AL-QISTH LAW REVIEW
VOL 7 NO.2 (2024)

EVALUASI TERHADAP KEBOCORAN DATA DALAM SISTEM PERBANKAN DI INDONESIA (STUDI KASUS *RANSOMWARE* PADA BANK SYARIAH INDONESIA)

Fikriatul Nabila[1], Imran Bukhari Razief[2], Amiludin[3]
fikriatulnabila@gmail.com, fhumt.imran@gmail.com, tsamanytrans@gmail.com
Universitas Muhammadiyah Tangerang
Jl. Perintis Kemerdekaan I No.33, Babakan, Cikokol, Tangerang, Banten.

Abstrak

Sangat penting bagi masyarakat untuk memiliki akses ke layanan keuangan karena bank adalah lembaga keuangan utama. Sebagaimana tercantum dalam Pasal 40 ayat (1) Undang-Undang No. 10 Tahun 1998 tentang Perbankan, kemampuan bank untuk menjaga data privasi nasabah sesuai dengan hukum dan peraturan yang berlaku sangat penting bagi kemampuan mereka untuk tetap bertahan dalam bisnis. Terlebih lagi, UU No. 21 tahun 2008 menetapkan prinsip-prinsip Syariah sebagai landasan bagi layanan dan pengelolaan keuangan. Tujuan dari penelitian ini adalah untuk meningkatkan pengetahuan masyarakat tentang masalah yang terkait dengan kebocoran data internet dan hukuman yang dikenakan kepada pemilik data yang melanggar undang-undang perlindungan data pribadi. Penelitian juga berfokus pada upaya hukum yang dapat dilakukan oleh nasabah jika data pribadi mereka tidak dilindungi. Penelitian ini diharapkan dapat meningkatkan pemahaman kita tentang langkah-langkah praktik keamanan data di industri perbankan Indonesia.

Kata Kunci: Perlindungan Data Pribadi, Kebocoran Data, Ransomware.

Abstract

It is crucial for the public to have access to financial services as banks are the primary financial institutions. As stated in Article 40 paragraph (1) of the Amendment to Law No. 10 of 1998 on Banking, banks' ability to maintain customer privacy data in accordance with applicable laws and regulations is critical to their ability to stay in business. Moreover, Law No. 21 of 2008 establishes Shariah principles as the foundation for financial services and management. The purpose of this research is to increase public knowledge about issues related to internet data leakage and the penalties imposed on data owners who violate the personal data protection law. The purpose of this research is to increase knowledge about the problems associated with internet data leaks and the penalties given to data owners who violate personal data protection laws. The research also focuses on the legal remedies that customers can take if their personal data is not protected. This research is expected to improve our understanding of the steps of data security practices in the Indonesian banking industry.

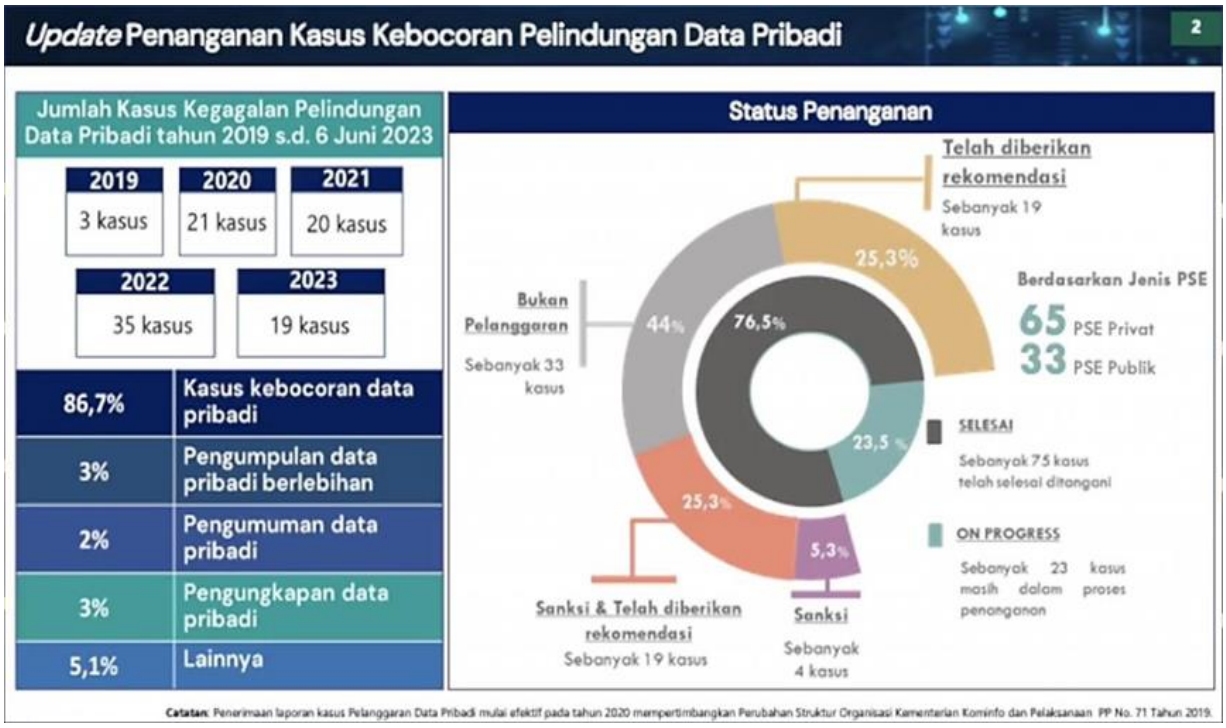
***Keywords**: Personal Data Protection, Data Breach, Ransomware.*

