktikan bahwa email yang dikirimkan adalah benar data pribadi kita sendiri maka ini diatur dalam prinsip pembuktian adanya hak yaitu dalam Pasal 7 UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Oleh karena itu, dapat dimengerti bahwa PT Bank Aladin Syariah Tbk tersebut menjalankan prinsip kehati-hatian. Ia tidak dapat memastikan bahwa kita adalah pengguna akun yang sah dari pemilik akun bank digital Aladin Syariah yang dimaksud, karena kita tidak dapat memastikan identitas, melalui mekanisme verifikasi yang ditentukan. Oleh karena itu, sepanjang identitas kita tidak dapat diverifikasi melalui E-Mail, hak Saudara juga akan tetap dipertanyakan.

Yang perlu diklarifikasi lebih jauh adalah apakah kita memberikan informasi yang benar pada waktu kita

mendaftarkan diri sebagai pengguna Akun Bank Digital Aladin Syariah yang dimaksud, misalnya, kita memberikan informasi mengenai nama, alamat, tempat dan tanggal lahir, nomor telepon yang benar. Jika informasi yang kita berikan telah benar dan kita dapat menunjukkan bukti-bukti untuk memverifikasi jati diri Saudara, maka hal tersebut merupakan petunjuk bahwa kita adalah pengguna e-mail yang dimaksud. [84]

b. Memasukkan Kode OTP yang dikirimkan melalui Nomor Ponsel Aktif Via SMS

One Time Password (OTP) atau kata sandi dinamis, adalah kata sandi yang hanya berlaku dalam waktu satu kali sesi atau transaksi log in, pada sistem komputer atau perangkat digital lainnya. *One Time Password* yang disinkronkan waktu biasanya terikat dengan perangkat keras yang disebut angka keamanan (misalnya, setiap pengguna diberi token pribadi yang menghasilkan kata sandi satu kali). angka ini dapat berupa perangkat berpemilik, atau ponsel atau perangkat seluler sejenis yang menjalankan perangkat lunak yang berpemilik, freeware, atau open-source .[85] OTP atau *One-Time Password* memiliki 4-6 digit huruf atau angka dengan durasi penggunaan maksimal 5 menit. Fungsi utama dari kode OTP adalah sebagai bentuk keamanan

[84] Josua Sitompul "Masalah Verifikasi Identitas di Dunia Siber" (https://www.hukumonline.com/klinik/a/masalah-verifikasi-identitas-di-duniasiberlt51f37ff48bc4c diakses tanggal 24 Mei 2022, Pukul 17:00)

[85] Eko Listiyani, *Kepastian Hukum Data Pribadi Terkait One Time Password (OTP) Dalam Penggunaan Media Elektronik* (UIN Surabaya: 2019), 22.

yang akan melindungi data-data dari pengguna sebuah aplikasi.

Dengan memberlakukan kode OTP ini, secara tidak langsung Bank Digital Aladin Syariah telah menerapkan bentuk manajemen risiko keamanan siber (*cyber security*) yang tertuang dalam *Consultative Paper* Manajemen Risiko Keamanan Siber Bank Umum yaitu acuan/standar minimal penerapan manajemen risiko keamanan siber tepatnya pada point 81 bagian d yang berbunyi:

"Bank menerapkan manajemen perlindungan terhadap akses dan pengguna dengan memperhatikan menggunakan verifikasi on time password (OTP) untuk transaksi yang berisiko tinggi".[86]

c. Pemindaian Wajah (Scan Wajah)

Pemindaian Wajah merupakan Sistem Pengenalan Wajah (*Face Recognition*) yang akan disesuaikan dengan database berkaitan data diri yang telah dikirimkan. Dalam aplikasinya sendiri pengenalan wajah menggunakan sebuah kamera untuk menangkap wajah seseorang kemudian dibandingkan dengan wajah yang sebelumnya telah disimpan di dalam database tertentu.[87] Teknik biometrika ini merupakan sebuah teknologi yang biasa digunakan untuk fitur keamanan menggunakan ciri-ciri fisik tubuh manusia yang khas dan berbeda-beda. Ada

[86] Departemen Penelitian dan Pengaturan Perbankan Otoritas Jasa Keuangan, *Consultative Paper Manajemen Risiko Keamanan Siber Bank Umum*, 2021 hlm. 34.

[87] Minartiningtyas, Brigida Arie. *Teori Pengenalan Wajah (Face Recognition)*, 2013.

beberapa data yang diambil melalui sistem *face recognition* ini mencakup data bentuk wajah, mata (iris mata), hidung, bentuk mulut dan lain sebagainya. Menurut *Center for Strategic & International Studies (CSIS)* mengatakan bahwa *face recognition* bisa memiliki tingkat akurasi yang nyaris sempurna, yaitu 99,97 persen.[88]

Berkaitan dengan pemindaian wajah yang berarti Bank Digital Aladin Syariah menerapkan teknik biometrika atau validasi biometrik. Hal ini bersesuaian dengan hasil penelitian dalam jurnal E-banking *security* oleh Fatima untuk menghindari serangan *phishing* dan *malware* yang hasil penelitiannya mengharuskan diterapkannya otentikasi 2 faktor yaitu menggunakan password dan proses validasi biometrik untuk menjamin keamanan nasabah. [89]

Dengan adanya sistem pemindaian wajah pada saat pembukaan rekening di aplikasi Bank Digital Aladin Syariah Tbk maka Bank Digital tersebut menggunakan sistem keamanan (*security*) yang tinggi untuk mencegah terjadinya kejahatan *cyber* yaitu penyalahgunaan data yang tidak bertanggung jawab oleh para oknum. Misalnya oknum mungkin saja bisa meretas data melalui sistem e-mail, kode OTP, Identitas diri orang lain namun dengan

[88] Bill Clinten, "*Apa itu Teknologi Face Recognition dan Bagaimana Cara Kerjanya*" (https://tekno.kompas.com/read/2022/04/14/17050047/apa-itu-teknologi-face-recognition-dan-bagaimana-cara-kerjanya-?page=all , diakses tanggal 3 Juni 2022 Pukul 20:35 WIB)

[89] Fatima, A., *E-Banking Security Issues-Is There A Solution in Biometrics?*. Journal of Internet Banking and Commerce, 16(2), p.1. 2011.

diterapkannya *face recognition*, oknum akan kesulitan dalam hal wajah dengan data diri yang tersimpan harus bersesuaian.

d. Penggunaan Kata Sandi / Password setiap kali membuka aplikasi Aladin dan Penggunaan PIN setiap kali akan bertransaksi.

Terlepas dari beraneka-ragamnya keberadaan sistem dan model keamanan Informasi berbasis teknologi yang canggih, pada tataran penggunaannya terutama untuk user awam dan kebanyakan – kata kunci atau yang dikenal sebagai "*password*". Password atau kata sandi merupakan hal yang sangat krusial dalam menjaga keamanan hak akses.[90] Dalam pembuatan kata sandi menurut Prof. Richardus Eko Indrajit dalam bukunya tentang Konsep dan Strategi Keamanan Informasi di Dunia Cyber, password yang baik maupun ideal memiliki kriteria diantaranya yaitu terdiri dari minimal 8 karakter dan penggunaan campuran secara random dari berbagai jenis karakter, yaitu: huruf besar, huruf kecil, angka dan simbol.[91]

Kata Sandi yang dibuat pada aplikasi Aladin maka harus mengandung minimal 8 karakter dan harus mengandung angka, huruf besar dan kecil serta simbol jika tidak memenuhi syarat maka sistem akan otomatis menolak dengan tanda merah dan PIN tidak bisa

[90] Richardus Eko Indrajit, *Konsep dan Strategi Keamanan Informasi di Dunia Cyber*, (Graha Ilmu :Yogyakarta, 2014), hlm. 131.
[91] Richardus Eko Indrajit, hlm. 132.

digunakan untuk membuka aplikasi Bank Digital pada PT Bank Aladin Syariah Tbk.

Jika dilihat dari pembuatan Kata Sandi maka Bank Digital pada PT Bank Aladin Syariah Tbk. Telah menerapkan manajemen password yang dikemukakan oleh Prof. Richardus Eko Indrajit yaitu dengan penggunaan minimum 8 karakter dan penggunaan karakter random. Dengan manajemen password ini maka gerbang keamanan nasabah untuk menangkal ancaman-ancaman kejahatan *cyber* pada Bank Digital khususnya pada aplikasi Aladin Syariah dapat diminimalisir.

Sistem keamanan PIN yang merupakan singkatan dari *personal identification number*, yaitu sebuah kode keamanan untuk memverifikasi identitas biasanya berupa angka. Menurut Dani Indra Junaedi peluang PIN dapat dibobol atau diretas adalah 1/1.000.000 kemungkinan.[92] Sehingga Penggunaan PIN merupakan keamanan yang paling tinggi yang diterapkan pada aplikasi Bank Digital Aladin Syariah.

2. Analisis Cyber Security pada Bank Digital sebagai Upaya Perlindungan terhadap Konsumen (Nasabah)

Security (Keamanan) dalam bertransaksi pada Bank Digital merupakan sesuatu yang harus diutamakan untuk menjamin kenyamanan, keamanan dan keselamatan konsumen (nasabah). Sebagaimana hal ini telah

[92] Dani Indra Junaedi, *Peluang Keamanan Password dalam Transaksi Perbankan*, Jurnal Ilmu-ilmu Informatika dan Manajemen STMIK, STMIK Sumedang, Vol 12 No.1 Mei (2018) Hlm.31.

diamanatkan dalam Undang-Undang Perlindungan Konsumen No. 8 Tahun 1999 tentang Perlindungan Konsumen, bahwa pada pasal 3 bagian 6:

"Perlindungan Konsumen bertujuan: meningkatkan kualitas barang dan/atau jasa yang menjamin kelangsungan usaha produksi barang dan/atau jasa, kesehatan, kenyamanan, keamanan, dan keselamatan konsumen".

