

**URGENSI REVISI UNDANG-UNDANG PERBANKAN (UNDANG-UNDANG
NOMOR 7 TAHUN 1992 JUNCTO UNDANG-UNDANG NOMOR 10 TAHUN 1998)
DALAM UPAYA PENCEGAHAN KEJAHATAN SIBER DI BIDANG PERBANKAN**

Ali Syariati (alisyariati32@gmail.com)

Fakultas Hukum Universitas Esa Unggul

Ade Hari Siswanto (ade.siswanto@esaunggul.ac.id)

Fakultas Hukum Universitas Esa Unggul

ABSTRAK

Kemajuan teknologi mendorong perkembangan pesat dalam sektor perbankan, antara lain dengan munculnya bank digital dan layanan perbankan digital. Peningkatan layanan perbankan elektronik (*E-Banking*) meningkatkan risiko kejahatan siber, terutama karena Indonesia masih dalam fase transformasi digital. Edukasi masyarakat tentang ancaman kejahatan siber masih belum merata, sementara modus operandi kejahatan siber terus berkembang, saat ini belum ada Undang-Undang khusus yang mengatur perbankan digital dan bank digital ketentuan tersebut masih diatur dalam peraturan otoritas jasa keuangan, hal tersebut menciptakan ketidakpastian hukum dan dapat berdampak negatif pada operasional bank digital serta perlindungan konsumen. Penelitian ini menggunakan metode normatif dengan pendekatan statute approach untuk menelaah undang-undang dan regulasi yang berkaitan. Pertumbuhan pesat layanan perbankan digital dalam beberapa tahun terakhir telah menciptakan kesenjangan regulasi yang signifikan, penelitian ini menunjukkan bahwa regulasi yang ada belum mampu mengimbangi perkembangan ini serta menimbulkan tantangan bagi bank dan regulator. Diperlukan revisi undang-undang perbankan untuk memperkuat kerangka regulasi yang ada guna mengakomodir pencegahan dan penindakan kejahatan siber di sektor perbankan. Undang-Undang perbankan harus mencakup standarisasi operasional bank digital dan layanan perbankan digital, manajemen risiko, keamanan data nasabah serta perlindungan konsumen. Selain itu, ketentuan pidana yang tegas dan spesifik terkait kejahatan siber perlu diperkuat, termasuk sanksi pidana dan administratif, serta pengakomodasian modus operandi kejahatan siber yang terus berkembang. Dengan demikian, undang-undang ini akan memperkuat sistem hukum dalam menghadapi tantangan siber, menjaga integritas serta kepercayaan terhadap sektor perbankan digital, dan memastikan perlindungan hukum yang lebih baik.

Kata Kunci: Kejahatan Siber, Upaya Pencegahan, Urgensi Revisi

ABSTRACT

Technological advancements are driving rapid development in the banking sector, notably through the emergence of digital banks and digital banking services. The growth of electronic banking (E-Banking) increases the risk of cybercrime, particularly as Indonesia is still in the phase of digital transformation. Public education on cybercrime threats is still uneven, while the modus operandi of cybercriminals continues to evolve. Currently, there is no specific law regulating digital banking and digital banks; these are still governed by Financial Services Authority regulations, which creates legal uncertainty and can negatively impact the operations of digital banks and consumer protection. This study uses a normative method with a statute approach to examine the relevant laws and regulations. The rapid growth of digital banking services in recent years has created a significant regulatory gap. This study shows that existing regulations are unable to keep pace with these developments and present challenges for banks and regulators. A revision of the banking law is needed to strengthen the existing regulatory framework to address the prevention and prosecution of cybercrime in the banking sector. The banking law should include standardization of digital bank operations and digital banking services, risk management, customer data security, and consumer protection. Additionally, specific and stringent criminal provisions related to cybercrime need to be reinforced, including criminal and administrative sanctions, as well as accommodating the evolving modus operandi of cybercrime. Thus, this law will enhance the legal system in facing cyber challenges, maintain the integrity and trust in the digital banking sector, and ensure better legal protection.

Keywords: Cybercrime, Prevention Efforts, Urgency of Revision

PENDAHULUAN

Kegiatan perbankan pada awalnya dimulai sebagai tempat bagi masyarakat untuk menitipkan uangnya yang disebut dengan kegiatan simpanan, pada perkembangannya bank menambah kegiatannya menjadi kegiatan peminjaman uang dengan cara uang yang di simpan oleh masyarakat kepada bank dipinjamkan kepada masyarakat yang sedang membutuhkan uang. Maka perbankan dapat diartikan sebagai kegiatan dan proses bank dalam melaksanakan usahanya.

Bank ialah institusi keuangan yang menghimpun dana melalui simpanan dari masyarakat yang kemudian menyalurkan dana tersebut pada masyarakat melalui kredit atau cara lainnya, dengan tujuan untuk peningkatan taraf hidup mereka. Dalam menjalankan fungsi tersebut bank berada dalam posisi yang rawan terhadap penyalahgunaan kewenangan baik dari internal perbankan maupun pihak luar (Sulisrudatin, 2018).

Dunia perbankan berkembang pesat seiring dengan kemajuan teknologi antara lain dengan kemunculan bank digital dan perbankan digital, terdapat perbedaan diantara dua hal tersebut, bank digital ialah bank di Indonesia yang beroperasi sebagian besar melalui sarana elektronik, dengan kantor fisik yang terbatas atau tidak memiliki kantor fisik selain kantor pusat

(POJK No.12/POJK.03/2021 Tentang Bank Umum, 2021). Sedangkan perbankan digital diatur pada POJK No.12/POJK.03/2018 tentang penyelenggaraan layanan perbankan digital oleh bank umum, dijelaskan bahwa layanan perbankan digital yaitu layanan keuangan elektronik yang secara efisien memanfaatkan data nasabah serta menawarkan layanan yang lebih cepat, lebih mudah, dan berpusat pada nasabah (*customer experience*), layanan ini memungkinkan nasabah melakukan transaksi secara mandiri (Heriani, 2023). Salah satu bentuk dari layanan perbankan elektronik adalah aplikasi *mobile banking (m-banking)* yang memberikan kemudahan dalam mengakses layanan perbankan. Seiring berjalannya waktu hal tersebut mempunyai dampak yang positif dan negatif, dengan adanya layanan perbankan elektronik (*E-Banking*) potensi terhadap kejahatan siber akan semakin meningkat, mengingat Indonesia masih melalui era transformasi digital edukasi terhadap masyarakat mengenai ancaman kejahatan siber belum dilakukan secara merata tetapi kejahatan siber akan terus berkembang dengan berbagai macam cara dan modus yang beragam (Widayanti & Fakultas, 2022).

Penulis menemukan kasus yang terjadi terhadap Bank BSI pada tahun 2023,

dimana para nasabah tidak dapat mengakses layanan BSI mobile, yang disebabkan oleh proses maintenance. Tetapi nasabah tidak dapat mengakses layanan tersebut selama beberapa hari hingga menyebabkan kecurigaan oleh para nasabah. Pakar keamanan siber mengkonfirmasi bahwa bank BSI mengalami serangan ransomware, yang diakui secara terbuka oleh bank BSI dalam akun media sosial mereka. Serangan tersebut menargetkan layanan seluler BSI dan mengakibatkan pencurian sekitar 1,5 terabyte data, termasuk 15 juta data dan kata sandi pelanggan. Akibatnya, akses internal dan layanan bank BSI dihentikan untuk sementara waktu, data yang dicuri oleh peretas tersebut dapat dimanfaatkan oleh dirinya ataupun meminta tebusan kepada bank BSI untuk data-data yang dicuri tersebut untuk keuntungan pribadi (Delvyan Putri Surya Ningrum & Jamiatur Robekha, 2023).