[1] Mahasiswa Fakultas Hukum Universitas Muhammadiyah Tangerang
[2] Mahasiswa Fakultas Hukum Universitas Muhammadiyah Tangerang
[3] Dosen Fakultas Hukum Universitas Muhammadiyah Tangerang

PENDAHULUAN

A. Latar Belakang Masalah

Bank merupakan institusi finansial yang memainkan peran krusial dalam menyajikan berbagai layanan finansial kepada public (Djoni & Rachmadi, 2010). Untuk mempertahankan kepercayaan dan eksistensi mereka, bank harus mematuhi aturan dan prinsip yang mengharuskan mereka menjaga kerahasiaan informasi bank. Ini berarti seberapa jauh nasabah dapat mempercayai bank untuk menyimpan dana mereka dan/atau menggunakan layanan lainnya tanpa membocorkan informasi keuangan dan transaksi mereka. Pencapaian ini sangat bergantung pada kemampuan bank untuk memenuhi kewajibannya untuk melindungi kerahasiaan informasi bank. Sesuai dengan Pasal 40 Undang-Undang No. 10 Tahun 1998. Bank bertanggung jawab untuk menjaga kerahasiaan informasi nasabah, menurut Undang-Undang Perbankan Nomor 07 tahun 1992. Menurut Pasal 40 ayat (1) Undang-Undang No. 10 Tahun 1998 tentang Perbankan, yang diubah oleh Undang-Undang No. 07 Tahun 1992 tentang Perbankan, Bank bertanggung jawab untuk menjaga kerahasiaan data nasabah dan uang yang mereka simpan. Pasal ini menekankan kewajiban bank untuk menjaga data nasabah dalam kapasitasnya sebagai penyimpan. Bank harus mematuhi semua peraturan dan regulasi yang berlaku untuk melindungi kepentingan nasabah dan menjaga keamanan dana dan informasi mereka (Hermansyah & Hum, 2005)



Tabel 1 *Efektif Penerimaan Laporan Kasus Pelanggaran Data Pribadi Pada Tahun 2020.*

Perbankan syariah adalah bagian dari perbankan yang didirikan berdasarkan prinsip-prinsip hukum Islam, atau syariah. Larangan terhadap bunga, riba, dan pelanggaran hukum syariah lainnya menjadi landasan utama perbankan syariah. Perbankan syariah menawarkan keuntungan melalui transaksi yang sesuai dengan aturan Islam dan skema hasil(Ramadhani dkk., 2021). Bisnis perbankan syariah diatur oleh Undang-Undang Perbankan Syariah No. 21 tahun 2008. Menurut Pasal 1 angka 1, ”Perbankan Syariah” mencakup semua yang berkaitan dengan Bank Syariah dan Unit Usaha Syariah, termasuk kelembagaan, bisnis, dan metode dan prosedur untuk menjalankan bisnis mereka.

Perbankan konvensional dan perbankan berbasis Syariah adalah dua bagian utama industri perbankan sepanjang sejarah. Bank konvensional menggunakan suku bunga dan perjanjian umum yang didasarkan pada hukum positif untuk menjalankan bisnis mereka. Sebaliknya, bank syariah menggunakan model hasil, di mana keuntungan nasabah ditentukan oleh pendapatan bank. Bank konvensional memiliki kemampuan untuk mengelola uang mereka di bisnis yang menguntungkan selama

mereka mengikuti undang-undang yang berlaku. Di sisi lain, bank Islam/syariah menggunakan hukum Islam untuk mengelola dana mereka (Sutedi, 2007).