Perihal aspek *security* (keamanan) yang harus diterapkan pada Bank Digital ini bersesuaian dengan asas-asas yang terdapat dalam pasal 2 Undang-Undang No. 8 Tahun 1999 tentang Perlindungan konsumen yaitu :

"Perlindungan Konsumen berasaskan manfaat, keadilan, keseimbangan, keamanan, dan keselamatan konsumen serta kepastian hukum".

a. Asas Manfaat
   Asas ini mengamanatkan bahwa segala upaya dalam penyelenggaraan perlindungan konsumen harus memberikan manfaat sebesar-besarnya untuk kepentingan konsumen dan pelaku usaha secara bersamaan.

b. Asas Keadilan
   Asas ini dimaksudkan agar dapat memberikan kesempatan kepada konsumen dan pelaku usaha mendapatkan haknya dan melaksanakan kewajibannya secara adil.

c. Asas Keseimbangan
   Asas ini dimaksudkan untuk memberikan perlindungan antara kepentingan konsumen, pelaku

usaha dan pemerintah baik materil dan spiritual sesuai dengan hak dan kewajibannya masing-masing.

d. Asas Keamanan dan Keselamatan Konsumen
   Asas ini dimaksudkan untuk memberikan jaminan atas keamanan dan keselamatan kepada konsumen dalam penggunaan, pemakaian dan pemanfaatan barang/jasa yang digunakan. Asas ini menghendaki adanya jaminan hukum bahwa konsumen akan memperoleh manfaat dari produk yang dikonsumsi atau dipakai, dan sebaliknya bahwa produk itu tidak akan akan mengancam ketentraman dan keselamatan jiwa dan harta bendanya.

e. Asas Kepastian Hukum
   Asas ini dimaksudkan agar baik pelaku usaha maupun konsumen menaati hukum dan memperoleh keadilan dalam penyelenggaraan perlindungan konsumen serta Negara menjamin kepastian hukum.[93]

Dari asas-asas diatas Berkaitan dengan *Cyber Security* pada Bank Digital maka penerapan *Security* (keamanan) merupakan pengamalan dalam Asas Hukum Perlindungan Konsumen yaitu asas keamanan dan keselamatan konsumen dalam hal ini nasabah bank Digital. Dimana *cyber security* pada Bank Digital adalah jaminan atau upaya keamanan dan keselamatan dalam penggunaan bertransaksi di Bank Digital. Secara tersirat diartikan bahwa Undang Undang Perlindungan Konsumen ini mengamanatkan sebuah kewajiban terhadap Bank

[93] Aulia Muthiah, *Hukum Perlindungan Konsumen Dimensi Hukum Positif dan Ekonomi Syariah*, (Yogyakarta: Pustaka Baru Press, 2018) hlm.42-43.

Digital untuk memberikan keamanan data maupun dana nasabah dari ancaman-ancaman kejahatan transaksi digital.

Berkenaan dengan Konsumen yang dalam hal ini adalah nasabah Bank Digital, maka menurut John F. Kennedy dalam Pidatonya mengemukakan Hak-Hak Konsumen secara umum dikenal menjadi empat hak dasar:

a. Hak memperoleh keamanan (*the right to safety*)
b. Hak memilih (*the right to choose*)
c. Hak untuk mendapat informasi (*the right to be informed*)
d. Hak untuk didengar (*the right to be heard*)

Sedangkan Masyarakat Ekonomi juga menetapkan hak-hak dasar konsumen (warga masyarakat Eropa) yang perlu mendapat perlindungan di dalam perundang-undangan Negara-negara Eropa yaitu :

a. Hak Perlindungan kesehatan dan keamanan
b. Hak perlindungan kepentingan ekonomi
c. Hak mendapatkan ganti rugi
d. Hak untuk didengar.

Adapun hak-hak Konsumen juga diatur dalam pasal 4 Undang-Undang No. 8 Tahun 1999 tentang Perlindungan konsumen yaitu adalah sebagai berikut :

a. Hak atas kenyamanan, keamanan dan keselamatan dalam mengkonsumsi barang dan/atau jasa;
b. Hak untuk memilih barang dan/atau jasa serta

mendapatkan barang dan/atau jasa tersebut sesuai dengan nilai tukar dan kondisi serta jaminan yang dijanjikan;

c. Hak atas informasi yang benar, jelas, dan jujur mengenai kondisi dan jaminan barang dan/atau jasa;

d. Hak untuk didengar pendapat dan keluhannya atas barang dan/atau jasa yang digunakan;

e. Hak untuk mendapatkan advokasi, perlindungan, dan upaya penyelesaian sengketa perlindungan konsumen secara patut;

f. Hak untuk mendapat pembinaan dan pendidikan konsumen;

g. Hak untuk diperlakukan atau dilayani secara benar dan jujur serta tidak diskriminatif;

h. Hak untuk mendapatkan kompensasi, ganti rugi dan/atau penggantian, apabila barang dan/atau jasa yang diterima tidak sesuai dengan perjanjian atau tidak sebagaimana mestinya;

i. Hak-hak yang diatur dalam ketentuan peraturan perundang-undangan lainnya.

Berdasarkan pemaparan diatas tentang hak-hak konsumen yang dalam penelitian ini adalah nasabah maka baik dari sudut pandang John F.Kennedy, masyarakat Ekonomi Eropa dan Undang-Undang Perlindungan Konsumen semua merujuk bahwa setiap konsumen (nasabah) mempunyai hak atas keamanan dan keselamatan dalam penggunaan jasa yang diperolehnya. Hak ini dimaksudkan agar nasabah dapat terhindar dari kerugian materil dan imateril apabila bertransaksi pada

Bank Digital. Maka sudah sepatutnya *Cyber Security* pada Bank Digital harus diutamakan agar tidak mencederai hak-hak konsumen (nasabah) Bank Digital.

Jika dilihat dari klausul klausul yang tercantum dalam syarat dan ketentuan di aplikasi Bank Digital Aladin Syariah maka Bank Digital Aladin Syariah telah berupaya untuk menerapkan keamanan/*security* dan keselamatan terhadap nasabahnya baik data/informasi pribadi nasabah maupun tentang dana simpanan nasabah. Selain itu dari klausul syarat dan ketentuan Bank Digital Aladin Syariah juga mengandung makna bahwa Bank Menjamin keamanan serta kerahasiaan data/informasi nasabah kecuali diminta oleh pihak yang berwenang sesuai peraturan yang berlaku. Sebagaimana tercantum pada point-point berikut ini :

- "kami menyimpan kerahasiaan dan keamanan data/informasi diri yang anda berikan. Penggunaan data Anda akan kami lakukan dengan mengacu pada bagian Kebijakan Privasi*".*
- "Informasi keamanan berupa email Nasabah, kata sandi, One Time Password (OTP), dan Personal Identification Number (PIN) akan dibutuhkan untuk login, aktivasi perangkat, dan mengeksekusi setiap transaksi yang menurut Bank dibutuhkan sebagai tujuan otentikasi".
- "Bank tidak akan pernah meminta Nasabah memberitahukan kata sandi, OTP, dan PIN kepada Nasabah" .
- "Sesuai ketentuan yang berlaku, Bank wajib merahasiakan data penyimpan dan simpanannya

kecuali diminta oleh pihak yang berwenang sesuai Peraturan Yang Berlaku".

Dari klausul-klausul diatas, penulis menyimpulkan bahwa Bank Digital Aladin syariah telah berupaya dan berkomitmen untuk menjamin kerahasiaan informasi nasabah. Sehingga dapat dikatakan Bank Digital Aladin Syariah telah memenuhi hak-hak konsumen (nasabah) perihal hak perlindungan, keamanan, dan keselamatan dari kejahatan-kejahatan *cyber*.

Dari klausul-klausul yang tercantum dalam syarat dan ketentuan berkaitan dengan komitmen Bank Digital untuk menjamin kerahasiaan informasi dan/atau data nasabah maka Bank Digital Aladin Syariah telah menerapkan prinsip-prinsip Perlindungan Konsumen yaitu prinsip kerahasiaan dan keamanan data/informasi Konsumen sebagaimana yang tertuang dalam pasal 2 bagian d. Peraturan Otoritas Jasa Keuangan Nomor: 1/POJK.07/2013/Tentang Perlindungan Konsumen Sektor Jasa Keuangan.[94]

Klausul-klausul dalam menjamin kerahasiaan informasi/data nasabah pada Bank Digital Aladin Syariah juga telah bersesuaian dengan persyaratan yang harus dipenuhi oleh Bank Digital yang tercantum dalam Peraturan Otoritas Jasa Keuangan Republik Indonesia NOMOR 12 /POJK.03/2021 Tentang Bank Umum pasal 24 ayat 1 bagian e. yang berbunyi "Bank BHI yang

[94] Pasal 2 Peraturan Otoritas Jasa Keuangan Nomor:1/POJK.07/2013 Tentang Perlindungan Konsumen Sektor Jasa Keuangan

beroperasi sebagai Bank Digital sebagaimana dimaksud dalam Pasal 23 ayat (1) harus memenuhi persyaratan: menjalankan perlindungan terhadap keamanan data nasabah".

