Indonesian Journal of Law and Justice Volume: 3, Number 1, 2025, *Page*: 1-17

Tanggung Jawab Bank BSI Atas Kebocoran Data Nasabah

Muhammad Azfar Mulya Pratama[1]*, Pramukhtiko Suryokencono[2]

1,2 Universitas Muhammadiyah Jember

DOI: https://doi.org/10.47134/ijlj.v3i1.4804
*Correspondence: Muhammad Azfar Mulya Pratama
Email: azfarmuhammadpratama@gmail.com

Received: 05-07-2025
Accepted: 16-08-2025
Published: 28-09-2025

Abstrak: Penelitian ini menelaah tanggung jawab hukum Bank Syariah Indonesia (BSI) atas kasus kebocoran data nasabah pada Mei 2023 yang dikaitkan dengan kelompok peretas LockBit 3.0. Peristiwa tersebut menimbulkan kerugian material maupun immaterial bagi nasabah sekaligus menyoroti lemahnya perlindungan hukum di sektor perbankan digital. Penelitian ini bertujuan untuk menganalisis sejauh mana kewajiban hukum BSI sebagai pengendali data pribadi dapat ditegakkan serta mengevaluasi kemungkinan penerapan pertanggungjawaban pidana korporasi. Metode penelitian menggunakan pendekatan yuridis normatif dengan teknik deduktif-sintesis. Kajian dilakukan melalui *statute approach* dengan menelaah Undang-Undang Perlindungan Data Pribadi (UU No. 27 Tahun 2022), Undang-Undang Informasi dan Transaksi Elektronik, serta POJK No. 38/POJK.03/2016. Selain itu, digunakan pendekatan konseptual untuk mengulas doktrin hukum mengenai perlindungan data dan corporate criminal liability, serta pendekatan historis untuk menelusuri perkembangan regulasi. Analisis dilakukan tidak hanya pada teks hukum, tetapi juga praktik implementasi dan peran lembaga pengawas. Hasil penelitian menunjukkan BSI bahwa memiliki kewajiban hukum menjaga kerahasiaan, integritas, dan ketersediaan data nasabah. Namun, pelaksanaan regulasi belum optimal akibat keterbatasan infrastruktur, minimnya audit keamanan, lemahnya akuntabilitas, dan kurangnya koordinasi dengan otoritas eksternal. Dari sisi hukum pidana, bank dapat dimintai pertanggungjawaban korporasi apabila terbukti lalai mengantisipasi dan menangani insiden siber. Kesimpulannya, perlindungan data perbankan di Indonesia masih menghadapi hambatan normatif maupun praktis. Oleh karena itu, penguatan regulasi, penerapan prinsip kehati-hatian, penegakan doktrin corporate criminal liability, peningkatan kapasitas lembaga pengawas, serta transparansi, akuntabilitas, edukasi, inovasi, dan mekanisme pemulihan efektif diperlukan. Partisipasi masyarakat, dukungan teknologi modern, serta konsistensi pengawasan menjadi faktor vital menjaga kepastian hukum, stabilitas, dan kepercayaan publik terhadap sistem perbankan nasional.

Kata Kunci: Tanggung jawab hukum; Kebocoran data pribadi; Bank Syariah Indonesia (BSI)

Abstract This research examines the legal responsibility of Bank Syariah Indonesia (BSI) for the customer data breach in May 2023, which was linked to the LockBit 3.0 hacker group. This event caused both material and immaterial losses for customers and also highlighted the weak legal protection in the digital banking sector. This research aims to analyze the extent to which BSI's legal obligations as a personal data controller can be enforced and to evaluate the possibility of applying corporate criminal liability. The research method uses a normative juridical approach with deductive-synthetic techniques. The study was conducted thru a statute approach by examining the Personal Data Protection Law (Law No. 27 of 2022), the Electronic Information and Transactions Law, and POJK No. 38/POJK.03/2016. Additionally, a conceptual approach was used to review legal doctrines regarding data protection and corporate criminal liability, and a historical approach was used to trace the development of regulations. The analysis was conducted not only on legal texts, but also on implementation practices and the role of supervisory bodies. The research results show that BSI has a legal obligation to maintain the confidentiality, integrity, and availability of customer data. However, the implementation of the regulations has not been optimal due to limited infrastructure, a lack of security audits, weak accountability, and insufficient coordination with external authorities. From a criminal law perspective, banks can be held corporately liable if proven negligent in anticipating and handling cyber incidents. In conclusion, banking data protection in Indonesia still faces both normative and practical obstacles. Therefore, strengthening regulations, applying the principle of prudence,

enforcing the doctrine of corporate criminal liability, increasing the capacity of supervisory institutions, and promoting transparency, accountability, education, innovation, and effective recovery mechanisms are necessary. Community participation, support for modern technology, and consistent supervision are vital factors in maintaining legal certainty, stability, and public trust in the national banking system.