Kejahatan siber juga telah berkembang dengan kemajuan teknologi, memasukkan jenis kejahatan baru dan teknik operasi baru. Hal ini berkaitan dengan peningkatan jenis kejahatan yang berbeda yang dilakukan melalui internet. Termasuk yang lebih umum seperti peretasan, *cracking*, dan *carding,* serta yang lebih khusus seperti *probe*, yang merupakan upaya berskala besar untuk mendapatkan akses ke suatu sistem; kompromi akun, yang merupakan penggunaan akun secara tidak sah; kompromi root, yang merupakan penggunaan akun secara tidak sah dengan hak istimewa untuk penyusup); penolakan layanan, atau DOS, yang merupakan lalu lintas yang berlebihan yang mencegah jaringan berfungsi; dan penyalahgunaan nama domain (Wisnubroto, 2010).

Undang-undang Perlindungan Data Pribadi No. 27 Tahun 2022 mengatur jenis dan kategori data pribadi, hak subjek, prosedur pemrosesan, sanksi administratif, institusi, peran masyarakat, hukum acara dan penyelesaian sengketa, dan pembatasan penggunaan. Perlindungan informasi pribadi adalah salah satu hak asasi manusia yang termasuk dalam perlindungan pribadi, jadi Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 harus menjadi dasar. Menurut Undang-Undang Perlindungan Data Pribadi No. 27 Tahun 2022, prosesor dan pengendali data pribadi adalah dua lembaga yang bertanggung jawab atas pengelolaan data pribadi di perusahaan, kementerian, dan lembaga lainnya. Individu, badan pemerintah, atau organisasi internasional dapat bertindak sebagai pengendali atau pemroses data, sesuai dengan Bab VI, Pasal 19 Undang-undang Perlindungan Data Pribadi. Selama pemrosesan data, adalah tanggung jawab pengendali data untuk menjamin kepentingan yang memberikan data pribadi. Undang-undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi membahas perbankan syariah dan perlindungan data pribadi. Menurut Pasal 1 angka 1 Undang-undang No. 27 Tahun 2022 ini, data pribadi adalah semua data yang dapat digunakan untuk mengidentifikasi seseorang

dengan berbagai cara. Sebagaimana dinyatakan dalam Pasal 2 angka 2 Undang-undang No. 27 Tahun 2022, tujuan pengaturan perlindungan data pribadi adalah untuk melindungi hak-hak konstitusional baik subjek data pribadi maupun data pribadi yang sedang diproses (Duata dkk., 2023).

Contoh terbaru dari kebocoran data terjadi pada tahun 2023 di Bank Syariah Indonesia (BSI), ketika organisasi *ransomware* bernama *LockBit* bocor 1,5 TB data bank nasional ke jaringan pasar gelap internet. Kasus ini mengganggu layanan bank pada tanggal 8 Mei 2023, ketika grup ransomware *LockBit* menyerang. Serangan berakhir pada 11 Mei 2023. *LockBit* mengumumkan setelah peretasan tersebut, bahwa mereka telah memperoleh data BSI, yang termasuk NDA, catatan keuangan, dokumen hukum, kata sandi untuk sistem bank internal dan eksternal, dan informasi pribadi milik lebih dari 15 juta nasabah dan karyawan. Mereka menetapkan tenggat waktu hingga 15 Mei 2023, dan membayar tebusan sebesar Rp 295,6 miliar (Redaksi, t.t.). *LockBit* mengklaim bahwa setelah tenggat waktu berlalu, mereka telah mengunggah data yang dicuri di internet. Mereka meminta nasabah mereka untuk mengadukan BSI ke pihak berwenang, dengan tuduhan bahwa perusahaan tersebut tidak bertanggung jawab atas data nasabahnya.