Sehingga menurut hemat penulis, penerapan *cyber security* pada aplikasi Bank Digital Aladin Syariah telah bersesuaian dengan keamanan yang diamanatkan Undang-Undang No. 8 Tahun 1999 tentang Perlindungan Konsumen hal ini dapat dilihat dari Awal Pembuatan Rekening Digital hingga bertransaksi dan pada klausul klausul klausul yang tercantum dalam syarat dan ketentuan. Bank Digital Aladin Syariah telah berupaya dan berkomitmen untuk menerapkan keamanan/*security* dan keselamatan terhadap nasabahnya agar tidak mencederai asas-asas dan hak-hak perlindungan konsumen sebagaimana diamanatkan dalam Undang-Undang Perlindungan Konsumen, dan beberapa Peraturan Terkait dengan Perlindungan Konsumen dalam hal ini Nasabah.

3. Analisis Cyber Security pada Bank Digital sebagai Upaya Keamanan dan Perlindungan Informasi Transaksi Elektronik

Security (Keamanan) dalam bertransaksi pada Bank Digital merupakan sesuatu yang bertujuan untuk melindungi keutuhan, kerahasiaan dan keteraksesan Informasi Elektronik dalam Penyelenggaraan Sistem Elektronik. Sebagaimana yang tertuang dalam pasal 16 ayat (1) point b. Pada Undang-Undang Nomor 11 Tahun 2008 jo. Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik yang berbunyi :

"Setiap penyelenggara Sistem Elektronik wajib mengoperasikan Sistem Elektronik yang memenuhi persyaratan minimum yaitu dapat melindungi ketersediaan, keutuhan, keotentikan, kerahasiaan, dan keteraksesan Informasi Elektronik dalam Penyelenggaraan Sistem Elektronik tersebut". [95]

Lebih lanjut ditekankan pada pasal 15 ayat 1 Undang Undang ITE bahwa Bank Digital yaitu sebagai Penyelenggara Sistem Elektronik diharuskan untuk melakukan sistem elektronik yang aman.

"Setiap Penyelenggara Sistem Elektronik harus menyelenggarakan Sistem Elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya Sistem Elektronik sebagaimana mestinya."

Konsep Keamanan (*Security*) yang harus diterapkan pada Bank Digital juga eksplisit tertuang dalam Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik dalam pasal 4 yang berbunyi:

"Sepanjang tidak ditentukan lain oleh undang-undang tersendiri, setiap Penyelenggara Sistem Elektronik wajib mengoperasikan Sistem Elektronik yang memenuhi persyaratan minimum sebagai berikut: dapat melindungi ketersediaan, keutuhan, keotentikan, kerahasiaan, dan keteraksesan Informasi Elektronik dalam penyelenggaraan Sistem Elektronik tersebut;"

[95] Undang-Undang No. 11 Tahun 2008 jo. Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik

Jika dilihat dari proses awal pembukaan rekening pada Bank Digital di aplikasi Aladin Syariah dengan menggunakan E-mail, Bank Digital untuk membuktikan bahwa email yang dikirimkan adalah benar data pribadi orang yang bersangkutan maka ini diatur dalam prinsip pembuktian adanya hak. Prinsip ini diimplementasikan dalam Pasal 7 UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yaitu:

*"*Setiap Orang yang menyatakan hak, memperkuat hak yang telah ada, atau menolak hak Orang lain berdasarkan adanya Informasi Elektronik dan/atau Dokumen Elektronik harus memastikan bahwa Informasi Elektronik dan/atau Dokumen Elektronik yang ada padanya berasal dari Sistem Elektronik yang memenuhi syarat berdasarkan Peraturan Perundang-undangan".

Pada tahap awal pembukaan rekening pada Bank Digital di aplikasi Aladin Syariah dengan menggunakan kode OTP. Perihal penyalahgunaan kode OTP atau terjadinya penipuan maka Undang-Undang ITE pasal 28 ayat (1) UU ITE jo. Pasal 45A ayat (1) perubahan ITE yang berbunyi :

"Setiap orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda

paling banyak Rp1.000.000.000,00 (satu miliar rupiah).”[96]

Dari klausul klausul syarat dan Ketentuan Bank Digital Aladin Syariah telah berupaya untuk menerapkan keamanan/*security* dan keselamatan terhadap nasabahnya baik data/informasi pribadi nasabah maupun tentang dana simpanan nasabah. Dari klausul syarat dan ketentuan Bank Digital Aladin Syariah juga mengandung makna bahwa Bank Menjamin keamanan serta kerahasiaan nasabah kecuali diminta oleh pihak yang berwenang sesuai peraturan yang berlaku. Hal ini bersesuaian dengan Undang-Undang ITE bahwa bank Bank Digital (Aladin Syariah) sebagai penyelenggara Sistem Elektronik telah memenuhi persyaratan minimum dalam mengoperasikan Bank Digital tersebut.

Dari klausul-klausul syarat dan ketentuan Bank Digital Aladin Syariah juga mengandung makna bank telah menerapkan manajemen keamanan data dan informasi (baik elektronik dan *hard copy*) dan memastikan bahwa informasi dan dokumen dikelola sesuai dengan strategi risiko organisasi untuk melindungi kerahasiaan, integritas, dan ketersediaan informasi. Sebagaimana yang tertuang dalam *Consultative Paper* Manajemen Risiko Keamanan Siber Bank Umum halaman 31 point 79.

Kriteria perlindungan terkait kerahasiaan, integritas, dan ketersediaan informasi merupakan kriteria

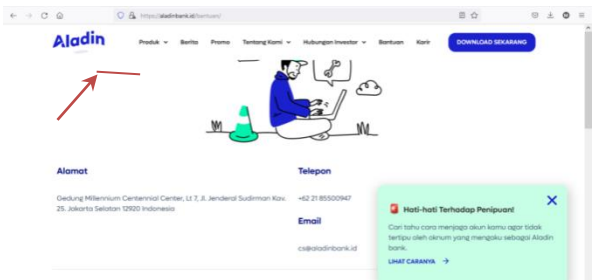
[96] Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, pasal 45 ayat 1.

istilah “aman” dalam konsep kriptografi. Kriptografi merupakan Ilmu yang mempelajari bagaimana cara penyampaian pesan dari pengirim kepada penerima secara aman. Yang hal ini diartikan bahwa penyampaian pesan dari nasabah (baik terkait pembukaan rekening maupun transaksi pada Bank Digital) kepada penerima pesan yaitu Bank Digital. Dalam rangka mencapai tujuan tersebut secara teknis pengamanan/*security* nya dapat berupa :

a. *Secure Sockets Layer* (SSL)

Penggunaan http:// pada internet merupakan bentuk aplikasi level protokol yang keberadaannya dinilai tidak aman. Karena itu fungsi utama SSL ialah untuk mengamankan jaringan komunikasi antara browser dengan web server. Dan setelah dilengkapi dengan fasilitas ini, http:// akan berubah menjadi https:// dan terlihat tanda gembok pada bagian kanan bawah. [97]

Pada aplikasi Bank Aladin Syariah dalam Transaksi Elektroniknya telah menggunakan sistem SSL hal ini dapat dicermati pada gambar berikut ini :



Gambar 4.16

[97] Burhanuddin, *Pemikiran Hukum Perlindungan Konsumen & Sertifikasi Halal*, (Malang: UIN Maliki Press, 2011), hlm 133.

b. *Secure Electronic Transaction* (SET)

Pada skenario SET, pihak-pihak yang bertransaksi via internet, menggunakan sertifikat digital yang dibuat oleh *Certificate authority* (CA). Masing-masing akan memberikan informasi jati dirinya kepada CA yang akan memeriksa keaslian jati diri mereka, sebelum mengesahkan sertifikat digital. [98]

Di dalam sertifikat digital, tercantum informasi pemilik kunci publik (*public key*) yang otentik dan informasi CA sebagai penerbit sertifikat. Pasangan kunci publik dan kunci privat (private key) dipakai untuk melakukan tanda tangan digital dan *secure communication* melalui https atau email dengan sistem enkripsi asimetrik. *Private key* inilah yang berperan sebagai pembuat tanda tangan digital. Dokumen yang dibubuhi dengan tanda tangan digital dapat diidentifikasi kepemilikannya oleh CA dan dijamin integritasnya.

Sesuai Undang Undang ITE pasal 11, tanda tangan digital memiliki kekuatan hukum dan akibat hukum yang sah pada dokumen elektronik.

Pada Aplikasi Bank Digital Aladin Syariah telah menggunakan *Secure Electronic Transaction* (SET) yang artinya Bank Digital Aladin Syariah telah memiliki sertifikat elektronik. Sertifikasi elektronik ini merupakan dokumen yang harus dipenuhi pada Permohonan persetujuan produk Layanan Perbankan Elektronik dalam pasal 5 bagian c Peraturan Otoritas Jasa Keuangan Nomor

[98] Burhanuddin, hlm. 134.

12 /POJK.03/2018 Tentang Penyelenggaraan Layanan Perbankan Digital Oleh Bank Umum.

C. Analisis Cyber Security pada Bank Digital menurut Hukum Ekonomi Syariah

Dalam Hukum Ekonomi Syariah yang kaitannya dengan dunia digitalisasi keharusan adanya *Security* dalam penggunaan internet untuk menangkal serangan dan ancaman dari dunia *Cyber* belum ada ayat Alquran, Sunnah dan Ijma' yang secara jelas menerangkan perihal tersebut. Sehingga untuk menjabarkan *Cyber Security* dalam perspektif Hukum Ekonomi Syariah diperlukan adanya Kaidah-kaidah Fiqh yang berkaitan dengan Keamanan (*Security).*

Perkembangan Ilmu dan Teknologi, serta tuntutan masyarakat yang semakin meningkat, melahirkan model-model transaksi baru yang membutuhkan penyelesaiannya dari sisi hukum Islam. Penyelesaian yang disatu sisi tetap Islami dan disisi lain mampu menyelesaikan masalah kehidupan yanng nyata. Caranya yaitu sudah tentu dengan menggunakan Kaidah-Kaidah Fikih dibidang Muamalah.