Pada kasus tersebut Bank Syariah Indonesia (BSI) mengalami serangan ransomware yang berdampak signifikan terhadap keamanan data pribadi nasabah. Serangan ini mengakibatkan pencurian 1,5 terabyte data, termasuk informasi pribadi 15 juta nasabah, yang menimbulkan kekhawatiran serius mengenai kepatuhan bank terhadap Undang-Undang Perlindungan Data Pribadi (UU PDP). Insiden ini mencerminkan kegagalan bank

dalam menerapkan langkah-langkah keamanan yang memadai untuk melindungi data dari akses yang tidak sah, yang berpotensi merugikan nasabah dan merusak reputasi institusi keuangan tersebut. Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) memiliki peran penting dalam menangani kejahatan siber di sektor perbankan. UU ini menetapkan kewajiban bagi bank sebagai pengendali data untuk melindungi data pribadi nasabah dari ancaman akses dan penggunaan yang tidak sah. Dalam konteks perbankan, dimana data sensitif seperti informasi keuangan dan identitas nasabah sering menjadi target serangan siber, penerapan langkah-langkah keamanan yang ketat adalah keharusan. UU PDP mengharuskan bank untuk menerapkan langkah-langkah teknis dan prosedural guna mencegah pencurian data, serta mengatur kewajiban pelaporan jika terjadi pelanggaran keamanan.

Dalam kasus lainnya Pada bulan Mei 2022, Bank BRI Cabang Tabing di Koto Tengah Kota Padang mengalami insiden yang mengakibatkan seorang nasabah kehilangan Rp 1,1 miliar dari rekeningnya. Kejadian ini berawal ketika nasabah menerima pesan melalui *WhatsApp* yang menawarkan layanan transaksi tanpa batas dengan biaya Rp 150 ribu per bulan. Dengan mengklik tautan dalam pesan

tersebut, nasabah secara tidak sengaja memberikan informasi yang memungkinkan pelaku untuk mengakses dan mengganti PIN rekeningnya. Hasilnya pelaku berhasil mencuri sebagian besar saldo rekening, menyisakan hanya Rp 14 juta dari jumlah yang terancam. Dalam perspektif Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), insiden yang dialami Bank BRI Cabang Tabing pada Mei 2022 melanggar ketentuan yang diatur dalam Pasal 30 dan Pasal 32. Pasal 30 melarang akses tidak sah ke sistem elektronik, sementara Pasal 32 melarang perubahan data elektronik tanpa hak. Pelaku menggunakan metode penipuan untuk mengakses dan mengubah PIN rekening nasabah, yang merupakan pelanggaran hukum berdasarkan UU ITE. Kasus ini menekankan perlunya penegakan hukum yang lebih ketat dan langkah-langkah keamanan yang lebih baik dari pihak bank untuk melindungi dan mencegah kejahatan siber terhadap nasabah (Achlina dkk., 2023).

Selanjutnya dari perspektif perlindungan konsumen terkait kejahatan siber di bidang perbankan penulis menemukan kejadian yang terjadi ketika Bank Syariah Indonesia mengalami serangan ransomware yang dampaknya sangat mengejutkan. Pada kuartal pertama

2022, grup ransomware LockBit berhasil melakukan sekitar 38% dari total serangan ransomware yang ada. Mereka berhasil mencuri data dari lebih dari 15 juta nasabah dan pegawai, termasuk nomor telepon, alamat, nama, informasi dokumen, saldo rekening, nomor kartu, dan detail transaksi. Serangan ini memberikan dampak besar baik bagi bank maupun nasabahnya. Jika dilihat dari sudut pandang dari Undang-Undang Perlindungan Konsumen (UUPK) Bank Syariah Indonesia (BSI) sebagai subjek usaha memiliki tanggung jawab untuk memberikan kompensasi atas kerugian, pencemaran, atau dampak negatif yang dialami konsumen akibat penggunaan barang dan jasa yang mereka tawarkan. Hal ini sesuai dengan Pasal 19 ayat (1), (2), (3), dan (4) dari Undang-Undang Perlindungan Konsumen (UUPK), yang mengharuskan bank untuk mengganti kerugian yang timbul akibat gangguan sistem yang menghambat transaksi. Kompensasi ini bisa berupa pengembalian uang atau penyediaan barang dan jasa yang setara (Muhammad dkk., 2024).

Melihat kasus kejahatan siber yang ada maka akan menimbulkan kerugian yang berdampak kepada berbagai pihak, mulai dari bank yang kehilangan kepercayaan dari para nasabahnya, hingga nasabah sendiri yang mendapatkan kerugian dari kejahatan siber. Berdasarkan penelusuran penulis

menemukan data dari *Checkpoint Research 2022* terhadap sektor layanan keuangan termasuk perbankan mengalami 1.131 serangan siber pada tiap minggunya. Pada data lain yang ditemukan oleh *International Monetary Fund (IMF)* pada tahun 2020 menunjukkan rata-rata kerugian yang diterima tiap tahunnya akibat dari kejahatan siber di sektor layanan keuangan secara global mencapai sekitar US\$100 miliar (Burhan, 2023).

Berdasarkan kasus-kasus dan data yang dipaparkan penulis kejahatan siber di bidang perbankan sangatlah variatif, maka revisi undang-undang perbankan merupakan hal yang sangat mendesak dalam upaya pencegahan serta penindakan kejahatan siber di sektor perbankan. Dengan semakin berkembangnya teknologi dan meningkatnya ancaman siber, regulasi yang ada saat ini perlu diperbarui untuk memastikan perlindungan yang memadai bagi nasabah dan integritas sistem perbankan. Kejahatan siber terus berkembang maka peraturan hukum pun harus berkembang seiring dengan kebutuhan masyarakat.

Pada penelitian ini penulis menyoroti urgensi revisi Undang-Undang Perbankan yang telah lama diterapkan, agar lebih sesuai dengan perkembangan teknologi digital dan meningkatnya ancaman siber. Berbeda dari penelitian sebelumnya yang

berfokus pada aspek hukum perbankan tradisional, penelitian ini menggarisbawahi perlunya penambahan ketentuan khusus dalam regulasi perbankan untuk mencegah kejahatan siber. Pendekatan ini menghadirkan perspektif baru bahwa undang-undang yang ada perlu mencakup perlindungan yang lebih menyeluruh terhadap kejahatan siber khususnya di bidang perbankan.

RUMUSAN MASALAH

Berdasarkan pendahuluan yang telah penulis uraikan diatas, penulis membagi rumusan masalah sebagai berikut:

1. Bagaimana hukum perbankan mengakomodir kejahatan siber di bidang perbankan?
2. Bagaimana urgensi revisi undang-undang perbankan dalam mengantisipasi kejahatan siber?

METODE PENELITIAN

Dalam melakukan penelitian penulis memakai metode penelitian normatif yang mana penulis berfokus pada analisis terhadap bahan hukum yang relevan untuk mengkaji isu-isu yang diangkat dalam penelitian (Benuf dkk, 2020). Penulis mengumpulkan bahan hukum primer, sekunder dan tersier seperti Undang-Undang, jurnal, buku, pendapat ahli untuk dianalisis dengan komprehensif agar mendapatkan bahan hukum yang

kredibel. Dalam mengumpulkan bahan-bahan hukum tersebut penulis menggunakan pendekatan *statute approach* yang merupakan pendekatan terhadap undang-undang dan regulasi yang berkaitan terhadap penelitian penulis (Ariawan, 2013).

HASIL DAN PEMBAHASAN

Ketentuan-Ketentuan Bank Digital, Perbankan Digital dan Kejahatan di Bidang Perbankan Digital Dalam Peraturan Perundang-Undangan di Indonesia

Bank digital ialah institusi keuangan yang operasinya sepenuhnya secara online tanpa kehadiran fisik kantor cabang. Bank digital menawarkan berbagai layanan perbankan melalui platform digital seperti aplikasi mobile dan situs web, hal tersebut memungkinkan nasabah untuk melaksanakan transaksi perbankan kapanpun dan dimanapun. Dengan mengadopsi teknologi canggih bank digital mampu memberikan layanan yang lebih cepat dibandingkan bank konvensional, selain itu biaya operasional yang lebih rendah menjadi keuntungan tersendiri bagi bank digital dikarenakan tidak adanya kebutuhan untuk mempertahankan kantor cabang fisik (Vahzrianur dkk, 2023).