Ada beberapa penelitian sebelumnya, yang telah membahas tema dan isu yang diangkat oleh penulis. Penulis mencari variasi tema penelitian dengan melakukan tinjauan literatur terhadap penelitian-penelitian lain yang membahas topik yang sama, sehingga menambah keunikan penelitian ini. Penulis menemukan beberapa publikasi ilmiah yang membahas topik yang sama, antara lain: Pertama, penelitian yang berjudul Perlindungan Hukum Terhadap Data Pribadi di Media Elektronik (Analisis Kasus Kebocoran Data Pengguna Facebook di Indonesia) oleh Muhammad Bayu Satrio dan M.W. Widiatno (Satrio & Widiatno, 2020), dan Kedua, penelitian yang ditulis oleh Deanne Destriani Firmansyah, P., dan M. Helmi Fahrozi, dengan judul RUU Perlindungan Data Pribadi: Upaya untuk Mencegah Kebocoran Data Konsumen (Studi Kasus E-Commerce Bhinneka.com) (Putri & Fahrozi, 2021).

Tujuan umum dari penelitian ini adalah untuk memberikan pengetahuan dan ide tentang kebocoran data internet (*ransomware*). Tujuan khusus dari penelitian ini adalah untuk mengetahui bagaimana penindakan terhadap kebocoran data di Indonesia, dan untuk mengetahui langkah-langkah yang diambil dalam menangani kebocoran data serta pertanggungjawaban semua pihak yang terlibat.

B. Rumusan Masalah

Berdasarkan penjelasan dalam latar belakang tersebut, penulis tertarik untuk mengkaji terkait kebocoran data (*ransomware*) perbankan digital dengan dua rumusan masalah yaitu:

1. Bagaimana upaya hukum yang harus dilakukan oleh nasabah jika data pribadi dalam perbankan tidak terlindungi?
2. Bagaimana tanggung jawab hukum dari pemegang data yang melanggar ketentuan dalam Undang-Undang PDP yang mengalami kebocoran data?

C. Metode Penelitian

Penelitian adalah kegiatan ilmiah yang bertujuan untuk mempelajari satu atau beberapa gejala hukum tertentu. Metodologi adalah langkah yang tepat untuk memulai proses. Data dikumpulkan melalui tinjauan undang-undang yang relevan dan penelitian kepustakaan. Analisis deskriptif digunakan untuk mengatasi masalah saat mengevaluasi data. Penelitian ini dapat menggunakan yuridis normatif. Penelitian hukum yuridis normatif biasanya ”hanya” berbentuk studi dokumen yang bertujuan untuk menjelaskan fakta-fakta dan karakteristik yang diselidiki. Metode kualitatif normatif digunakan dalam analisis data penelitian ini, dan bahan hukum primer-yaitu peraturan perundang-undangan yang relevan seperti UU No. 10 Tahun 1998, yang mengubah UU No. 07 Tahun 1992 tentang perbankan, dan UU No. 27 Tahun 2022, yang mengatur tentang perlindungan data pribadi-digunakan. Sebaliknya, bahan hukum sekunder terdiri dari surat kabar, jurnal, buku-buku

hukum, literatur, dan penelusuran online. Penulis akan menguraikan proses analisis kebocoran data di sektor perbankan Indonesia.

PEMBAHASAN

A. Upaya Hukum Yang Harus Dilakukan Oleh Nasabah Jika Data Pribadi Dalam Perbankan Tidak Terlindungi

Pemberdayaan dan perlindungan konsumen adalah tujuan utama komitmen Bank Indonesia dan sektor perbankan untuk memberikan perlakuan yang sama kepada nasabah dengan bank. Nasabah sering dianggap sebagai pihak yang lemah atau kurang menguntungkan ketika terjadi perselisihan atau konflik hukum antara nasabah dan bank yang mengakibatkan kerugian bagi nasabah. Untuk melindungi nasabah bank, beberapa implementasi telah dilakukan, antara lain (Kusuma & SH, 2019):

a) Proses restrukturisasi industri perbankan Indonesia sedang berlangsung. Ini mencakup petunjuk tentang aspek institusional, kepemilikan, dan pola operasional bank atau grup bank, dengan tujuan mencapai visi dan misi yang telah ditetapkan.
b) Bank telah menekankan bahwa penelitian harus menjadi dasar undang-undang perbankan, dan bahwa konsultasi harus dilakukan dengan praktik terbaik dan standar internasional, serta keterlibatan profesional perbankan dalam proses pengaturan bank.
c) Prinsip Dasar Basel (*Basel Core Principles*), yang menjelaskan prinsip-prinsip pengawasan bank yang baik, harus selalu diingat saat membangun sistem pengawasan yang independen dan efektif. Bank juga akan melakukan *re-engineering* di beberapa bidang terkait pengawasan dalam rangka menerapkan strategi pengawasan berbasis resiko. Hal ini akan memastikan bahwa pengawasan bank akan dilakukan dengan baik. Membangun program kualifikasi pengawas bank, penerapan pengawasan *Real Time*, dan penilaian kelayakan penerapan pengawasan konsolidasi adalah tindakan tambahan yang akan dilakukan