Kaidah-kaidah fiqh lahir dari Al-Qur'an, al-hadits, dan ijma'. Kaidah-kaidah fiqih lahir dengan tujuan menetapkan hukum Islam dalam persoalan-persoalan baru yang terus berkembang seiring perkembangan zaman, terkhusus dalam transaksi ekonomi atau *muamalah maliyah* yang senantiasa berkembang di lembaga keuangan syariah. Dengan demikian kaidah-kaidah fiqh merupakan produk ijtihad dan merupakan generalisasi dari tema-tema fiqh yang tersebar di kalangan ulama mazhab. Adanya kaidah-kaidah fiqh merupakan suatu keharusan untuk memperoleh kemudahan mengetahui

hukum-hukum kontemporer terkhusus persoalan ekonomi yang banyak tidak memiliki *nash sharîh* (dalil pasti) dalam Al-Qur'an maupun hadits. Begitu pula untuk mempermudah menguasai permasalahan *furu'iyah* (cabang) yang terus berkembang dan tidak terhitung jumlahnya terkhusus dalam persoalan ekonomi yang berkembang di lembaga keuangan syariah.

1. **Cyber Security pada Bank Digital sebagai Produk Muamalah Kontemporer**

   Bank Digital merupakan Bank yang melakukan layanan jasa berbasis digital yang kemunculannya adalah *impact* dari kemajuan dan kecanggihan teknologi. Sebagaimana disebutkan Bank Digital menurut Arwin Rasyid, bank digital adalah bank yang tumbuh melakukan pelayanan jasa keuangan yang berdasarkan teknologi sehingga tidak perlu lagi ada kantor cabang.[99]

   Layanan berbasis Teknologi memang sebuah solusi dan memberikan dampak positif bagi masyarakat apalagi pada saat pandemi COVID-19 untuk mengurangi angka penularan. Namun disisi lain tidak semua orang tingkat Literasi Digitalnya tinggi bahkan yang lebih penting layanan berbasis teknologi harus diimbangi dengan mitigasi kejahatan siber dari

[99] Daniel Deha, *Banking Everywhere: Neobank dan Sejarah Bank Digital* (https://www.trenasia.com/banking-everywhere-neobank-dan-sejarah-bank-digital-part-3-habis diakses tanggal 04 Juni 2022, Pukul 13:55 WITA).

Bank Digital itu sendiri yaitu dengan adanya *cyber security*.

Bank Digital yang hadir di Indonesia sejak tahun 2016 silam, tidak dapat diindahkan dengan ancaman kejahatan siber. Bank tradisional yang memiliki layanan *digital banking* saja sudah sangat rentan terhadap *cyber crime*, apalagi dengan Bank digital yang layanannya *fully* digital. Sehingga sangat diperlukan adanya *cyber security* yang dapat mencegah dan meminimalisir ancaman kejahatan siber pada Bank Digital.

Perbedaan mendasar antara bank digital dan konvensional terletak di wujudnya. Bank konvensional memiliki wujud fisik berupa kantor cabang, sedangkan bank digital tidak memiliki kantor cabang. Cukup dengan berbekalkan sebuah smartphone, kita sudah bisa melakukan aneka transaksi perbankan pada bank digital.

Sebagaimana pada umumnya, Bank Digital dan *Cyber security* merupakan salah satu bentuk kegiatan yang termasuk dalam kajian muamalah. Dikarenakan Bank Digital dan *Cyber security* sama-sama memiliki kebermanfaatan bagi kehidupan manusia. Bank Digital memiliki manfaat untuk kemudahan dan kecepatan kapanpun dan dimanapun dalam bertransaksi perbankan dibanding perbankan tradisional, sedangkan *Cyber Security* memiliki manfaat sebagai penjamin keamanan jika bertransaksi melalui saluran digital. Hal ini sejalan dengan pengertian Muamalah menurut Hudhari Bek yaitu

"Muamalah adalah semua akad yang membolehkan manusia saling bertukar manfaat". Juga sejalan dengan pengertian Muamalah menurut Rasyid Ridha yaitu "Muamalah adalah tukar menukar barang atau sesuatu yang bermanfaat dengan cara-cara yang telah ditentukan".[100]

Pada dasarnya segala kegiatan muamalah itu diperbolehkan hingga ada dalil yang melarangnya. Sebagaimana kaidah fiqh:

الْأَصْلُ فِي الْمُعَامَلَاتِ الْإِبَاحَةِ اِلاَّ اَنْ يَدُلَّ دَلِيْلٌ عَلَى تَحْرِيْمِهَا

"Pada dasarnya segala bentuk muamalah adalah boleh, kecuali ada dalil yang mengharamkannya".[101]

Maksud kaidah ini adalah bahwa dalam setiap muamalah dan transaksi pada dasarnya boleh, seperti jual beli, sewa menyewa, gadai, kerja sama (*mudharabah* atau *musyarakah*), perwakilan, dan lain-lain. Kecuali yang tegas diharamkan seperti mengakibatkan kemudaratan, tipuan, judi dan riba.[102]

---

[100] Hendi Suhendi, *Fiqh Muamalah*, (Jakarta : PT Raja Grafindo Persada, 2011). hlm. 2.

[101] Ibnu Taimiyah, *al-Qawa'id al-Nuraniyah al-fiqhiyyah*, Riyadh : Maktabah al-Rusyd, cet. I, Juz II, hlm. 306.

[102] A. Djazuli, *Kaidah-Kaidah Fikih Kaidah-Kaidah Hukum Islam Dalam Menyelesaikan Masalah-Masalah Yang Praktis* (Jakarta: Kencana, 2007), Hlm. 130.

Dalil dari Kaidah Fikih ini adalah Al-Qur'an Surah Al-Mâ'idah/5: 87.

"Wahai orang-orang yang beriman, janganlah kamu mengharamkan sesuatu yang baik yang telah Allah halalkan bagi kamu, dan janganlah kamu melampaui batas. Sesungguhnya Allah tidak menyukai orang-orang yang melampaui batas."[103]

Menurut Kamus Ushul Fiqh kata الْأَصْلُ memiliki makna sebagai berikut:

1. Perkara yang hukumnya dijelaskan dalam *nash* atau *Ijma'*.
2. *Nash* yang berkaitan dengan ketentuan pada kasus yang bersangkutan.
3. Peristiwa hukum yang hendak dijadikan rujukan penyamaan dengan peristiwa hukum lainnya.
4. Ketentuan yang berlaku pada sesuatu, sebelum

يٰٓاَيُّهَا الَّذِيْنَ اٰمَنُوْا لَا تُحَرِّمُوْا طَيِّبٰتِ مَآ اَحَلَّ اللّٰهُ لَكُمْ وَلَا تَعْتَدُوْا ۗاِنَّ اللّٰهَ لَا يُحِبُّ الْمُعْتَدِيْنَ

berlakunya hukum *syara'*. Sebuah *statement* berbunyi: "*Ketentuan umum pada sebuah pembicaraan adalah, memahaminya secara hakiki";* juga "*ketentuan umum pada suatu tindakan adalah boleh"*, artinya semua perbuatan

[103] Kementerian Agama Republik Indonesia, *Quran Kemenag* (https://quran.kemenag.go.id/surah/5/87) diakses tanggal 25 Juni 2022.

adalah boleh selagi belum ada dalil pencegahnya.[104]

Masalah muamalah senantiasa berkembang di dalam kehidupan masyarakat. Salah satu bidang kajian muamalah yaitu dibidang perbankan yang saat ini telah berkembang ke arah Digitalisasi atau yang disebut dengan Bank Digital. Merujuk pada kaidah prinsip kegiatan muamalah maka hukum asalnya adalah boleh*"*. **Setiap muslim diberikan kebebasan untuk melakukan aktivitas-aktivitas ekonomi dan mengembangkannya serta menyesuaikannya dengan perkembangan zaman selama tidak ada unsur-unsur transaksi terlarang yang terdapat di dalamnya**, karena itu sifat fleksibel dan dinamis melekat pada perkara muamalah. Hal ini dapat dipersamakan bahwa *Cyber Security* pada Bank Digital merupakan suatu tindakan/aktivitas yang diperbolehkan karena hingga hari ini tidak ditemukan unsur-unsur terlarang sebagaimana menjadi larangan dalam dalil-dalil hukum Islam, kecuali jika dalam praktik *Cyber Security* pada Bank Digital terdapat hal-hal yang bertentangan dengan hukum syara' atau bentuk aktivitas yang mengandung unsur-unsur yang dilarang.

Penyebab dilarangnya suatu transaksi adalah disebabkan karena faktor-faktor : (1) haram zatnya (haram *li-dzatihi)*; (2) haram selain zatnya

[104] H.Jaenal Aripin, *Kamus Ushul Fiqh Dalam Dua Bingkai Ijtihad*, (Kencana Prenada Media Group : Jakarta, 2012) hlm. 22.

(haram *li ghairihi*); dan (3) tidak sah atau tidak lengkap akadnya.