Di Indonesia pengaturan terkait bank digital di atur pada Peraturan Otoritas

Jasa Keuangan Nomor 12/POJK.03/2021 pasal 1 angka 22, pada peraturan tersebut didefinisikan bahwa bank digital, juga dikenal sebagai BHI (bank berbadan hukum indonesia), beroperasi sebagian besar melalui saluran elektronik dan memiliki lokasi kantor fisik yang minimal, biasanya terbatas pada kantor utama. Peraturan Otoritas Jasa Keuangan yang selanjutnya di singkat POJK, pada POJK Nomor 12/POJK.03/2021 memberikan kerangka regulasi terkait operasional bank digital di Indonesia. Regulasi ini mencakup berbagai aspek penting yang harus dipenuhi oleh bank digital, mulai dari persyaratan pendirian, manajemen risiko, hingga perlindungan nasabah. Salah satu poin utama yang diatur dalam peraturan ini adalah syarat pendirian bank digital, termasuk modal minimum yang harus dimiliki dan persyaratan administratif lainnya yang harus dipenuhi oleh calon pendiri. Selain itu POJK ini juga mengatur tentang tata kelola perusahaan (*good corporate governance*), yang mencakup struktur organisasi, tugas dan tanggung jawab direksi serta dewan komisaris, dan mekanisme pengawasan internal. Dalam hal manajemen risiko, peraturan ini menekankan pentingnya bank digital untuk memiliki sistem manajemen risiko yang efektif dan terintegrasi, terutama dalam menghadapi ancaman siber dan perlindungan data nasabah. Bank digital

diwajibkan untuk menerapkan standar keamanan yang tinggi dalam pengelolaan teknologi informasi dan komunikasi untuk memastikan integritas, kerahasiaan dan ketersediaan data nasabah (Ismail dkk, 2022).

Kemunculan bank digital merupakan salah satu faktor pendorong adanya perbankan digital, bank digital yang beroperasi sepenuhnya secara online tanpa kehadiran kantor cabang fisik menghadirkan berbagai inovasi dan kemudahan yang kemudian mempengaruhi bank konvensional untuk memperbarui dan meningkatkan layanan digital mereka. Perbankan digital didefinisikan sebagai suatu layanan perbankan digital bagi nasabah bank dalam mendapatkan informasi dan melaksanakan transaksi perbankan melalui media elektronik. POJK Nomor 21 Tahun 2023 mengatur tentang layanan perbankan digital. Menurut peraturan ini, layanan digital ialah produk bank yang disediakan bank dengan menggunakan teknologi informasi melalui media elektronik. Layanan ini bertujuan untuk memberikan akses kepada nasabah atau calon nasabah terhadap produk bank dan produk dari mitra bank yang bisa diakses secara mandiri.

POJK Nomor 21 Tahun 2023 memainkan peran penting dalam mengatur aspek-aspek krusial layanan perbankan

digital seperti tata kelola dan manajemen risiko hingga keamanan. Bank diwajibkan untuk menerapkan sistem manajemen risiko yang komprehensif untuk menghadapi ancaman siber dan melindungi data nasabah, Standar keamanan yang ketat diimplementasikan untuk memastikan data nasabah terlindungi dari berbagai bentuk kejahatan siber. Selain itu, POJK Nomor 21 Tahun 2023 mengatur kewajiban pelaporan dan pengawasan oleh Otoritas Jasa Keuangan untuk memastikan kepatuhan bank terhadap regulasi. Secara keseluruhan POJK Nomor 21 tahun 2023 memberikan landasan yang kuat bagi penyelenggaraan layanan perbankan digital di Indonesia, memastikan bahwa layanan tersebut dapat beroperasi dengan aman, efisien dan bertanggung jawab. Regulasi ini tidak hanya mendukung inovasi dalam layanan perbankan digital tetapi juga memastikan inovasi tersebut terjadi dalam kerangka yang teratur dan terkontrol serta melindungi kepentingan nasabah.

Terhadap kejahatan siber di bidang perbankan peraturan perundang-undangan yang dapat digunakan terdapat pada Undang-Undang Informasi dan Transaksi Elektronik No. 11 Tahun 2008 yang sudah diamandemen dengan Undang-Undang No. 19 Tahun 2016, terdapat beberapa pasal pada Undang-Undang tersebut yang mencakup kejahatan siber antara lain, pasal

30 mengatur tentang akses ilegal seperti peretasan sistem perbankan, pasal 31 mengatur intersepsi ilegal seperti penyadapan transaksi perbankan, pasal 32 dan 33 meliputi perusakan data dan serangan siber yang melumpuhkan layanan bank, pasal 35 menangani manipulasi data seperti pemalsuan saldo rekening nasabah dan kegiatan kriminal lainnya yang menggunakan teknologi informasi sebagai alat dalam melakukan pelanggaran hukum. Perlindungan terhadap data dan informasi keuangan nasabah menjadi fokus utama pada undang-undang ini.

Undang-Undang Perbankan Tidak Mengatur Bank Digital dan Perbankan Digital Terkait Kejahatan Siber Perbankan

Dalam bidang perbankan terdapat undang-undang yang mengatur terkait sektor perbankan, undang-undang perbankan di Indonesia diatur dalam Undang-Undang No. 7 tahun 1992 dan perubahannya Undang-Undang No 10 Tahun 1998. Undang undang tersebut menyediakan kerangka hukum yang mengatur aspek operasional perbankan yang tujuannya untuk menciptakan sistem perbankan yang sehat agar dapat mendukung pembangunan ekonomi nasional. Beberapa pengaturan yang dapat penulis simpulkan sebagai berikut:

- a) **Ketentuan Umum:** Pada bagian ini menguraikan terkait definisi dan istilah-istilah dasar yang digunakan dalam undang-undang, termasuk pengertian bank, jenis-jenis kegiatan perbankan, serta lembaga-lembaga yang berwenang dalam pengawasan perbankan. Hal tersebut merupakan landasan hukum yang menjelaskan ruang lingkup dan tujuan dari undang-undang perbankan.
- b) **Asas, Fungsi dan Tujuan:** Mengatur terkait operasional, fungsi dan tujuan perbankan di Indonesia, tujuannya mencakup taraf hidup masyarakat dan mendukung pembangunan ekonomi nasional. Bank diharapkan beroperasi berdasarkan prinsip kehati-hatian dan efisiensi.
- c) **Jenis dan Usaha Bank:** Teks ini memberikan penjelasan tentang 2 tipe bank yang diakui: Bank Umum dan Bank Perkreditan Rakyat (BPR). Bab ini menjelaskan perbedaan mendasar antara bank umum dan BPR, yang mencakup bentuk-bentuk usaha yang diizinkan untuk dilaksanakan dari masing-masing bank, serta kegiatan usaha yang dilarang untuk keduanya.

d) Perizinan, Bentuk Hukum dan

Kepemilikan: Terkait perizinan bank undang-undang ini memberikan aturan detail untuk pendirian dan operasional bank di Indonesia. Proses tersebut dimulai dengan mengajukan permohonan kepada Bank Indonesia (BI) dengan menyertakan persyaratan seperti struktur organisasi, permodalan dan rencana kerja. Pada bagian ini juga mengatur mengenai bentuk hukum dari bank umum atau bank perkreditan rakyat (BPR) seperti perseroan terbatas, koperasi atau perusahaan daerah. Selain itu mengenai struktur kepemilikan diatur terkait kepemilikan yang memiliki batasan antara kepemilikan asing dan domestik.

e) Pembinaan dan Pengawasan:

Pada bab ini diatur bahwa Bank Indonesia (BI) memegang peranan utama dalam mengawasi dan mengatur kegiatan bank di Indonesia (sekarang sudah beralih kepada OJK), bank diwajibkan untuk menjaga keuangan mereka dengan baik, termasuk memenuhi aturan tentang modal dan prinsip kehati-hatian pada operasional mereka. Undang-undang ini juga menyatakan bahwa setiap bank harus menyampaikan neraca dan

perhitungan laba/rugi tahunan serta penjelasannya, dan laporan berkala kepada bank Indonesia. Bank Indonesia juga mempunyai wewenang untuk memeriksa bank secara rutin dan memberi sanksi jika diperlukan untuk menjaga stabilitas perbankan. Selain itu untuk melindungi dana simpanan masyarakat setiap bank wajib menjamin dana masyarakat pada Lembaga Penjamin Simpanan (LPS).