d) Beberapa masalah penting yang akan dioptimalkan termasuk penerapan manajemen resiko, penanganan kredit bermasalah, peran intermediasi, sistem informasi manajemen perbankan, tata kelola yang baik, dan kemungkinan perbankan nasional untuk menerapkan anti pencucian uang.
e) Infrastruktur pendukung harus disiapkan, seperti penggunaan teknologi informasi yang tepat guna dan penggunaan lembaga peringkat, LPS, asuransi kredit, dan Biro Kredit sebagai pusat informasi debitur. Entitas-entitas ini diharapkan akan berdampak positif pada kinerja sektor perbankan.
f) Salah satu persyaratan yang dianggap penting untuk disiapkan adalah sistem yang akan menangani pengaduan nasabah bank. Nasabah yang menggunakan jasa keuangan juga harus diperhatikan. Salah satu cara untuk mencapai hal tersebut adalah dengan memberikan informasi menyeluruh tentang produk dan layanan perbankan, termasuk risiko yang mungkin dihadapi oleh nasabah.

Sesuai dengan Peraturan Bank Indonesia No. 07/07/PBI/2005 dan 10/10/PBI/2008 tentang penyelesaian nasabah, nasabah memiliki opsi untuk mengajukan pengaduan terhadap bank. Peraturan ini mengatur prosedur pengaduan nasabah. Bank harus menangani setiap keluhan yang diajukan oleh nasabah atau perwakilan mereka. Bank harus membuat prosedur dan kebijakan tertulis untuk menangani pengaduan. Prosedur ini harus mencakup hal-hal seperti menerima, mengelola, dan menyelesaikan pengaduan serta melakukan pengawasan proses, antara lain:

1) Pengaduan Secara Lisan: Nasabah dapat mengajukan pengaduan melalui telepon atau dengan mendatangi cabang bank terdekat. Layanan *switchboard* yang tersedia 24/24 juga dapat digunakan.
2) Pengaduan Tertulis: Nasabah memiliki banyak pilihan untuk mengajukan pengaduan tertulis. Ini termasuk mengajukan pengaduan resmi langsung ke bank melalui fax, surat, email, atau situs web bank. Selain itu, salinan identitas dan dokumentasi pendukung lainnya, seperti bukti setoran, penarikan, transfer,

rekening koran, dan catatan lain yang terkait dengan transaksi atau keluhan, harus disertakan dengan pengaduan tertulis.

3) Pengaduan oleh Perwakilan Nasabah: Dalam kasus di mana nasabah mengajukan pengaduan atas nama mereka, perwakilannya harus memberikan salinan dokumen identifikasi nasabah serta surat kuasa yang menunjukkan kemampuan hukum perwakilan untuk bertindak atas nama nasabah. Jika perwakilan adalah organisasi atau badan hukum, harus ada konfirmasi tertulis dari orang yang berwenang mewakili entitas tersebut.

4) Bank Menerima Pengaduan: Bank menerima pengaduan secara tertulis atau lisan. Pada saat pengaduan diajukan, bank memberikan penjelasan tentang kebijakan dan cara penyelesaian pengaduan kepada nasabah atau perwakilan nasabah. Pengaduan nasabah dapat diterima di kantor bank mana pun.

5) Prosedur Konsiliasi: Peraturan Bank Indonesia No. 08/5/PBI/2006 *juncto* Peraturan Bank Indonesia No. 10/10/PBI/2008 mengatur prosedur konsiliasi bank. Persyaratan untuk proses ini termasuk penandatanganan perjanjian konsiliasi, pengajuan dokumen penyelesaian sengketa, dan pelaksanaan proses konsiliasi. Karena pentingnya konsumen dalam industri perbankan, konsumen harus mendapat perhatian khusus dan perlindungan hukum (Kusuma & SH, 2019). Perlindungan nasabah berfokus pada ketentuan hukum dan perjanjian yangmengatur hubungan antara bank dan nasabah. Perjanjian ini dapat berbentuk akta di bawah tangan atau otentik.