Transaksi yang tergolong ke dalam transaksi haram zatnya adalah transaksi dilarang karena objek (barang dan/atau jasa) yang ditransaksikan dilarang.[105] Seperti memperjualbelikan alkohol, narkoba, organ manusia, dan lain-lain. Jika dalam praktik *cyber security* pada Bank Digital untuk melindungi keamanan dan kelancaran jasa yang mengarah kepada kejahatan maka sudah tentu *cyber security* termasuk dalam aktivitas yang diharamkan pula.

Transaksi yang tergolong ke dalam transaksi haram selain zatnya yakni karena transaksi tersebut melanggar prinsip *'an taradin minkum* yaitu unsur keridhaan di antara para pihak.[106] Maksudnya adalah jika dalam praktik *cyber security* pada Bank Digital terdapat unsur kezhaliman, penipuan, pemaksaan dan hal-hal lain yang merugikan para pihak seperti aktivitas keinginan mencuri data/informasi nasabah dari para pegawai/karyawan bank maka praktik Bank Digital tergolong dalam transaksi haram selain zatnya.

Transaksi yang tidak sah atau tidak lengkap akadnya akan menyebabkan dilarangnya suatu transaksi. Akad yang tidak sah atau tidak lengkap berarti akadnya tidak shahih dan mengandung makna

[105] Fathurrahman Azhari, *Qawaid Fiqhiyyah Muamalah* (Banjarmasin, LKPD, 2015) hlm. 137.

[106] Fathurrahman Azhari, hlm. 138.

terdapat kekurangan rukun dan syaratnya maupun dalam prinsipnya. Seperti jika dalam klausul akad praktik Bank Digital, Bank tidak menyebutkan untuk menjamin kerahasiaan data nasabah maka Bank Digital mencederai Prinsip amanah /kejujuran pada prinsip-prinsip Akad.

Para fuqaha menerangkan secara umum faktor penyebab muamalah yang diharamkan yaitu sebagai berikut : Faktor kezhaliman, Faktor Gharar (penipuan), Faktor Riba, Faktor Risywah (Suap), Perjudian dan ketidakabsahan akad.

Menurut Fathurrahman Azhari Apabila praktik muamalat di dalamnya mengandung kezaliman terhadap salah satu pihak atau pihak manapun, maka muamalah itu menjadi diharamkan. Berdasarkan firman Allah pada surah An-Nisâ'/4: 29.

يٰٓاَيُّهَا الَّذِيْنَ اٰمَنُوْا لَا تَأْكُلُوْٓا اَمْوَالَكُمْ بَيْنَكُمْ بِالْبَاطِلِ اِلَّآ اَنْ تَكُوْنَ تِجَارَةً عَنْ تَرَاضٍ مِّنْكُمْ ۗ وَلَا تَقْتُلُوْٓا اَنْفُسَكُمْ ۗ اِنَّ اللّٰهَ كَانَ بِكُمْ رَحِيْمًا

"Wahai orang-orang yang beriman, janganlah kamu memakan harta sesamamu dengan cara yang batil (tidak benar), kecuali berupa perniagaan atas dasar suka sama suka di antara kamu. Janganlah kamu membunuh dirimu. Sesungguhnya Allah adalah Maha Penyayang kepadamu."[107]

[107] Kementrian Agama Republik Indonesia, *Quran*

Kezaliman itu meniadakan unsur suka sama suka atau rela sama rela dan termasuk juga memakan harta orang lain dengan jalan yang batil.[108] Jika dalam praktik Bank Digital terjadi kejahatan siber seperti pencurian dan peretasan yang dilakukan oleh hacker maka hal ini akan menimbulkan kezaliman, karena praktik *cyber crime* bukan hanya tidak disukai dari pihak nasabah maupun pihak bank tetapi juga menimbulkan kerugian kepada kedua belah pihak.

Cyber security pada Bank Digital secara implisit memberikan jaminan keamanan terhadap nasabah/konsumen/masyarakat dari serangan kejahatan siber. Hal ini dapat disimpulkan bahwa Praktik *cyber* security pada Bank Digital tidak memiliki tujuan untuk hal-hal yang mengarah kepada kezaliman, justru dengan adanya *cyber security* unsur kezaliman yang disebabkan karena kejahatan siber (*cyber crime*) dapat diminimalisir dan dicegah oleh Bank Digital.

2. Cyber Security pada Bank Digital sebagai Upaya Preventif dan Perlindungan terhadap Tindak Kejahatan

Dengan adanya *cyber security* pada Bank Digital, maka sebuah Bank Digital dalam operasionalnya memiliki sebuah jaminan perlindungan dan keamanan kepada nasabahnya

---

Kemenag, (https://quran.kemenag.go.id/surah/4/29) diakses tanggal 26 Juni 2022 pukul 13.00.

[108] Fathurrahman Azhari, *Qawaid Fiqhiyyah Muamalah*, hlm. 138-139.

dari serangan siber. Sehingga transaksi pada Bank Digital dapat memberikan manfaat maksimal kepada nasabahnya. Dalam perbuatan muamalah yang di dalamnya mengandung manfaat maka adalah halal dan yang mengandung bahaya adalah haram. Sebagaimana kaidah fiqh:

الْاَصْلُ فِى الْمَنَافِعِ الْحِلِ, وَالْمَضَارُّ الْحُرْمَةُ بِاَدِلَّةٍ شَرْعِيَّة

"Pada dasarnya segala yang bermanfaat adalah halal, dan yang membahayakan adalah haram dengan petunjuk syariat"[109]

Tanpa adanya *cyber security* maka Bank Digital akan menghadapi sebuah bahaya atau ancaman dan serangan kejahatan siber. Tidak jarang akibat serangan tersebut sejumlah nyawa manusia melayang. Sebagaimana kaidah fiqh bahwa segala sesuatu yang menyebabkan terjadinya bahaya maka adalah haram dan harus dihilangkan.

كُلُ مَا أَدَّى اِلَى ضَرَرٍ مُحَقِّقٍ فَهُوَ حَرَامٌ

"Segala apa yang menyebabkan terjadinya kemudharatan (bahaya) maka hukumnya haram."

Kaidah fiqh ini mengandung makna secara implisit bahwa jika Bank Digital tidak menerapkan *cyber security* dalam praktik operasionalnya maka akan muncul terjadinya kemudharatan bagi Bank Digital maupun nasabahnya, dan operasionalnya pun harusnya dapat dihentikan.

[109] Fathurrahman Azhari, hlm.160.

Menjadi rekomendasi kepada pihak Otoritas Jasa Keuangan (OJK) yang meloloskan dan membolehkan Bank Digital beroperasi bahwa harus memiliki sistem *cyber security* yang telah lulus uji dan sesuai standar minimal yang ditetapkan baik standar *cyber security* di dunia maupun Indonesia agar tidak terjadi hal-hal yang akan merugikan nasabah di kemudian hari. Saat ini Indonesia telah memiliki acuan standar minimal yang harus dipenuhi oleh Bank dalam menerapkan manajemen risiko keamanan siber yang tertuang dalam *Consultative Paper Manajemen Risiko Keamanan Siber Bank Umum*. *Consultative paper* ini memuat konsep dasar keamanan siber, uraian mengenai standar penerapan manajemen risiko keamanan siber.

Jika sebuah Bank Digital belum dapat menerapkan *cyber security* sesuai dengan standar minimal manajemen risiko keamanan siber, maka seharusnya dari pihak OJK bisa saja menghentikan operasionalnya Bank Digital hingga Bank Digital tersebut dapat menerapkan sesuai dengan standar keamanan siber yang telah ditetapkan. Apabila bertransaksi di Bank Digital hukumnya adalah boleh dan akan mendatangkan berbagai kemaslahatan seperti kemudahan, kenyamanan bertransaksi bisa dimana saja dan berbagai fitur yang dapat dimanfaatkan untuk kehidupan ekonomi sehari-hari, namun jika mengandung mafsadat (ancaman *Cyber*) maka Bank Digital harus mendahulukan keamanan untuk terhindar ancaman kejahatan siber yaitu dengan mengutamakan *Cyber Security*. Hal ini bertujuan untuk mencegah adanya *cyber crime* pada Bank Digital.

Cyber crime atau kejahatan siber merupakan bahaya yang ancaman dan serangannya harus dicegah dibanding mendahulukan kenyamanan dan kemudahan dalam bertransaksi perbankan. Hal ini bersesuaian dengan kaidah fiqh bahwa mencegah bahaya itu lebih diutamakan dibanding mendahulukan kemaslahatan yaitu:

دَرْءُ الْمَفَاسِدِ أَوْلَى مِنْ جَلْبِ الْمَصَالِحِ

"Mencegah kemudharatan itu lebih utama daripada menarik datangnya kemaslahatan".[110]

Sebagaimana diketahui bahwa ancaman *cyber crime* atau kejahatan siber pada sektor perbankan lebih rentan daripada lembaga lainnya apalagi jika tidak diterapkannya upaya-upaya *cyber security*. Ancaman dan bahaya serangan dari *cyber crime* merupakan hal yang akan mendatangkan kemudharatan bagi kehidupan manusia yang harus dihilangkan. Dalam kaidah fiqh berkaitan dengan "kemudaratan harus dihilangkan" sebagaimana berbunyi:

الضرار يزال

Arti dari kaidah ini menunjukan bahwa kemudaratan itu telah terjadi dan akan terjadi. Apabila demikian halnya maka wajib untuk dihilangkan.[111] Menurut Muhammad al-Zarqa dalam kitabnya *Syarh al-Qawa'id al-Fiqhiyyah*, kaidah fiqh "al-dhâraru yuzâlu" menunjukkan bahwa menghilangkan kemudaratan adalah wajib.