f) Dewan Komisaris, Direksi dan

Tenaga Asing: Ketentuan ini mengatur terkait mekanisme pengangkatan direksi, komisaris dan kewajiban pelaporan jika terjadi perubahan dewan komisaris dan direksi bank. Pengaturan mengenai penggunaan tenaga asing juga diatur dalam bab ini.

g) Rahasia Bank:

Rahasia bank dalam Undang-Undang Perbankan menetapkan bahwa bank harus menjaga kerahasiaan semua informasi terkait nasabah dan rekening mereka. Bank dilarang mengungkapkan data nasabah kecuali dalam kondisi tertentu yang diizinkan oleh hukum, seperti atas permintaan otoritas hukum atau pengadilan. Informasi yang harus dirahasiakan meliputi segala hal

terkait simpanan nasabah dan transaksi yang mereka lakukan di bank. Ketentuan ini bertujuan untuk melindungi privasi nasabah serta menjaga kepercayaan masyarakat terhadap sistem perbankan.

h) Ketentuan Pidana dan Sanksi

Administratif: Ketentuan pidana dan sanksi administratif pada undang-undang perbankan menetapkan berbagai hukuman untuk pelanggaran dan kejahatan yang dilakukan oleh bank atau individu yang terlibat dalam aktivitas perbankan. Kejahatan serius seperti penggelapan dana, pelanggaran atas ketentuan rahasia bank dapat dihukum dengan denda besar atau penjara. Selain itu terdapat sanksi administratif untuk pelanggaran regulasi yang tidak termasuk kedalam kejahatan, seperti ketidakpatuhan dalam penyampaian laporan keuangan atau pelanggaran aturan operasional lainnya. Sanksi administratif dapat berupa peringatan, pembekuan izin operasional atau bahkan pencabutan izin usaha bank (UNDANG-UNDANG NOMOR 10 TAHUN 1998).

Berdasarkan penjabaran penulis bisa dikatakan bahwa undang-undang

perbankan tidak mengatur mengenai bank digital dan perbankan digital, antara lain terkait kejahatan siber yang sangat berpotensi pada era digitalisasi perbankan. Perkembangan teknologi yang signifikan setelah pembuatan undang-undang tersebut menjadi salah satu faktor yang membuat ketentuan dalam undang-undang tersebut tidak mampu mengakomodir keberadaan bank digital dan perbankan digital. Pada saat undang-undang tersebut dibuat, konsep perbankan digital dan bank digital seperti yang kita kenal saat ini belum ada atau belum berkembang secara signifikan. Undang-undang tersebut lebih menekankan pada pengaturan aspek-aspek tradisional perbankan seperti operasional perbankan, manajemen risiko dan perlindungan nasabah.

Undang-Undang ITE Digunakan Sebagai Dasar Transaksi Perbankan Digital Termasuk Pidana Bank Digital

Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) di Indonesia pada awalnya diundangkan dalam Undang-Undang Nomor 11 Tahun 2008 dan kemudian diubah dengan Undang-Undang Nomor 19 Tahun 2016. Pemberlakuan UU ITE didorong oleh pesatnya perkembangan teknologi informasi dan komunikasi yang mengharuskan adanya peraturan khusus untuk mengatur kegiatan di dunia maya, menjamin kejelasan hukum bagi para

pelaku transaksi elektronik, dan melindungi masyarakat dari penyalahgunaan teknologi informasi.

UU ITE adalah salah satu bentuk hukum maya (*cyber law*) pertama yang ada di Indonesia, pada undang-undang tersebut memiliki cakupan yang cukup luas untuk mengatur *cyberspace*, tetapi dalam peraturan tersebut masih ada beberapa peraturan yang tidak diatur secara spesifik. Undang-Undang tersebut dibuat untuk menangani problematika hukum terkait komunikasi elektronik, penyampaian informasi dan transaksi elektronik (Winarno, 2011). UU ITE mengatur berbagai aspek penting terkait informasi elektronik dan transaksi elektronik, salah satu aspeknya adalah Undang-Undang tersebut memberikan panduan mengenai pelaksanaan transaksi elektronik serta menetapkan kewajiban penyelenggaraan sistem elektronik untuk menjaga keamanan dan kerahasiaan data pengguna. Dalam konteks kejahatan siber UU ITE menetapkan berbagai jenis kejahatan siber seperti hacking, phishing dan penyebaran virus komputer serta mengatur sanksi bagi pelakunya.

UU ITE memiliki cakupan dalam mengatur transaksi yang menggunakan komputer dan jaringan termasuk terkait transaksi perbankan digital, UU ITE merupakan sebuah landasan hukum untuk

perbankan digital di Indonesia. Meskipun UU ITE tidak mengatur bank digital dan layanan perbankan digital, Undang-Undang tersebut memberikan dasar yang cukup esensial untuk memastikan keamanan dan keandalan transaksi elektronik. Dalam transaksi perbankan digital UU ITE mengatur aspek-aspek krusial seperti autentikasi elektronik, tanda tangan digital dan perlindungan data pribadi yang relevan bagi operasional perbankan digital. Pengaturan tersebut juga meliputi sanksi pidana terhadap kejahatan siber seperti pencurian identitas, penipuan elektronik dan serangan siber lainnya. Namun karena tidak dirancang secara khusus untuk mengatur perbankan digital, terdapat kelemahan pada UU ITE sebagai landasan hukum bagi bank digital dan perbankan digital, diperlukan regulasi yang lebih spesifik untuk mengakomodir hal tersebut serta disesuaikan dengan kebutuhan hukum bank digital dan layanan perbankan digital agar dapat melindungi sistem perbankan digital dari berbagai risiko, termasuk kejahatan siber penipuan online dan akses ilegal ke sistem perbankan. UU ITE lebih berfokus kepada pengakuan keabsahan hukum dokumen elektronik dan tanda tangan elektronik, perlindungan data pribadi, serta penegahan hukum terhadap kejahatan siber secara umum.

Hukum Perbankan Tidak Mengakomodir Pencegahan dan Penindakan Kejahatan Siber di Bidang Perbankan

Undang-Undang tentang hukum perbankan yang ada di Indonesia saat ini terdapat pada Undang-Undang No 7 Tahun 1992 dan perubahannya Undang-Undang No 10 Tahun 1998, hukum perbankan di Indonesia saat ini belum sepenuhnya dapat mengakomodir kejahatan siber yang terjadi di bidang perbankan, meskipun pada undang-undang tersebut ada ketentuan yang mengatur tentang keamanan dan kerahasiaan data nasabah. Regulasi yang ada cenderung lebih fokus pada aspek perbankan konvensional seperti manajemen risiko keuangan dan kepatuhan terhadap standar perbankan konvensional tanpa memberikan perhatian yang memadai terhadap ancaman siber yang semakin kompleks dan berkembang, dalam ketentuan pidana yang ada pada Undang-Undang Perbankan hanya meliputi kejahatan perbankan yang konvensional seperti penggelapan dana dan pelanggaran atas ketentuan rahasia bank.

Peraturan perundang-undangan yang dapat mengakomodir kejahatan siber di bidang perbankan saat ini adalah Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), di dalam UU ITE pada pasal 27 hingga pasal 36 memiliki

pengaturan terkait kejahatan siber, namun dalam ruang lingkup yang sangat luas, peraturan tersebut tidak dikhususkan untuk menangani terkait kejahatan siber di bidang perbankan. Terdapat beberapa kejahatan di bidang perbankan yang dapat ditangani dengan UU ITE meliputi berbagai bentuk aktivitas yang dilarang dan menargetkan sistem perbankan dan data nasabah, beberapa contohnya seperti pada pasal 30 UU ITE yang mengatur akses ilegal terhadap sistem elektronik (*hacking*) yang bertujuan mencuri informasi sensitif seperti data keuangan nasabah. Selain itu pada pasal 27 UU ITE yang melarang distribusi konten yang mengandung unsur penipuan (*phishing*) dan sering digunakan untuk menipu nasabah untuk memberikan informasi pribadi mereka.