Menurut Pasal 4 Ayat 4 UU Data Pribadi, Pengontrol Data Pribadi adalah kelompok orang, pemerintah, dan organisasi internasional yang bertanggung jawab untuk menentukan alasan mengapa mereka memiliki data dan bagaimana mereka menanganinya. Sesuai dengan Pasal 20 Ayat 2 Huruf a UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi, pengelola data harus mendapatkan persetujuan yang jelas dan sah dari pihak yang bersangkutan sebelum mengolah data pribadi untuk satu atau lebih tujuan tertentu. Oleh karena itu, pengelola data harus memiliki alasan yang sah untuk mengolah data pribadi.

Selama mereka memiliki persetujuan tertulis dari nasabah, lembaga keuangan dapat mengungkapkan informasi pribadi nasabah untuk tujuan bisnis, meskipun informasi ini harus disimpan sebagai rahasia. Namun, lembaga keuangan hanya dapat mengungkapkan informasi pribadi nasabah untuk tujuan bisnis, dan mereka harus mendapatkan persetujuan nasabah dan menjelaskan mengapa mereka melakukannya. Sangat penting bagi bank untuk melindungi data pribadi nasabah, termasuk informasi keuangan dan pribadi mereka, karena mereka diwajibkan untuk melakukannya. Lima prinsip konseptual yang digunakan untuk melindungi kerahasiaan keuangan nasabah bank, menurut Bambang Setioprodjo (Satjipto, 2000):

1. Menghormati Privasi: Setiap orang memiliki hak atas privasi yang harus dihormati.
2. Perlindungan terhadap Hak-hak Nasabah: Sesuai dengan ketentuan perjanjian nasabah-bank, bank harus memperhatikan kepentingan nasabah.
3. Perlindungan Data Pribadi: Nasabah berhak atas perlindungan data pribadi mereka oleh bank sesuai dengan Undang-Undang No. 10 Tahun 1998 tentang Perubahan atas Undang-Undang No. 07 Tahun 1992 tentang Perbankan.
4. Praktik Umum: Konsep ini diterapkan secara teratur oleh sektor keuangan.

Dalam waktu maksimal 72 jam, Bank Syariah Indonesia diharuskan untuk memberikan notifikasi tertulis kepada subjek data pribadi nasabah Bank BSI dan institusi terkait. Untuk sebagian besar, pemberitahuan tersebut harus mencakup informasi tentang data pribadi yang bocor, bagaimana dan kapan data tersebut bocor, dan tindakan yang diambil oleh pengontrol data pribadi untuk mengelola dan memulihkan data yang terpengaruh. Ada lembaga yang diberi wewenang untuk melindungi data pribadi, seperti yang dinyatakan dalam pemberitahuan kepada lembaga sesuai dengan Pasal 46 ayat (1). Pasal 58 memberikan informasi dan bantuan tambahan mengenai hal ini. Pasal ini menetapkan bahwa badan ini akan memiliki wewenang dan tanggung jawab, dan akan melapor langsung kepada presiden dan ditunjuk oleh presiden. Beberapa tanggung jawab yang terkait dengan perlindungan informasi pribadi adalah sebagai berikut:

a) Membuat dan menetapkan rencana dan pedoman yang berfungsi sebagai aturan bagi mereka yang mengontrol, memproses, dan menerima data pribadi;
b) Mengawasi pelaksanaan perlindungan data pribadi;
c) Menerapkan hukuman administrative atas pelanggaran ini; dan
d) Memfasilitasi penyelesaian sengketa di luar pengadilan.

Bank Syariah Indonesia harus melakukan hal-hal berikut sebagai bagian dari tanggung jawabnya:

a) Membuat dan menetapkan kebijakan yang berkaitan dengan perlindungan data pribadi;
b) Memantau ketaatan pengendali data pribadi;
c) Menerapkan sanksi administratif terhadap pelanggaran perlindungan data pribadi yang dilakukan oleh pengendali dan/atau pengolah data; dan
d) Membantu penegak hukum melakukan penyidikan atas dugaan tindak pidana yang diduga dilakukan oleh pengendali data pribadi.

B. Mekanisme Penegakan Hukum Dan Sanksi Yang Diberikan Jika Pemegang Data Melanggar Ketentuan Dalam Undang-Undang Perlindungan Data Pribadi Yang Mengalami Kebocoran Data

Undang-Undang Perlindungan Data Pribadi di Indonesia mengatur sanksi administratif dan pidana bagi pelanggaran terhadap ketentuan perlindungan data pribadi, mencakup hal berikut:

1. Jenis Data Pribadi
    a) Data Pribadi Spesisfik mencakup data kesehatan, data biometric, data genetic, riwayat kriminal, data anak, data pribadi, dan/atau data lain yang diatur oleh undang-undang;
    b) Data pribadi umum terdiri dari informasi seperti nama lengkap, jenis

kelamin, kewarganegaraan, agama, status perkawinan, dan/atau jenis informasi pengenal lainnya.