Keywords: *Legal responsibility; Personal data breach;* Bank Syariah Indonesia (BSI)

Pendahuluan

Era digital telah menghadirkan perubahan signifikan pada industri perbankan. Selama dua dekade terakhir, proses digitalisasi di sektor ini mengalami perkembangan yang sangat cepat. Sebagai institusi keuangan, bank memiliki peran penting untuk memastikan kerahasiaan serta keamanan data nasabah tetap terjaga agar tidak dimanfaatkan secara tidak semestinya oleh pihak yang tidak berwenang.

Perkembangan layanan perbankan digital kini menjadi penopang utama aktivitas transaksi dalam perekonomian modern. Di Indonesia, adopsi teknologi digital di sektor perbankan terus mengalami lonjakan yang cukup besar. Berdasarkan laporan Bank Indonesia, nilai transaksi digital banking pada April 2024 tercatat mencapai Rp5.335,33 triliun, atau meningkat 17,19% dibandingkan periode yang sama tahun sebelumnya (year on year) (Martha Herlinawati Simanjuntak, 2024), mengindikasikan semakin tingginya ketergantungan masyarakat pada layanan perbankan daring.

Insiden kebocoran data nasabah yang menimpa Bank Syariah Indonesia (BSI) menarik perhatian masyarakat dan menimbulkan perdebatan mengenai tanggung jawab bank dalam menjaga kerahasiaan informasi pribadi nasabah.

Bank Syariah Indonesia (BSI), yang menempati posisi sebagai salah satu institusi perbankan syariah terbesar di Indonesia, dilaporkan mengalami gangguan sistem pada Mei 2023. Insiden tersebut diduga menyebabkan kebocoran data nasabah setelah kelompok peretas LockBit 3.0 mengklaim telah mengakses sekitar 1,5 terabyte data yang mencakup informasi pribadi, catatan transaksi, dan kredensial pegawai (CNN Indonesia, 2023).

Peristiwa ini membawa konsekuensi besar, tidak hanya terhadap operasional lembaga perbankan, tetapi juga terhadap tingkat kepercayaan masyarakat pada sistem keamanan perbankan syariah di Indonesia. Dari sisi hukum, isu kebocoran data pribadi telah mendapatkan perhatian melalui sejumlah regulasi, di antaranya Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) beserta perubahannya dalam UU Nomor 19 Tahun 2016, serta Undang-Undang Nomor 27 Tahun 2022 mengenai Pelindungan Data Pribadi (UU PDP).

Undang-Undang Perlindungan Data Pribadi (UU PDP) melalui Pasal 57 serta Pasal 67 hingga Pasal 70 menetapkan adanya sanksi administratif maupun pidana bagi pelanggaran terkait data pribadi (UU No. 27 Tahun 2022 tentang PDP). Meski demikian, implementasinya masih menghadapi kekosongan norma dan ketidakpastian mekanisme pertanggungjawaban, terutama terhadap lembaga berisiko tinggi seperti bank digital yang rawan mengalami pelanggaran data.

Pasal 26 ayat (1) UU ITE menegaskan bahwa setiap individu berhak memperoleh perlindungan atas data pribadinya dalam sistem elektronik. Aturan tersebut menyatakan bahwa, kecuali diatur lain dalam peraturan perundang-undangan, pemanfaatan informasi elektronik yang berkaitan dengan data pribadi seseorang hanya dapat dilakukan apabila telah mendapatkan persetujuan dari pihak yang bersangkutan (UU No. 19 Tahun 2016 sebagai perubahan atas UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik). Selain itu, ketentuan ini diperkuat melalui Pasal 14 dan Pasal 29 ayat (1) UU Perlindungan Data Pribadi, yang mewajibkan pengendali data pribadi untuk menjamin ketepatan, kelengkapan, dan konsistensi data sesuai dengan aturan hukum yang berlaku.(Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang PDP, 2022).

Belum adanya regulasi teknis khusus yang mengatur standar keamanan sistem elektronik di perbankan digital menyebabkan tanggung jawab atas kebocoran data masih multitafsir. Ini berdampak pada posisi nasabah yang dirugikan, membuat mereka lemah dalam proses hukum dan penyelesaian sengketa.