[110] Fathurrahman Azhari, hlm.109.

[111] Abdul Mujib, *Kaidah-Kaidah Ilmu Fiqih* (Jakarta: Kalam Mulia, 2013) hlm.34.

Dasar hukum kaidah fiqh ini adalah penggalan Qur'an surah Al-A'Râf/7: 56.

وَلَا تُفْسِدُوْا فِى الْاَرْضِ

"Janganlah kamu berbuat kerusakan di bumi....".[112]

Dan hadits Nabi Muhammad SAW yang berbunyi:

لا ضَرَرَ ولا ضِرارَ

*"*Tidak boleh membuat kemudaratan pada diri sendiri dan membuat kemudaratan pada orang lain.*"* (HR Ibnu Majah No. 2340, shahih)

Secara etimologi, al-dharar (الضرر) adalah membahayakan orang lain secara mutlak, sedangkan al-dhirar (الضرار) adalah membahayakan orang lain dengan cara yang tidak disyariatkan. Sedangkan *Dharar* secara terminologi adalah kesulitan yang sangat menentukan eksistensi manusia, karena jika ia tidak diselesaikan maka akan mengancam agama, jiwa, nasab, harta serta kehormatan manusia. [113]

Menurut al-Syatibi, Islam melarang seseorang berbuat sesuatu yang dapat memudaratkan diri sendiri maupun orang lain. Islam juga melarang seseorang membunuh jiwa, merusak akal, mengganggu keturunan, merusak harta, mengganggu kehormatan, melakukan

[112] Kementerian Agama Republik Indonesia, *Quran Kemenag* (https://quran.kemenag.go.id/surah/7/56) diakses tanggal 27 Juni 2022 pukul 19.30.

[113]Fathurrahman Azhari, *Qawaid Fiqhiyyah Muamalah*, hlm. 100.

penganiayaan serta setiap perbuatan yang memudaratkan diri sendiri maupun orang lain.[114]

Kaidah fiqh ini kembali kepada tujuan untuk merealisasikan *maqāşid al-syarī'at* dengan menolak kemafsadatan, yaitu menghilangkan kemudharatan atau meringankannya.

Ancaman Kejahatan siber/*cyber* crime merupakan kejahatan yang akan menimbulkan banyak permasalahan atau kemudharatan untuk berbagai pihak terutama nasabah. *Dharar* yang kaitannya dengan *cyber crime* tentu akan mengancam keamanan data/informasi dan harta nasabah bahkan dari pihak bank. Walaupun konsep *cyber security* tidak menjamin 100% dapat menangkal serangan kejahatan siber namun setidaknya *cyber security* pada Bank Digital dapat meminimalisir dan harapannya menghilangkan kejahatan siber tersebut agar nasabah merasa aman dalam bertransaksi di Bank Digital. Sebagaimana kaidah fiqh yang berbunyi:

اَلضَّرَرُ يُدْفَعُ عَلَى قَدرِ الْإِمْكَانِ

"Kemudharatan dihilangkan semaksimal mungkin meskipun tidak seluruhnya hilang".[115]

Ini merupakan kaidah yang penting terutama dalam masalah nahi mungkar, karena di antara bentuk

[114] Ade Dedi Rohayana, *Ilmu Qawa'id Fiqhiyyah Kaidah-Kaidah Hukum Islam* (Jakarta: Gaya Media Pratama, 2008) hlm. 215.

[115] A.Djazuli, *Kaidah-Kaidah Fikih Kaidah-Kaidah Hukum Islam dalam Menyelesaikan Masalah-Masalah yang Praktis* (Jakarta: Kencana, 2007). Hlm. 73.

kemudaratan adalah kemungkaran. Patut diketahui bahwa nahi mungkar ada dua bentuk, pertama nahi munkar untuk menghilangkan kemungkaran secara total, kedua nahi munkar dengan cara meminimalkan kemungkaran tersebut. Bahkan dalam beberapa kondisi, perbuatan nahi munkar itu sendiri mengandung kemungkaran, tetapi itu dilakukan demi menghilangkan kemungkaran yang lebih besar darinya.

Diantara dalil kaidah ini, Allah berfirman dalam Qur'an Surah At-Tagâbun/64: 16.

فَاتَّقُوا اللّٰهَ مَا اسْتَطَعْتُمْ وَاسْمَعُوْا وَاَطِيْعُوْا وَاَنْفِقُوْا خَيْرًا لِّاَنْفُسِكُمْۗ وَمَنْ يُّوْقَ شُحَّ نَفْسِهٖ فَاُولٰۤىِٕكَ هُمُ الْمُفْلِحُوْنَ

"Bertakwalah kamu kepada Allah sekuat kemampuanmu! Dengarkanlah, taatlah, dan infakkanlah harta yang baik untuk dirimu! Siapa yang dijaga dirinya dari kekikiran, mereka itulah orang-orang yang beruntung". [116]

Dan dalil dari hadits Nabi adalah:

"Barangsiapa di antara kalian melihat kemungkaran, hendaklah dia merubahnya dengan tangannya. Apabila tidak mampu, hendaklah dia merubah hal itu dengan lisannya. Apabila tidak mampu lagi, hendaknya dia ingkari dengan hatinya dan inilah selemah-lemah iman." (HR Muslim No. 49)

[116] Kementerian Agama Republik Indonesia, *Quran Kemenag*, (https://quran.kemenag.go.id/surah/64/16) diakses tanggal 27 Juni 2022 Pukul 20.00.

Diantara contoh penerapan kaidah ini adalah seperti Nabi Yusuf yang menjadi bendahara negeri Mesir padahal negeri Mesir saat itu adalah negeri kafir. Namun Nabi Yusuf masuk ke dalam sistem kafir tersebut untuk mengurangi kemudaratan negeri tersebut walaupun tidak akan seluruhnya hilang. Demikian pula di zaman sekarang, berkaitan dengan keamanan dalam hal *Cyber* pada aplikasi perbankan digital walaupun perihal *cybercrime* selalu lebih unggul dibanding *cyber security* namun setidaknya usaha-usaha pada aplikasi perbankan digital seperti keamanan dari tahap awal verifikasi data dan klausula-klausula pada syarat dan ketentuan sebelum bertransaksi di aplikasi bank digital bisa menjadi *tameng* awal untuk mengurangi ancaman serangan *cyber crime*.

Walaupun *Cyber Security* tidak secara eksplisit disebutkan dalam Alquran dan Sunnah. Namun praktik dan prinsip *Security* atau keamanan secara tersirat terkandung di dalamnya seperti contoh tentang kisah Zulkarnain dengan Ya'juj dan Ma'juj. Pada saat itu Zulkarnain diminta untuk membangun sebuah dinding tinggi dan tebal yang tidak dapat ditembus oleh Ya'juj dan Ma'juj untuk melindungi kaumnya dari kejahatan mereka. Zulkarnain pun kemudian membangun sebuah dinding yang terbuat dari bahan tembaga dan besi panas. Dinding tersebut digunakan untuk memenuhi kebutuhan kaum yang membutuhkan keamanan tersebut. Kisah tersebut tersirat dalam Qur'an Surah Al-Kahfi ayat 94-98.

Konsep dinding tembaga dan besi panas tersebut kemudian dapat diadopsi dalam dunia digitalisasi yang populer dengan sebutan *Cyber Security* (Keamanan Siber). Fungsi *Security* ini tidak lain adalah untuk

menangkal adanya serangan *Cyber Crime* seperti pengaksesan dari pihak-pihak yang tidak dikehendaki terhadap data maupun aplikasi perbankan seseorang.[117]

Security (Keamanan) menurut Hukum Islam juga berkaitan dengan Asas Keamanan dan Keselamatan, dalam hukum Islam ada lima hal yang wajib dijaga dan dipelihara *(al-dharuriyyat alkhamsah*), yaitu: (1) memelihara agama (*hifdh al-din*), (2) memelihara jiwa (*hifdh al-nafs*), (3) memelihara akal (*hifdh al-aql*), (4) memelihara keturunan (*hifdh nasl*), dan memelihara harta (*hifdh al-maal*).[118] Jika ditelaah dari proses awal hingga dalam bertransaksi praktik *cyber security* yang diterapkan pada bank digital telah mengaplikasikan dan memelihara dari *al-dharuriyyat alkhamsa.*

[117] Soediro, "*Prinsip Keamanan, Privasi, dan Etika dalam Undang-Undang Informasi dan Transaksi Elektronik dalam Perspektif Hukum Islam*", Jurnal Kosmik Hukum, Edisi No.2 Vol. 18, Fakultas Hukum Universitas Muhammadiyah Purwokerto, 2018, hlm. 102

[118] Nurhalis, *Perlindungan Konsumen Dalam Perspektif Hukum Islam Dan Undang-Undang Nomor 8 Tahun 1999*, (Jurnal Kajian Hukum dan Keadilan Institut Agama Islam Hamzanwadi (IAIH) NW Lombok Timur, 2015) hlm. 529.

Daftar Pustaka

Buku

A. Djazuli, *Kaidah-Kaidah Fikih Kaidah-Kaidah Hukum Islam Dalam Menyelesaikan Masalah-Masalah Yang Praktis* (Jakarta: Kencana, 2007), Hlm. 130.

A. Qodri Azizy, *Eklektisisme Hukum Nasional*, Cet. ke-1 (Yogyakarta: Gama Media, 2002). hlm. 177

A.Djazuli, *Kaidah-Kaidah Fikih Kaidah-Kaidah Hukum Islam dalam Menyelesaikan Masalah-Masalah yang Praktis* (Jakarta: Kencana, 2007). Hlm. 73.