2. Larangan Penggunaan Data Pribadi
    a) Mendapatkan atau mengumpulkan Data Pribadi tentang orang lain tanpa izin untuk menggunakan untuk keuntungan mereka sendiri atau orang lain adalah illegal;
    b) Tidak boleh memberikan data pribadi yang tidak mereka butuhkan;
    c) Dilarang menggunakan informasi pribadi orang lain.
3. Sanksi Pidana
    a) Setiap orang yang dengan sengaja dan melawan hukum memperoleh atau mengumpulan Data Pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian pada subjek Data Pribadi sebagaimana dimaksud dalam Pasal 65 ayat (1) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp. 5.000.000.000,00 (lima miliar rupiah);
    b) Setiap orang yang dengan sengaja dan melawan hukum mengungkapkan Data Pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 65 ayat (2) dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau pidana denda paling banyak Rp. 4.000.000.000,00 (empat miliar rupiah);
    c) Setiap orang yang dengan sengaja dan melawan hukum menggunakan Data Pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 65 ayat (3) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp. 5.000.000.000,00 (lima miliar rupiah);
    d) Setiap orang yang dengan sengaja membuat Data Pribadi palsu atau memalsukan Data Pribadi dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian bagi orang lain

sebagaimana dimaksud dalam Pasal 66 dipidana dengan pidana penjara paling tama 6 (enam) tahun dan/atau pidana denda paling banyak Rp. 5.000.000.000,00 (enam miliar rupiah).

Dalam era digital saat ini, perlindungan data pribadi menjadi semakin penting karena ancaman kebocoran data yang kian meningkat. Pasal 26 Undang-Undang Informasi dan Transaksi Elektronik, menegaskan bahwa siapa pun memiliki hak untuk menuntut penyalahgunaan informasi pribadi tanpa persetujuan mereka. Pelanggaran terhadap Perlindungan Data Pribadi dapat digugat baik sebagai perbuatan melawan hukum (PMH). Berdasarkan Pasal 1365 Kitab Undang-Undang Hukum Perdata (KUH Perdata) maupun karena ketidakmampuan atau kelalaian sesuai Pasal 1366 KUH Perdata. Selain itu, Pasal 3 Undang-Undang Informasi dan Transaksi Elektronik menegaskan prinsip kehati-hatian, yang mengharuskan semua Penyelenggara Sistem Elektronik, termasuk perusahaan dan pemerintah, untuk menjalankan sistem elektronik yang aman dan dapat dipercaya, serta bertanggung jawab atas kerahasiaan data pribadi pengguna.

Sebagai contoh, Bank Syariah Indonesia (BSI) harus mengambil berbagai langkah penting untuk mengatasi masalah kebocoran data nasabah. Untuk mengurangi dampak negatif yang mungkin dialami oleh pengendali, pemroses, dan subjek data, BSI perlu menentukan penyebab kebocoran data secara transparan. Selain itu, BSI harus memastikan bahwa semua data kredensial, termasuk kata sandi dan PIN, diperbarui guna mencegah akses yang tidak sah oleh pihak yang tidak bertanggung jawab. Langkah-langkah ini merupakan bagian dari upaya untuk meningkatkan keamanan data pribadi dan menjaga kepercayaan nasabah. (*BSI Didesak Transparan Soal Dugaan Kebocoran Data Nasabah - Teknologi Katadata.co.id*, t.t.).

PENUTUP

Penulis menyimpulkan dari tulisan-tulisan di atas, jika Data Pribadi nasabah dalam perbankan tidak terlindungi, nasabah memiliki beberapa upaya hukum yang dapat dilakukan. Pertama, Nasabah harus mendeteksi dan mendokumentasikan