Dalam menghadapi kejahatan siber yang mengancam data nasabah di sektor perbankan, Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) memainkan peran krusial. Salah satu contohnya terdapat pada pasal 35 Undang-Undang tersebut yang memiliki peran penting dalam menangani kejahatan siber di bidang perbankan. Pasal ini mengatur kewajiban pengendali data untuk menerapkan langkah-langkah keamanan yang memadai dalam pengelolaan data pribadi. Dalam konteks perbankan, di mana data nasabah seperti informasi rekening,

transaksi, dan identitas pribadi menjadi target utama serangan siber. Pasal 35 mengharuskan pengendali data, termasuk bank, untuk menerapkan prosedur teknis dan administratif yang memadai guna melindungi data pribadi dari akses, perubahan, pengungkapan, atau penghancuran yang tidak sah. Ini mencakup langkah-langkah seperti enkripsi data, sistem keamanan jaringan, dan kontrol akses yang ketat. Dengan adanya ketentuan ini, bank diharapkan dapat mengurangi risiko pelanggaran data yang disebabkan oleh kejahatan siber, seperti peretasan atau ransomware. Kewajiban ini memberikan dasar hukum yang kuat bagi institusi perbankan untuk mengimplementasikan dan memelihara sistem keamanan yang efektif, serta melindungi data nasabah dari potensi risiko kejahatan siber. Dengan demikian, pasal ini berfungsi sebagai alat untuk memastikan bahwa bank digital dan konvensional berkomitmen untuk melindungi data pribadi nasabah mereka dan mencegah terjadinya pelanggaran yang dapat merugikan konsumen.

Selain peraturan-peraturan tersebut dalam konteks kejahatan siber di bidang perbankan, Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen (UUPK) juga memberikan kerangka hukum yang relevan untuk penanganan masalah kejahatan siber.

Dalam Undang-Undang tersebut terdapat ketentuan yang relevan untuk menangani kejahatan siber di bidang perbankan, dengan fokus pada perlindungan hak-hak konsumen antara lain: Pasal 4 mengatur hak-hak konsumen, termasuk hak atas kenyamanan, keamanan, dan keselamatan dalam menggunakan produk dan layanan, termasuk layanan perbankan elektronik. Jika terjadi kejahatan siber seperti penipuan atau pencurian data yang merugikan nasabah bank, konsumen memiliki hak untuk mendapatkan perlindungan hukum dan kompensasi atas kerugian yang diderita; Pasal 7 mewajibkan pelaku usaha termasuk bank untuk memberikan informasi yang benar, jelas, dan jujur mengenai kondisi dan jaminan produk atau layanan yang ditawarkan serta menjamin keamanan konsumen dalam transaksi elektronik; Pasal 19 menekankan tanggung jawab pelaku usaha untuk memberikan ganti rugi jika produk atau layanan yang diberikan menimbulkan kerugian bagi konsumen. Dalam konteks kejahatan siber di perbankan, hal ini menjelaskan bahwa bank harus bertanggung jawab atas kerugian yang dialami nasabah akibat kegagalan sistem keamanan atau penanganan yang tidak tepat terhadap insiden siber.

Meskipun memberikan kerangka hukum terkait dengan kejahatan siber,

Undang-Undang tersebut tidak sesuai dengan karakteristik kejahatan siber di bidang perbankan yang mencakup berbagai bentuk dan metode yang terus berkembang seiring dengan kemajuan teknologi informasi. Salah satu karakteristik utama adalah sifatnya yang sangat dinamis dan adaptif, di mana pelaku kejahatan siber terus mengembangkan teknik baru untuk mengelabui sistem keamanan dan memanfaatkan celah yang ada. Kejahatan ini memanfaatkan anonimitas internet untuk menghindari deteksi dan penegakan hukum. Dengan karakteristik kejahatan perbankan yang terus berkembang, regulasi yang ada pada Undang-Undang tersebut tidak cukup untuk menangani kejahatan siber di bidang perbankan secara komprehensif dan mencakup semua aspek operasional serta keamanan bank digital dan perbankan digital.

Urgensi Revisi Undang-Undang Perbankan Dalam Upaya Pencegahan Kejahatan Siber di Bidang Perbankan

Berkembangnya teknologi informasi yang signifikan membawa masyarakat kedalam era revolusi 4.0, revolusi 4.0 diartikan sebagai transformasi digital dengan pergerakan digitalisasi, sektor perbankan tidak luput beradaptasi dalam era transformasi digital. Revolusi 4.0 menuntut sektor perbankan untuk bertransformasi menjadi bank digital dan

mengembangkan layanan perbankan digital (Otoritas Jasa Keuangan, 2021). Kemunculan perbankan digital telah membawa transformasi yang signifikan di sektor perbankan konvensional. Dengan memanfaatkan kemajuan teknologi, bank digital memanfaatkan platform digital untuk menawarkan layanan keuangan, sehingga tidak lagi memerlukan interaksi di kantor cabang secara fisik. Layanan ini mencakup berbagai aktivitas perbankan, termasuk inisiasi rekening, transfer uang, pemrosesan pembayaran, dan administrasi keuangan. Semua layanan ini dapat diakses melalui perangkat elektronik termasuk ponsel dan laptop. Manfaat utama dari sistem perbankan digital adalah kenyamanan dan efektivitasnya. Nasabah dapat dengan mudah dan nyaman mengelola rekening mereka dari jarak jauh tanpa harus datang ke kantor cabang. Transaksi dapat dipercepat dengan biaya yang lebih murah, sehingga menarik bagi nasabah dan Perusahaan (Vahzrianur dkk, 2023).

Meski begitu dalam transisi kedalam sistem bank digital dan layanan perbankan digital mendapatkan beberapa tantangan terkait keamanan informasi dan privasi hingga ancaman kejahatan siber yang terus berkembang dengan modus beragam seiring dengan kemajuan teknologi, mengingat bank digital

mengandalkan platform digital dalam melaksanakan aktivitas usahanya, bank digital dan layanan perbankan digital tidak diatur pada sebuah undang-undang layaknya perbankan konvensional yang diatur dalam undang-undang perbankan. Regulasi yang mengatur terkait hal tersebut adalah POJK No 21 Tahun 2023 Tentang Layanan Digital Oleh Bank Umum, peraturan tersebut mengatur bahwa terhadap bank yang menggunakan layanan digital diperlukan untuk memperhatikan aspek manajemen risiko, keamanan data nasabah serta perlindungan konsumen, peraturan tersebut lebih menekankan upaya preventif dalam mencegah kejahatan siber, tetapi tidak dapat mencakup kedalam kebijakan pidana yang dapat menangani kejahatan siber pada layanan perbankan digital, POJK lebih mengarah kepada penerapan sanksi terhadap bank yang tidak melaksanakan ketentuan dan standar-standar pada POJK.

Dalam menghadapi kejahatan siber di bidang perbankan diperlukan hukum khusus yang dapat melakukan penindakan terhadap kejahatan siber pada perbankan digital secara langsung, dimana selama ini penindakan kejahatan siber dalam perbankan digital menggunakan Undang-Undang Informasi dan Transaksi Elektronik yang mengatur terkait penindakan kejahatan transaksi elektronik secara

umum, UU ITE pada pasal 27 hingga pasal 36 menetapkan sejumlah tindakan yang dianggap sebagai suatu tindak pidana seperti pencemaran nama baik, penyebaran berita bohong (*hoaks*), dan ujaran kebencian yang dilakukan melalui platform digital. Selain itu undang-undang ini juga mengatur tentang akses ilegal terhadap sistem elektronik, penyalahgunaan data pribadi serta aktivitas peretasan dan distribusi konten yang melanggar hukum seperti pornografi atau perjudian online. Tindakan yang diklasifikasikan sebagai sebuah tindak pidana dalam UU ITE tidak dispesifikasikan khusus untuk menindak kejahatan siber pada perbankan digital. Selain itu terdapat beberapa Undang-Undang lainnya yang masih digunakan untuk menangani kejahatan siber di bidang perbankan seperti Undang-Undang Perlindungan Data Pribadi yang mengatur berbagai aspek terkait perlindungan data pribadi di Indonesia, Undang-Undang Perlindungan Konsumen yang mengatur aspek terkait hak dan kewajiban dalam hubungan antara konsumen dan pelaku usaha serta Undang-Undang lainnya yang harus disesuaikan terlebih dahulu dengan bentuk dari kejahatan siber juga modus yang dilakukan oleh pelaku.

Selain itu terhadap pencegahan kejahatan siber pada perbankan digital diperlukan aturan hukum yang lebih kuat.