A.Djazuli, *Kaidah-Kaidah Fikih Kaidah-Kaidah Hukum Islam dalam Menyelesaikan Masalah-Masalah yang Praktis* (Jakarta: Kencana, 2007). Hlm. 73.

Abdoel Djamali, *Pengantar Hukum Indonesia*, (Jakarta: PT. Raja Grafindo Persada, 2005), hal.3

Abdul Mujib, Kaidah-Kaidah 'Ilmu Fiqh, (Jakarta: Kalam Mulia, 2005), hlm 61.

Abdul Mujib, *Kaidah-Kaidah Ilmu Fiqih* (Jakarta: Kalam Mulia, 2013) hlm.34.

Abdullah bin Sa'id Muhammad al-Lahji al-Hadrami, *Idah al-Qawa'id al-Fiqhiyyah*, (Surabaya: Hidayah. 1410H) hlm. 10.

Ade Dedi Rohayana, *Ilmu Qawa'id Fiqhiyyah Kaidah-Kaidah Hukum Islam* (Jakarta: Gaya Media Pratama, 2008)

Ade Dedi Rohayana, *Ilmu Qawa'id Fiqhiyyah Kaidah-Kaidah Hukum Islam* (Jakarta: Gaya Media Pratama, 2008) hlm. 215.

Ahmad Sarwat, Qiyas Sumber Hukum Syariah Keempat (Jakarta: Rumah Fiqh Publishing, 2019). hlm. 13

Aulia Muthiah, *Hukum Perlindungan Konsumen Dimensi Hukum Positif dan Ekonomi Syariah*, (Yogyakarta: Pustaka Baru Press, 2018) hlm.42-43.

Bank dan Lembaga Keuangan Lainnya (Jakarta: Raja Grafindo Persada 2012). hlm.43.

Burhanuddin, *Pemikiran Hukum Perlindungan Konsumen & Sertifikasi Halal*, (Malang: UIN Maliki Press, 2011), hlm 133.

Departemen Penelitian dan Pengaturan Perbankan Otoritas Jasa Keuangan, *Consultative Paper Manajemen Risiko Keamanan Siber Bank Umum*, 2021 hlm. 34.

Deris Setiawan, *Sistem Keamanan Komputer*, (Jakarta: PT Elex Media Komputindo, 2005). Hlm. 40

Eko Listiyani, *Kepastian Hukum Data Pribadi Terkait One Time Password (OTP) Dalam Penggunaan Media Elektronik* (UIN Surabaya: 2019), 22.

Fathurrahman Azhari, *Qawaid Fiqhiyyah Muamalah* (Banjarmasin, LKPD, 2015) hlm. 137.

Fathurrahman Azhari, *Qawaid Fiqhiyyah Muamalah* (Banjarmasin, LKPD, 2015) hlm. 109.

H.Jaenal Aripin, *Kamus Ushul Fiqh Dalam Dua Bingkai Ijtihad*, (Kencana Prenada Media Group : Jakarta, 2012) hlm. 22.

Hendi Suhendi, *Fiqh Muamalah*, (Jakarta: PT Raja Grafindo Persada, 2011). hlm. 2.

Hendi Suhendi, *Fiqh Muamalah*, (Jakarta: PT Raja Grafindo Persada, 2011). hlm. 2.

Ibnu Taimiyah, *al-Qawa'id al-Nuraniyah al-fiqhiyyah*, Riyadh: Maktabah al-Rusyd, cet. I, Juz II, hlm. 306.

Kasmir, Analisis Laporan Keuangan., Jakarta: PT. Raja Grafindo Persada, 2012.

Lukman Dendawijaya, *Manajemen Perbankan*, (Jakarta: Ghalia Indonesia, 2009) hlm.16-18.

M. Syukri Azwar Lubis, *Materi Pendidikan Agama Islam* (Surabaya: Media Sahabat Cendekia, 2019). hlm. 92

Maskun, *Kejahatan Siber (Cybercrime) Suatu Pengantar*, Kencana Prenada Media Group: Jakarta, 2013, hlm.29.

Maskun, *Kejahatan Siber Cyber Crime Suatu Pengantar* (Jakarta: Kencana Prenada Media Group, 2013). hlm.51-54.

Minartiningtyas, Brigida Arie. *Teori Pengenalan Wajah (Face Recognition)*, 2013.

Moh Mufid, *Ushul Fiqh Ekonomi dan Keuangan Kontemporer: Dari Teori ke Aplikasi* (Jakarta: Kencana, 2018). hlm. 100

Noor Halimah Anjani, *Ringkasan Kebijakan No. 9 Perlindungan Keamanan Siber di Indonesia, Center For Indonesian Policy Studies (CIPS)*, Maret 2021. hlm.4.

Prayudi, Y dan Kurniawan, A, *Teknik Live Forensics Pada Aktivitas Zeus Malware Untuk Mendukung Investigasi Malware Forensics. HADFEX (Hacking and Digital Forensics Exposed)*, 2014, hlm. 1-5

Richardus Eko Indrajit, *Konsep dan Strategi Keamanan Informasi di Dunia Cyber*, (Graha Ilmu: Yogyakarta, 2014), hlm. 131.

Richardus Eko Indrajit, *Konsep dan Strategi Keamanan Informasi di Dunia Cyber*, Yogyakarta: Graha Ilmu, 2014, hlm. 1.

Richardus Eko Indrajit, *Konsep dan Strategi Keamanan Informasi di Dunia Cyber*, hlm.2

Rulli Nasrullah, *Teori dan Riset Media Siber (Cybermedia*), (Jakarta: Prenada Media Group, 2014). hlm. 17-18.

Rusdaya Basri, Ushul fikih 1 (Pare pare: IAIN Parepare Nusantara Press, 2020). hlm. 18.

Satjipto Rahardjo, *Sosiologi Hukum Esai-Esai Terpilih* (Yogyakarta: Genta Publishing, 2010). hlm. 99.

Syamsuddin, Anita Marwin, dan Mohammad Tahmid Nur, *Realitas 'Urf Dalam Reaktualisasi Pembaharuan Hukum Islam Di Indonesia* (Madura: Duta Media Publishing, 2020). hlm. 10.

Tercantum pada syarat dan ketentuan dalam aplikasi Bank Digital Aladin Syariah

Tim Dosen STAINU Tangerang, Modul Mata Kuliah Hukum Ekonomi Syariah, (PSP Nusantara: 2018) H 11.

William Gibson, *Neuromancer* (New York: Berkley Publishing Group, 1989), pp. 128.

Y. Sri Susilo, Sigit Triandaru, dan A. Totok Budi Santoso, *Bank dan Lembaga Keuangan Lain*" (Yogyakarta: Salemba Empat, 2006). hlm.36.

Jurnal/Artikel

Aulia Febriana. *Pengaruh Penggunaan Modul Pada Model Pembelajaran Kooperatif Tipe Student Team Achievement Divisions terhadap Hasil Belajar Siswa Pada Mata Pelajaran Keterampilan Komputer dan Pengelolaan Informasi di SMK Negeri 2 Bukittinggi*. Jurnal, Program Studi Pendidikan teknik Informatika, Fakultas Teknik: Universitas negeri Padang, 2014.

Awinitya Paresti, *Pengaruh Hukum Masa Kolonial Terhadap Hukum Positif Indonesia*, UNAIR.

Catejan & Mbama, *Digital banking, customer experience and bank financial performance: UK customers perception*, International Journal of Bank Marketing, Vol. 36, No.2,2018. hlm. 230-255.

Dani Indra Junaedi, *Peluang Keamanan Password dalam Transaksi Perbankan*, Jurnal Ilmu-ilmu Informatika dan Manajemen STMIK, STMIK Sumedang, Vol 12 No.1 Mei (2018) Hlm.31.

Departemen Penelitian dan Pengaturan Perbankan OJK, *Consultative Paper Manajemen Risiko Keamanan Siber Bank Umum*, 2021, hlm. 9.

Departemen Penelitian dan Pengaturan Perbankan OJK, *Consultative Paper Manajemen Risiko Keamanan Siber Bank Umum*, 2021, hlm. 6.

Departemen Penelitian dan Pengaturan Perbankan OJK, hlm. 15.

Dewi Triwahyuni, *Security Pengertian Dasar&Jenisnya* disampaikan pada paparan mata kuliah studi Keamanan Internasional, 2017.

Dista Amalia Arifah, *Kasus Cybercrime di Indonesia*, Jurnal Bisnis dan Ekonomi (JBE), September 2011, Vol. 18, No. 2, ISSN: 1412-3126, hlm. 190.

Fatima, A., *E-Banking Security Issues-Is There A Solution in Biometrics?*. Journal of Internet Banking and Commerce, 16(2), p.1. 2011.

Handrini Ardiyanti, *Cybersecurity Dan Tantangan Pengembangannya Di Indonesia*, Politica Vol. 5, No.1 Juni 2014, hlm.98-99

Hopkinson, G., Klarova, D., Turcan, R. V., & Gulieva, V. *How Neobanks' Business Models challenge*

Traditional Banks. International Business Centre at Aalborg University, August, 3, 2019.

Islam, S., *Systematic literature review: Security challenges of mobile banking and payments system. International Journal of u-and e-Service, Science and Technology*, 7(6), 2014, hlm.116.