pelanggaran yang terjadi, serta melaporkannya kepada Bank terkait untuk dilakukan investigasi. Jika langkah ini tidak memadai, nasabah dapat melaporkan insiden tersebut kepada otoritas yang berwenang seperti Otoritas Jasa Keuangan (OJK) dan Bank Indonesia (BI). Konsultasi dengan pengacara juga sangat dianjurkan untuk mendapatkan nasihat hukum mengenai hak-hak nasabah dan langkah-langkah hukum yang dapat diambil. Jika perlu, nasabah dapat mengajukan gugatan hukum terhadap bank di pengadilan untuk mendapatkan kompensasi atas kerugian yang dialami. Pemegang data yang melanggar ketentuan dalam Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi dan mengalami kebocoran data memiliki tanggung jawab hukum yang signifikan. Mereka dapat digugat secara Perbuatan Melawan Hukum (PMH) berdasarkan Pasal 1365 Kitab Undang-Undang Hukum Perdata (KUH Perdata) atau karena ketidakmampuan atau kelalaian sesuai Pasal 1366 KUH Perdata. Selain itu, prinsip kehati-hatian yang diatur dalam Pasal 3 Undang-Undang Informasi dan Transaksi Elektronik, mengharuskan Penyelenggara Sistem Elektronik, termasuk perusahaan dan pemerintah, untuk menjalankan sistem yang aman dan dapat dipercaya. Apabila kebocoran data terjadi, pemegang data harus mengambil langkah-langkah yang diperlukan untuk mengatasi dampak negatif yang mungkin dialami oleh subjek data dan memastikan perlindungan yang memadai terhadap Data Pribadi.

DAFTAR PUSTAKA

BSI Didesak Transparan Soal Dugaan Kebocoran Data Nasabah – Teknologi Katadata.co.id. (t.t.). Diambil 26 Juli 2024.

Djoni, G. S., & Rachmadi, U. (2010). Hukum Perbankan. *Jakarta: Sinar Grafika*.

Duata, M. I., Ridanhus, F., & Tarina, D. D. Y. (2023). PERLINDUNGAN HUKUM TERHADAP DATA DIRI NASABAH BANK PADA KASUS BANK SYARIAH INDONESIA. *NUSANTARA: Jurnal Ilmu Pengetahuan Sosial*, *10*(11), 4979–4989.

Hermansyah, S. H., & Hum, M. (2005). Hukum perbankan nasional Indonesia. *Jakarta: Kencana Predana Media Group*.

Kitab Undang-Undang Hukum Perdata.

Kusuma, M. J., & SH, M. (2019). *Hukum perlindungan nasabah bank: Upaya hukum melindungi nasabah bank terhadap tindak kejahatan ITE di bidang perbankan*. Nusamedia.

Pasal 19 Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi Pasal 40 ayat (1) UU No. 10 Tahun 1998 tentang Perubahan atas UU No. 07 Tahun 1992 tentang Perbankan.

Putri, D. D. F., & Fahrozi, M. H. (2021). Upaya Pencegahan Kebocoran Data Konsumen Melalui Pengesahan Ruu Perlindungan Data Pribadi (Studi Kasus E-Commerce Bhinneka. Com). *Borneo Law Review*, *5*(1), 46–68.

Ramadhani, T. R., Brawijaya, A., & Aziz, I. A. (2021). Peran Lembaga Alternatif Penyelesaian Sengketa Perbankan Indonesia (LAPSPI) Dalam Penyelesaian Sengketa Pembiayaan Di Bank Syariah. *Tawazun: Journal of Sharia Economic Law*, *4*(1).

Redaksi. (t.t.). *BSI Diserang Ransomware, Nasib Uang Nasabah Gimana?* CNBC Indonesia. Diambil 25 Juli 2024, dari https://www.cnbcindonesia.com/tech/20230510174928-37-436279/bsi-diserang-ransomware-nasib-uang-nasabah-gimana

Satjipto, R. (2000). Ilmu hukum. *Bandung: Citra Aditya Bakti*.

Satrio, M. B., & Widiatno, M. W. (2020). Perlindungan Hukum Terhadap Data Pribadi Dalam Media Elektronik (Analisis Kasus Kebocoran Data Pengguna Facebook Di Indonesia). *JCA of Law*, *1*(1).

Sutedi, A. (2007). Hukum Perbankan Suatu Tinjauan Pencucian Uang. *Merger, Likuidasi, dan Kepailitan, Sinar Grafika, Jakarta*.

Undang-Undang No. 09 Tahun 2016 Tentang Infomasi Dan Transaksi Elektronik. Undang-Undang No. 10 Tahun 1998 tentang Perbankan.

Undang-Undang No. 21 Tahun 2008 tentang Perbankan Syariah. Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi.

Wisnubroto, A. (2010). *Strategi Penanggulangan Kejahatan Telematika*. Universitas Atma Jaya Yogyakarta.