Perlindungan hukum bagi nasabah terkait kejahatan siber saat ini masih cenderung fokus pada pencegahan. Upaya yang dilakukan umumnya berupa edukasi kepada nasabah dan penguatan sistem keamanan internal di lembaga keuangan. Namun, mekanisme penindakan atau pemulihan setelah terjadinya kejahatan siber, seperti ganti rugi dan penentuan pertanggungjawaban hukum, dinilai belum berjalan efektif. Ini berarti nasabah masih kesulitan mendapatkan hak mereka setelah menjadi korban.

Di samping itu, Peraturan Otoritas Jasa Keuangan (POJK) No. 38/POJK.03/2016 mengenai Penerapan Manajemen Risiko pada Pemanfaatan Teknologi Informasi oleh Bank Umum, pada dasarnya mengatur kewajiban setiap bank untuk memastikan adanya sistem keamanan yang memadai guna melindungi data nasabah. Lebih lanjut, Pasal 16 secara khusus mengatur bahwa.

Bank berkewajiban memastikan pelaksanaan pengamanan informasi secara optimal dengan memperhatikan hal-hal berikut:

a. perlindungan informasi untuk menjamin kerahasiaan (*confidentiality*), keutuhan (*integrity*), serta ketersediaannya (*availability*) secara efektif, efisien, dan sesuai dengan ketentuan yang berlaku;
b. penerapan pengamanan informasi yang mencakup aspek teknologi, sumber daya manusia, serta proses dalam pemanfaatan Teknologi Informasi;
c. penerapan pengamanan informasi yang didasarkan pada hasil penilaian risiko (risk assessment) terhadap informasi yang dimiliki Bank;
d. penyediaan mekanisme manajemen insiden guna mendukung perlindungan informasi. (Peraturan Otoritas Jasa Keuangan Nomor 38/POJK.03/2016 Tahun 2016, n.d.).

selanjutnya, pasal 19 menekankan kewajiban bank dalam mengembangkan serta menyediakan Teknologi Informasi dengan disertai penerapan langkah-langkah pengendalian guna memastikan kerahasiaan dan integritas sistem maupun data, termasuk data nasabah. Sementara itu, Pasal 22 mengharuskan bank melakukan evaluasi mandiri terkait tingkat kematangan keamanan siber yang dimilikinya.

Namun, meskipun regulasi telah tersedia, implementasi dan efektivitas pengawasan masih menjadi tantangan besar. Kasus kebocoran data BSI menimbulkan pertanyaan hukum terkait sejauh mana tanggung jawab bank dalam insiden kebocoran data tersebut.

Apakah bank dapat dikenakan sanksi hukum jika terbukti lalai dalam menjaga keamanan data nasabah? Bagaimana penerapan prinsip kehati-hatian dalam industri perbankan dalam konteks perlindungan data pribadi? Dan yang lebih penting, bagaimana sistem hukum Indonesia saat ini mampu memberikan perlindungan yang optimal bagi nasabah dalam menghadapi ancaman kejahatan siber di sektor keuangan?

Beberapa tantangan utama yang dihadapi dalam penelitian ini adalah lemahnya sistem keamanan perbankan yang masih rentan terhadap serangan siber, kesenjangan antara regulasi dan implementasi di lapangan, serta kurangnya kesadaran nasabah terhadap pentingnya perlindungan data pribadi.

Sejumlah penelitian sebelumnya telah mengulas permasalahan terkait kebocoran data serta aspek perlindungan hukum di sektor perbankan. Penelitian yang dilakukan oleh Muhammad Esza Maulana Firmanda, Taufik Kukuh Efendi, Fathor Rozy Alfarisy, Alfado Chievo Javantara, dan Rachma Indrarini (2024) menelaah penerapan kebijakan perlindungan nasabah pada bank digital syariah di Indonesia. Kajian tersebut berfokus pada regulasi OJK, prinsip perlindungan konsumen syariah, serta peran efektivitas pengawasan internal di era digital. Namun, penelitian ini belum secara mendalam membahas mengenai tanggung jawab bank ketika terjadi kebocoran data (Kukuh Efendi et al., 2024).

Sementara itu, penelitian oleh Wyanda Kinanti Syauqi Ramadhan, Sidi Ahyar Wiraguna (2025) menyoroti implementasi UU PDP dalam industri keuangan, tetapi lebih banyak membahas regulasi dibandingkan dengan kasus konkret seperti kebocoran data BSI(Kinanti et al., 2025).

Meskipun telah ada berbagai penelitian terkait kebocoran data dan regulasi perlindungan data pribadi, masih terdapat kesenjangan dalam penelitian mengenai tanggung jawab spesifik bank dalam kasus kebocoran data di Indonesia. Sebagian besar penelitian sebelumnya hanya menyoroti aspek teknis keamanan data atau regulasi secara umum tanpa mengaitkannya secara mendalam dengan studi kasus spesifik seperti kebocoran data BSI.