Kholis,N. Perbankan Dlam Era Baru Digital. Jurnal Economicus, Vol.9, (No.1), 2018. hlm.88

Lene Hansen and Helen Nissenbaum, "*Digital Disaster, Cyber Security, and the Copenhagen School*", International Studies Quarterly, Vol. 53, No. 4, 2009. Hlm. 1160.

Marlina Asti, Bimo.Widhi Aryo. *Digitalisasi Bank Terhadap Peningkatan Pelayanan Dan Kepuasan Nasabah Bank*. Jurnal Ilmiah Inovator Edisi Maret 2018.

Muhammad Khairul Faridi, *Kejahatan Siber dalam Bidang Perbankan*, CyberSecurity dan Forensik Digital, Vol. 1, No. 2, November 2018, e-ISSN: 2615-8442, hlm. 59-60.

Niti Aayog, *Digital Banks A Proposal for Licensing & Regulatory Regime for India*, Discussion Paper, November 2021, page. 12

Nurhalis, *Perlindungan Konsumen Dalam Perspektif Hukum Islam Dan Undang-Undang Nomor 8 Tahun 1999*, (Jurnal Kajian Hukum dan Keadilan Institut Agama Islam Hamzanwadi (IAIH) NW Lombok Timur, 2015) hlm. 529.

Patrick Jagoda,*"Speculative Security", Dalam Reveron, Derek S., Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual*

World, (Washington, DC: Georgetown University Press, 2012), hlm. 22.

Quesada, V. *When Tech Meets Finance: A Roadmap for Digital Banking Transformation. Massachusetts: CreateSpace Independent Publishing Platform*. Edisis kedua, 2017.

Razatul Janna, *Faktor-Faktor Yang Mempengaruhi Nasabah Dalam Menggunakan Layanan Digital Banking Dengan Menggunakan Model Unified Theory Of Acceptance And Use Of Technology (UTAUT) pada PT. Bank Syariah mandiri cabang banda aceh*, 2019

Soediro, "*Prinsip Keamanan, Privasi, dan Etika dalam Undang-Undang Informasi dan Transaksi Elektronik dalam Perspektif Hukum Islam*", Jurnal Kosmik Hukum, Edisi No.2 Vol. 18, Fakultas Hukum Universitas Muhammadiyah Purwokerto, 2018, hlm. 102

Sofwan Jannah dan M. Naufal, *Penegakan Hukum Cyber Crime Ditinjau dari Hukum Positif dan Hukum Islam,* AL-MAWARID, VOL. XII, NO 1, FEB-AUGUST 2012, hlm. 74-77.

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Widi Aryo, Marlina, Asti & Bimo, *Digitalisasi Bank Terhadap Peningkatan Pelayanan&Kepuasan Nasabah Bank*. Jurnal Ilmiah Inovator, Maret 2018. hlm.34.

Wirianto Widjaja, *Digital Bank Trends and Regulations in Indonesia* disampaikan pada pertemuan Alumni Gathering MMSI 2022, Jakarta 19 Maret 2022.

Undang-Undang

Undang-Undang No. 10 Tahun 1998 tentang Perbankan

Undang-Undang No. 11 Tahun 2008 jo. Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen pasal 2

Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen pasal 4

Peraturan Otoritas Jasa Keuangan Nomor:1/POJK.07/2013 Tentang Perlindungan Konsumen Sektor Jasa Keuangan

Peraturan Otoritas Jasa Keuangan nomor 12/POJK.03/2021 tentang Bank Umum

Website/Internet

Adiyanti, Arsita Ika, *Pengaruh Pendapatan, Manfaat, Kemudahan Penggunaan, Daya Tarik Promosi, dan Kepercayaan Terhadap Minat Menggunakan Layanan E-Money*, 2015.

Aldo Fernando, CNBC Indonesia, *Hati-hati! Ini Risiko Mengintai Bank Digital di Masa Depan* (https://www.cnbcindonesia.com/market/20211103113315-17-288645/hati-hati-ini-risiko-mengintai-bank-digital-di-masa-depan/2) diakses tanggal 3 Desember 2021, pukul 14.05.

Aldo Fernando, CNBC Indonesia, *Hati-hati! Ini Risiko Mengintai Bank Digital di Masa Depan* (https://www.cnbcindonesia.com/market/20211103113315-17-288645/hati-hati-ini-risiko-mengintai-bank-digital-di-masa-depan diakses tanggal 13 Juni pukul 10:00WITA)

Bank Aladin Syariah, (https://id.wikipedia.org/wiki/Bank_Aladin_Syariah diakses tanggal 20 Mei 2022, Pukul 14:00)

Bank Indonesia, *Laporan Sistem Pembayaran dan Pengedaran Uang*, 2008.

BBVA Research, *Digital Economy Outlook*: January 2017. (https://www.bbvaresearch.com/wpcontent/uploads/2016/01/DEO_Jan16.pdf)

Bill Clinten, "*Apa itu Teknologi Face Recognition dan Bagaimana Cara Kerjanya*" (https://tekno.kompas.com/read/2022/04/14/17050047/apa-itu-teknologi-face-recognition-dan-bagaimana-cara-kerjanya-?page=all , diakses tanggal 3 Juni 2022 Pukul 20:35 WIB)

Chonnie Stephanie, *Daftar Bank Digital di Indonesia* (https://tekno.kompas.com/read/2021/04/22/10460097/daftar-bank-digital-di-indonesia?page=all) diakses tanggal 18 Oktober 2021 pukul 18:08 WIB.

Daniel Deha, Banking Everywhere: *Neobank dan Sejarah Bank Digital* (https://www.trenasia.com/banking-everywhere-neobank-dan-sejarah-bank-digital-part-3-habis-indonesia diakses tanggal 13 Juni 2022 Pukul 05.00 WITA).

Daniel Deha, *Banking Everywhere: Neobank dan Sejarah Bank Digital* (https://www.trenasia.com/banking-everywhere-neobank-dan-sejarah-bank-digital-part-3-habis diakses tanggal 04 Juni 2022, Pukul 13:55 WITA).

Definisi cyber security berdasarkan FSB Cyber Lexicon (https://www.fsb.org/wp-content/uploads/P121118-1.pdf). Diadaptasi dari International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27032:2012 – Guidelines for cybersecurity.

Definisi cyber security berdasarkan *FSB Cyber Lexicon (https://www.fsb.org/wp-content/uploads/P121118-1.pdf). Diadaptasi dari International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27032:2012 – Guidelines for cybersecurity.*

Josua Sitompul "Masalah Verifikasi Identitas di Dunia Siber"(https://www.hukumonline.com/klinik/a/masalah-verifikasi-identitas-di-duniasiberlt51f37ff48bc4c diakses tanggal 24 Mei 2022, Pukul 17:00)

Kementerian Agama Republik Indonesia, *Quran Kemenag* (https://quran.kemenag.go.id/surah/5/87) diakses tanggal 25 Juni 2022.

Kementerian Agama Republik Indonesia, *Quran Kemenag, (https://quran.kemenag.go.id/surah/2/283)* diakses tanggal 21 November 2021 Pukul 13.00.

Kementerian Agama Republik Indonesia, *Quran Kemenag,*

(https://quran.kemenag.go.id/surah/64/16) diakses tanggal 27 Juni 2022 Pukul 20.00.

M. Richard, *Ada Pembobolan Rekening Digital, Ini kata BTPN Soal Keamanan Akun Jeniuss (*https://finansial.bisnis.com/read/20200921/90/1294614/ada-pembobolan-rekening-digital-ini-kata-btpn-soal-keamanan-akun-jenius-indonesia) diakses tanggal 2 November 2021 pukul 12:10 WIB).

Nidia Zuraya, *Bagaimana Agar Bank Digital Syariah lebih Bisa Bersaing ? (*https://www.google.com/amp/s/m.republika.co.id/amp/r7rdzs383) diakses tanggal 11 April 2022, pukul 19:33.

Tentang Aladin, (https://aladinbank.id/tentang-aladin/ diakses tanggal 22 Mei 2022, Pukul 23:40)

Yuni Astutik, *Awas Kejahatan Cyber Mengincar Sektor Keuangan*(https://www.cnbcindonesia.com/tech/20201116154457-37-202172/awas-kejahatan-cyber-mengincar-sektor-keuangan) diakses tanggal 18 Oktober 2021 pukul 18:15.

BANK DIGITAL SYARIAH

ANALISIS CYBER SECURITY MENURUT HUKUM POSITIF DIINDONESIA DAN HUKUM EKONOMI SYARIAH

Buku ini disusun untuk para akademisi maupun praktisi di bidang hukum khususnya untuk memahami Cyber Security menurut hukum positif di Indonesia dan juga Cyber Security menurut hukum ekonomi syariah.

Buku ini akan membahas mengenai kumpulan alat keamanan, kebijakan, konsep, tindakan keamanan, pedoman, pendekatan manajemen risiko, tindakan, pelatihan, praktik terbaik, jaminan, dan alat dalam pandangan hukum positif dan hukum ekonomi syariah. Teknologi yang dapat digunakan untuk melindungi lingkungan jaringan dan aset organisasi dan pengguna. Organisasi mengamankan jaringan dan aset pengguna termasuk perangkat komputerisasi yang terhubung, personel, infrastruktur, aplikasi, layanan, sistem telekomunikasi, dan semua informasi yang dikirimkan dan/atau disimpan di dunia maya.

PT.BDProject

PT. BDProject

Alamat : Jl. Hasan Basri Komplek Polsek Banjarmasin Utara, Jalur 3 No. 9

Telp. : 0812-2369-2567
Email : office@bdproject.id
Website : www.bdproject.id

ISBN 978-623-98738-8-2

9 786239 873882