Saat ini kedudukan POJK sendiri dalam peraturan perundang-undangan di Indonesia merupakan sebuah peraturan pelaksana, dimana peraturan pelaksana sendiri adalah peraturan yang dibentuk berdasarkan instruksi dari peraturan perundang-undangan yang lebih tinggi serta bertujuan untuk mengatur aspek tertentu yang secara eksplisit atau implisit diamanatkan oleh undang-undang tersebut. Kedudukan POJK berada di bawah undang-undang dikarenakan statusnya sebagai peraturan pelaksana undang-undang. Kedudukan peraturan pelaksana jika ditinjau berdasarkan teori Hans Nawiasky yang disebut dengan “*theorie von stufenbau der rechtsordnung*” jika diterjemahkan menjadi ‘teori struktur bertingkat dalam tatanan hukum’. Berdasarkan teori tersebut susunan norma dibagi menjadi: a) Norma fundamental Negara (*staatsfundamentalnorm*) b) Aturan dasar Negara (*staatsgrundgesetz*) c) undang-undang formal (*formell gesetz*) dan d) Peraturan pelaksana dan peraturan otonom (*verordnung en autonome satzung*) (Prianto, 2024). Adanya teori tersebut semakin memperjelas bahwa tingkatan peraturan pelaksana berada di bawah undang-undang.

Peraturan pelaksana berfungsi untuk mengimplementasikan suatu undang-undang, peraturan pelaksana dibuat untuk

menjabarkan ketentuan undang-undang agar dapat diterapkan secara operasional. Dikarenakan peraturan pelaksana memiliki kekuatan hukum dan kedudukan di bawah undang-undang maka peraturan pelaksana tidak boleh bertentangan dengan undang-undang yang menjadi dasar pembuatannya. Peran utama peraturan pelaksana adalah memastikan bahwa ketentuan undang-undang dapat diimplementasikan dengan efektif dan sesuai dengan tujuan yang ingin dicapai oleh undang-undang tersebut. Maka dari itu POJK diharuskan konsisten dengan undang-undang yang menjadi dasar pembentukannya dan tidak boleh bertentangan dengan peraturan hukum yang lebih tinggi, dapat dikatakan Otoritas Jasa Keuangan mendapatkan batasan-batasan tertentu untuk mengeluarkan kebijakannya dan kedudukan Peraturan Otoritas Jasa Keuangan berada dibawah undang-undang dan tidak memiliki kekuatan hukum layaknya undang-undang.

Undang-Undang adalah instrumen hukum yang dibuat oleh badan legislatif yaitu Dewan Perwakilan Rakyat (DPR) bersama dengan presiden yang bertujuan untuk mengatur berbagai aspek kehidupan berbangsa dan bernegara. Peraturan perundang-undangan merupakan hukum tertulis yang memainkan peran penting dalam pembangunan hukum nasional, di Indonesia peraturan perundang-undangan

mempunyai fungsi signifikan dalam penciptaan hukum dan menjadi pilar utama sistem hukum nasional. Bagir Manan berpendapat bahwa peraturan perundang-undangan memiliki fungsi internal dan eksternal. Fungsi internal berkaitan dengan fungsi legislasi di dalam sistem hukum itu sendiri. Dalam lingkungan khusus ini, peraturan perundang-undangan memenuhi banyak tugas internal, yaitu: 1) penciptaan hukum (*rechts chepping*) 2) pembaharuan hukum 3) integrasi dan kepastian hukum 4) kepastian hukum. Di sisi lain, fungsi eksternal peraturan perundang-undangan meliputi 1) perubahan 2) stabilitasi 3) kemudahan. Fungsi peraturan perundang-undangan yang dikemukakan oleh Bagir Manan menunjukkan bahwa peraturan tersebut dibuat oleh organ yang berwenang dan dirancang untuk mencapai tujuan tertentu. Selain itu, peraturan perundang-undangan juga menegaskan batasan berlakunya suatu aturan hukum, serta berfungsi sebagai alat control maupun sebagai alat untuk mengarahkan perubahan masyarakat (Rokilah, 2020).

Peraturan perundang-undangan berfungsi sebagai instrument yang sangat efektif dalam reformasi hukum (*law reform*) karena memiliki kekuatan hukum yang mengikat dan memaksa. Peraturan perundang-undangan ini memiliki peran penting dalam memperbarui dan

menyesuaikan sistem hukum dengan kebutuhan dan perkembangan masyarakat. Bagir Manan menyatakan bahwa peranan peraturan perundang-undangan semakin signifikan dari waktu ke waktu, terutama di Indonesia. Hal ini diakibatkan oleh faktor-faktor berikut: 1) Hukum dan peraturan, sebagai norma hukum formal, mudah diidentifikasi, dapat diakses, dan ditelusuri karena bentuk, jenis, lokasi, dan pembuatnya yang jelas. 2) Hukum dan peraturan menawarkan lebih banyak kepastian hukum karena menetapkan aturan yang jelas dan mudah diidentifikasi. 3) Peraturan perundang-undangan memiliki struktur dan sistematika yang tertata dengan baik, sehingga memungkinkan untuk dianalisis dan dievaluasi dari segi substansi formal dan materialnya. 4) Perencanaan peraturan dan regulasi yang tepat dapat memastikan pembentukan dan pengembangannya. Aspek ini sangat penting bagi negara-negara yang sedang dalam tahap pembangunan, terutama dalam membangun kerangka hukum baru yang selaras dengan tuntutan dan kemajuan masyarakat yang terus berkembang. Faktor-faktor tersebut merupakan pendukung adanya pengaturan perbankan digital pada suatu undang-undang, kedudukan undang-undang dalam upaya pencegahan kejahatan siber di bidang perbankan sangatlah strategis dan krusial undang-undang berfungsi sebagai landasan

hukum yang memberikan kerangka kerja bagi institusi perbankan untuk mengimplementasikan langkah-langkah pencegahan terhadap ancaman siber yang saat ini hanya diatur pada Peraturan Otoritas Jasa Keuangan.

Perkembangan teknologi di sektor perbankan memerlukan regulasi yang cepat dan adaptif untuk mengatasi risiko baru dan memastikan perlindungan nasabah yang memadai. Proses legislasi yang melibatkan banyak tahapan dan persetujuan dari berbagai pihak sering kali tidak bisa mengikuti kecepatan perkembangan teknologi tersebut. Oleh karena itu OJK sebagai lembaga independen yang diberi mandat untuk mengatur dan mengawasi sektor jasa keuangan menggunakan POJK sebagai instrument untuk merespon dinamika yang terjadi dengan lebih cepat. Namun hal tersebut tidak bisa dilaksanakan dalam jangka waktu yang panjang, jika OJK terus menerus mengeluarkan regulasinya sendiri tanpa di implementasikan kedalam suatu undang-undang maka dapat dikatakan bahwa jumlah peraturan perundang-undangan di sektor perbankan tidak seimbang dan cenderung *over-regulated*, Hampir setiap instansi di Indonesia yang memiliki tugas dan fungsinya berhubungan dengan sektor usaha termasuk sektor perbankan membentuk peraturan tanpa koordinasi yang baik, cenderung

mengedepankan kepentingan sektornya masing-masing. Selain itu, para pembuat peraturan sering kali tidak menyadari bahwa proses pembentukan peraturan perundang-undangan sebenarnya adalah upaya untuk menyatukan atau mengharmonisasikan berbagai kepentingan yang ada (Rakia, 2021). Indonesia masih belum memiliki dasar hukum yang memadai untuk pelaksanaan bank digital dan perbankan digital. Sebagai Negara yang mendukung digitalisasi perbankan perlu memahami karakteristiknya secara mendalam, letak peraturannya dan peraturan apa saja yang menjadi acuan. Digitalisasi perbankan memungkinkan adanya kompleksitas permasalahan, maka diperlukan regulasi yang lebih tinggi atau setara dalam peraturan undang-undang dibandingkan Peraturan Otoritas Jasa Keuangan yang ada saat ini. Regulasi yang ada pada POJK saat ini belum sepenuhnya mencakup bank digital dan perbankan digital. Indonesia sebagai Negara dengan sistem hukum civil law telah menjadi koneskuensi bahwa semua hukum yang ada harus dikodifikasikan dan diatur sesuai dengan perundang-undangan yang berlaku (Kurniawan & Yuspin, 2023).

Peraturan-peraturan yang ditetapkan oleh Otoritas Jasa Keuangan saat ini dapat dikatakan cukup efektif dalam mengejar ketertinggalan undang-undang

perbankan yang tidak dapat mengakomodir pengaturan perbankan digital, POJK dapat digunakan sebagai rambu-rambu bagi perbankan digital dalam menjalankan kegiatannya, namun tidak dapat dijadikan payung hukum yang kuat layaknya sebuah undang-undang dikarenakan kedudukannya yang berada dibawah undang-undang. Realita yang terjadi saat ini bagi perbankan digital terhadap upaya-upaya pencegahan diatur dalam POJK dan terkait penindakan terhadap kejahatan siber diatur dalam UU ITE, dapat dikatakan bahwa pengaturan bagi bank digital dan perbankan digital masih belum konsisten dan konkret. Sebagai perbandingan terhadap bank konvensional aturan yang digunakan adalah Undang-Undang No 10 Tahun 1998 dan Undang-Undang No 7 Tahun 1992, pada undang-undang tersebut terhadap bank yang melaksanakan aktivitas usahanya diatur secara sistematis hingga mencakup kepada ketentuan tindak pidana perbankan. Perlu diingat bahwa bank digital dan perbankan digital mempunyai kegiatan yang sama layaknya bank konvensional dimana mereka mengimpon dana masyarakat disana dan terjadi perputaran uang, hanya berbeda pada implementasi dan cara penyediaan layanannya, dari sisi pengaturan hukum menunjukkan perbedaan signifikan. Bank konvensional diatur oleh regulasi yang sudah mapan terkait operasional cabang, kepemilikan modal,

dan layanan langsung, serta ketentuan mengenai pengawasan dan kepatuhan yang telah lama diterapkan. Sebaliknya, bank digital, yang lebih baru, menghadapi tantangan dalam menyesuaikan dengan kerangka hukum yang sering kali belum sepenuhnya diperbarui untuk model bisnis berbasis teknologi mereka.

Kemunculan layanan keuangan digital sangat luar biasa dalam beberapa tahun terakhir. Namun demikian, penelitian menunjukkan bahwa pembatasan yang ada tidak sepenuhnya mengimbangi kemajuan pesat ini, sehingga menimbulkan kesenjangan dan tantangan signifikan bagi pihak bank serta para regulator. Salah satu isu utama yang dihadapi adalah kurangnya regulasi spesifik yang secara langsung mengaddress aspek unik dari perbankan digital, perbankan digital memiliki karakteristik yang berbeda dari perbankan konvensional, antara lain seperti penggunaan teknologi canggih dalam operasional dan layanan kepada nasabah. Namun regulasi yang ada masih berfokus pada perbankan konvensional dan sering kali tidak mencakup kebutuhan khusus bagi perbankan digital. Hal ini menciptakan ketidakpastian hukum yang dapat berdampak negatif pada operasional perbankan digital serta perlindungan konsumen (Anwar, 2024). Kemajuan yang dicapai dalam teknologi informasi dan

komunikasi dalam industri perbankan sudah mengakibatkan munculnya proses hukum baru yang saat ini tidak diatur oleh peraturan dan regulasi yang ada. Saat ini, belum ada peraturan perundang-undangan yang secara khusus mengatur operasional perbankan digital. Kerangka hukum yang mengatur perbankan masih didasarkan pada UU No. 7 tahun 1992 dan revisi berikutnya, UU No. 10 tahun 1998. Pada dasarnya, undang-undang tersebut dapat diadaptasi dan harus mengikuti perkembangan masyarakat, terutama dengan adanya kemajuan teknologi informasi dan komunikasi berbasis internet dalam industri perbankan. Oleh karena itu, undang-undang ini perlu dimodifikasi untuk memasukkan konsep perbankan digital. Pembaharuan regulasi ini diperlukan untuk mencakup aspek-aspek teknologi finansial yang terus berkembang serta memastikan perlindungan konsumen dan stabilitas sistem keuangan (Utama, 2021).

Sudah seharusnya pencegahan dan penindakan kejahatan siber terkait bank digital dan layanan perbankan digital dikemas pada suatu undang-undang agar memberikan payung hukum yang kuat bagi perbankan digital dalam melakukan kegiatan operasional usahanya serta memberikan kepastian hukum bagi masyarakat, mengingat sebagian besar kejahatan siber terjadi pada sektor

perbankan. Urgensi revisi undang-undang perbankan dalam pencegahan kejahatan siber di bidang perbankan sangat mendesak mengingat pesatnya perkembangan teknologi dan meningkatnya ancaman siber. Sektor perbankan khususnya bank digital dan perbankan digital tidak bisa selalu bertumpu pada peraturan yang dikeluarkan POJK, meskipun POJK dinilai lebih adaptif dalam perkembangan zaman jika dibandingkan undang-undang yang lebih lambat dalam beradaptasi dan mempunyai mekanisme pembentukan yang lebih lambat, tetapi undang-undang bisa memberikan landasan hukum yang lebih kokoh serta memungkinkan penegakan hukum yang lebih efektif serta perlindungan yang lebih kuat bagi konsumen, dari sisi penegakan hukum sejalan dengan pendapat Brada Nawawi Arief yang mengemukakan bahwa tahap kebijakan legislasi (Revisi Undang-Undang) merupakan cara yang paling strategis dalam pengaturan sanksi pidana, pada tahapan ini kekuasaan legislatif memiliki wewenang untuk menetapkan dan merumuskan tindakan yang dapat dikenai pidana, serta berfokus pada inti dari masalah hukum pidana (Zaidan, 2016).

Revisi undang-undang diperlukan untuk memperbarui dan memperkuat kerangka regulasi yang ada agar dapat mengakomodir pencegahan dan penindakan

kejahatan siber di bidang perbankan. Perlu diaturnya dalam undang-undang terkait standarisasi bank digital dan layanan perbankan digital, aspek manajemen risiko, keamanan data nasabah serta perlindungan konsumen, selain itu diperlukan ketentuan pidana yang mengatur secara tegas dan spesifik terkait kejahatan siber mulai dari meningkatkan kejelasan dan ketegasan ketentuan hukum dengan memperkuat sanksi pidana dan administratif kepada para pelaku kejahatan siber serta dapat mengakomodir berbagai modus operandi seperti skimming, phishing, malware dan bentuk yang lainnya.

Pada praktiknya dalam merevisi undang-undang perbankan diperlukan sinergi dengan berbagai pihak yang mempunyai keahlian, kepentingan dan tanggung jawab, seperti OJK yang mempunyai peran dalam megawasi dan mengatur seluruh kegiatan di sektor perbankan haruslah dilibatkan dikarenakan lembaga tersebut mempunyai kompetensi dalam bidang perbankan dan mempunyai jam terbang dalam membuat peraturan mengingat OJK mempunyai wewenang dalam mengeluarkan POJK yang merupakan peraturan pelaksana undang-undang, selain itu para pihak yang mempunyai keahlian terkait karkarakteristik kejahatan siber seperti ahil/akademisi dibidang tersebut diperlukan untuk

memberikan masukan seperti bentuk kejahatan siber yang berkembang Indonesia serta kebutuhan hukum yang dibutuhkan, dan lembaga penegak hukum antara lain kepolisian, kejaksaan, Badan Siber dan Sandi Negara (BSSN) untuk memberikan masukan terkait aspek penegakan hukum dan keamanan siber. Dengan revisi undang-undang yang komprehensif, undang-undang perbankan dapat memastikan bank digital dan perbankan digital beroperasi dalam lingkungan yang aman dan terlindungi. Dengan demikian undang-undang tidak hanya berfungsi sebagai pencegah dan penindak yang efektif terhadap kejahatan siber tetapi juga memperkuat kepercayaan publik terhadap sistem bank digital dan layanan perbankan digital.

KESIMPULAN

Undang-Undang perbankan di Indonesia tidak mengatur secara khusus terkait kejahatan siber di era digitalisasi perbankan. UU No. 7 Tahun 1992 dan perubahannya UU No. 10 Tahun 1998 lebih fokus pada perbankan konvensional dan belum sepenuhnya mengakomodasi ancaman siber yang kompleks. Meskipun ada ketentuan tentang keamanan dan kerahasiaan data nasabah, regulasi ini cenderung lebih menitikberatkan pada manajemen risiko keuangan dan standar perbankan tradisional, serta kejahatan konvensional seperti penggelapan dana dan

pelanggaran atas ketentuan rahasia bank. Kejahatan siber di bidang perbankan saat ini lebih diatur oleh UU ITE, khususnya dalam pasal 27 hingga 36. Namun UU ITE memiliki cakupan yang luas dan tidak secara khusus berfokus pada kejahatan siber di sektor perbankan, sehingga masih terdapat kesenjangan regulasi yang perlu diisi untuk mengantisipasi ancaman siber yang semakin berkembang.

Undang-Undang memiliki peran krusial dalam sistem hukum nasional dan reformasi hukum karena kekuatan mengikatnya. Untuk mengantisipasi kejahatan siber di bidang perbankan, diperlukan undang-undang yang mampu mencegah dan menindak kejahatan siber di bidang perbankan secara langsung, khususnya bagi bank digital dan layanan perbankan digital. Revisi Undang-Undang ini harus mencakup standarisasi operasional, manajemen risiko, keamanan data nasabah dan perlindungan konsumen. Selain itu, dalam merevisi undang-undang harus memperkuat sanksi pidana dan administratif, serta mengakomodir modus operandi kejahatan siber yang terus berkembang. Dengan demikian undang-undang ini akan memperkuat sistem hukum dalam menghadapi tantangan siber, menjaga integritas serta kepercayaan terhadap sektor perbankan digital, dan

memastikan perlindungan konsumen yang lebih baik.

DAFTAR PUSTAKA

- Achlina, R., Putri, T., & Sugiyono, H. (2023). Tanggung Jawab Bank terhadap Tindakan Phising dalam Sistem Penggunaan E-Banking (Studi: Kasus Phising pada PT. Bank Rakyat Indonesia (Persero) Tbk). *Jurnal Interpretasi Hukum*, 4(3), 682–690. <https://www.ejournal.warmadewa.ac.id/index.php/juinhum/article/view/8318>
- Anwar, R. (2024). Tantangan Hukum dan Regulasi Terhadap Pertumbuhan Digital Banking Di Indonesia. *Jurnal Manajemen Dan Kewirausahaan*, 1(3), 121–132.
- Ariawan, I. G. K. (2013). *METODE PENELITIAN HUKUM NORMATIF*. 1(1), 21–30.
- Benuf, K., Mahmudah, S., & Priyono, E. A. (2020). Metodologi Penelitian Hukum sebagai Instrumen Mengurai Permasalahan Hukum Kontemporer. *Jurnal Gema Keadilan* 20, 7(1), 20–33. <https://doi.org/10.24246/jrh.2019.v3.i2.p145-160>
- Burhan, F. A. (2023). *Industri Finansial Banjir Serangan Siber, Bank Digital*

- Pasang Kuda-kuda*. Bisnis.Com. <https://finansial.bisnis.com/read/20230309/90/1635655/industri-finansial-banjir-serangan-siber-bank-digital-pasang-kuda-kuda>
- Delvyan Putri Surya Ningrum, & Jamiatur Robekha. (2023). Analisa Yuridis Dalam Kasus Kejahatan Siber Terhadap Internet Banking di Indonesia. *PESHUM: Jurnal Pendidikan, Sosial Dan Humaniora*, 2(4), 765–776. <https://doi.org/10.56799/peshum.v2i4.2115>
- Heriani, F. N. (2023). *Mengenal Perbankan Digital dan Bank Digital*. Hukumonline.Com. <https://www.hukumonline.com/berita/a/mengenal-perbankan-digital-dan-bank-digital-1t647683af1cb07/?page=1>
- Ismail, K., Ramadhan, R., Arva, R., Reswara, R., & Sugita, I. R. (2022). Perlindungan Hukum Nasabah Bank Digital di Indonesia yang Berkepastian Hukum. *Jurnal Hukum*, 1(12), 1–19.
- Kurniawan, D., & Yuspin, W. (2023). Menggagas Pendirian Bank Digital di Indonesia: Sebuah Telaah Yuridis. *Jurnal Supremasi*, 13(1), 1–14. <https://doi.org/10.35457/supremasi.v13i1.2158>
- Muhammad, A., Hutagalung, C., Marendra, N. R., & Ul, A. (2024). Perlindungan Terhadap Konsumen Dalam Kasus Kebocoran Data Bank Syariah Indonesia. *Jurnal Ilmu Hukum, Sosial, Dan Humaniora*, 2(1), 156–165.
- Otoritas Jasa Keuangan. (2021). *TRANSFORMASI DIGITAL PERBANKAN*. <https://ojk.go.id/id/berita-dan-kegiatan/info-terkini/Pages/Cetak-Biru-Transformasi-Digital-Perbankan.aspx>
- POJK No.12/POJK.03/2021 Tentang Bank Umum, Www.Ojk.Go.Id (2021). <https://sikepo.ojk.go.id/SIKEPO/Data-basePeraturan/PeraturanUtuh/84c36c57-c4bb-4815-9b13-c229>
- Prianto, W. (2024). ANALISIS HIERARKI PERUNDANG-UNDANGAN BERDASARKAN TEORI NORMA HUKUM OLEH HANS KELSEN DAN HANS NAWIASKY Wahyu. *Jisdik*, 2(1), 15–16.
- Rakia, A. S. R. . (2021). Simplifikasi Terhadap Peraturan- Peraturan Pelaksanaan Yang Dibentuk Oleh Presiden Dalam Sistem Ketatanegaraan Republik Indonesia. *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional*, 10(2), 249–262.

- Rokilah, R. (2020). The Role of the Regulations in Indonesia State System. *Ajudikasi : Jurnal Ilmu Hukum*, 4(1), 29–38. <https://doi.org/10.30656/ajudikasi.v4i1.2216>
- Sulisrudatin, N. (2018). Analisa Kasus Cybercrime Bidang Perbankan Berupa Modus Pencurian Data Kartu Kredit. *Jurnal Ilmiah Hukum Dirgantara*, 9(1), 26–39. <https://doi.org/10.35968/jh.v9i1.296>
- UNDANG-UNDANG NOMOR 10 TAHUN 1998, Pub. L. No. TAMBAHAN LEMBARAN NEGARA REPUBLIK INDONESIA NOMOR 3790, 1 (1998).
- Utama, A. S. (2021). Digitalisasi Produk Bank Konvensional Dan Bank Syariah Di Indonesia. *Jurnal Justisia : Jurnal Ilmu Hukum, Perundang-Undangan Dan Pranata Sosial*, 6(2), 113. <https://doi.org/10.22373/justisia.v6i2.11532>
- Vahzrianur, V., Putra, S. F., Pratama, R. B., Solihin, M. R., Halomoan, A. P., Tampubolon, & Siswajanthi, F. (2023). Tinjauan Yuridis dalam Sistem Perbankan Digital terhadap Perlindungan Nasabah. *Depositi: Jurnal Publikasi Ilmu Hukum*, 1(4), 371–380.
- Widayanti, P. W., & Fakultas. (2022). TINDAK PIDANA PENCURIAN DATA NASABAH DALAM BIDANG PERBANKAN SEBAGAI CYBER CRIME. *Jurnal Hukum Dan Perundang-Undangan*, 2(2), 1–21. <http://www.ifpri.org/themes/gssp/gssp.htm%0Ahttp://files/171/Cardon-2008-Coaching-d%27%2F%0Ahttp://journal.um-surabaya.ac.id/index.php/JKM/article/view/2203%0Ahttp://mpoc.org.my/malaysian-palm-oil-industry/%0Ahttps://doi.org/10.1080/23322039.2017>
- Winarno, W. A. (2011). SEBUAH KAJIAN PADA UNDANG-UNDANG INFORMASI DAN TRANSAKSI ELEKTRONIK (UU ITE). *Jurnal Ekonomi Akuntansi Dan Manajemen*, 10(1), 43–48.
- Zaidan, M. A. (2016). *KEBIJAKAN KRIMINAL*. Sinar Grafika.