Penelitian ini diharapkan dapat memberi sumbangan akademis melalui kajian sistematis mengenai ketentuan hukum terkait tanggung jawab bank atas kebocoran data nasabah. Metode yang dipakai adalah yuridis normatif, dengan menitikberatkan pada analisis terhadap peraturan perundang-undangan yang berlaku.

Dalam hal ini, penting pula untuk meninjau peran bank sebagai pengendali data pribadi (*data controller*) sebagaimana diatur dalam UU PDP pasal 1 angka 4. Bank tidak hanya memiliki tanggung jawab teknis untuk melindungi data, tetapi juga tanggung jawab hukum apabila terjadi pelanggaran, baik karena serangan dari luar maupun akibat kelalaian internal(Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang PDP, 2022).

Penyelenggaraan sistem elektronik oleh bank, termasuk mekanisme enkripsi, otorisasi akses, serta audit berkala terhadap sistem keamanan, menjadi bagian dari tanggung jawab hukum yang tidak bisa diabaikan(PERBANAS, 2024). Dalam praktiknya, kelemahan infrastruktur, kurangnya kapasitas sumber daya manusia, serta belum maksimalnya regulasi sektoral turut memperbesar risiko kebocoran data.

Kondisi ini menunjukkan bahwa perlindungan data pribadi tidak cukup hanya dengan regulasi normatif, tetapi juga membutuhkan sistem pertanggungjawaban pidana yang tegas dan dapat diterapkan secara efektif terhadap institusi yang melanggar(RRR Runtuwene, 2017). Dalam perspektif hukum pidana, apabila kelalaian bank dalam menjaga data menyebabkan kerugian terhadap nasabah, maka dimungkinkan untuk menerapkan pertanggungjawaban pidana korporasi.

Hal ini penting untuk menciptakan efek jera serta mendorong bank agar lebih serius dalam membangun sistem keamanan siber yang kuat dan akuntabel. Di sisi lain, kasus BSI menunjukkan bahwa masyarakat masih belum memiliki mekanisme pemulihan yang jelas ketika menjadi korban kebocoran data(CNN Indonesia, 2023). Banyak nasabah yang tidak tahu ke mana harus melapor atau bagaimana proses hukum bisa ditempuh untuk menuntut pertanggungjawaban bank.

Selain itu, belum adanya lembaga independen khusus yang menangani sengketa data pribadi membuat penyelesaian kasus seperti ini berlarut-larut dan cenderung tidak transparan. Dengan demikian, penelitian ini memiliki urgensi untuk dilakukan mendorong penguatan regulasi, memperjelas dasar hukum pertanggungjawaban pidana bank dalam kebocoran data, serta membangun kerangka hukum yang mampu melindungi nasabah sebagai pemilik data pribadi.

Dengan menggunakan pendekatan statute approach, penelitian ini tidak hanya berfokus pada kajian normatif, melainkan juga menelaah sejauh mana peraturan yang ada dapat diimplementasikan secara nyata dalam kasus kebocoran data, khususnya pada lembaga keuangan seperti Bank Syariah Indonesia. Selain aspek hukum perdata dan administrasi, peristiwa kebocoran data nasabah bank seperti yang dialami Bank Syariah Indonesia (BSI) juga penting dikaji dari perspektif hukum pidana.

Hal ini dikarenakan kebocoran data yang mengakibatkan kerugian bagi nasabah dapat memenuhi unsur-unsur tindak pidana, terutama jika kebocoran tersebut disebabkan oleh kelalaian berat atau adanya unsur kesengajaan dari pihak internal maupun eksternal bank. Dalam konteks ini, penting untuk menelaah kemungkinan penerapan pertanggungjawaban pidana baik terhadap individu pelaku maupun terhadap korporasi (bank) dalam kedudukan sebagai pihak yang dapat dikenai hukum pidana.

Dalam perkembangan hukum pidana modern, termasuk di Indonesia, telah dikenal konsep pertanggungjawaban pidana korporasi. Doktrin ini memungkinkan badan hukum, seperti bank, untuk dikenakan sanksi pidana apabila terbukti melakukan atau terlibat dalam suatu tindak pidana. Ketentuan tersebut tertuang dalam Pasal 46 ayat (1) dan (2) Undang-Undang Nomor 1 Tahun 2023 yang menegaskan bahwa korporasi dapat dipidana jika tindak pidana dilakukan atas nama maupun untuk kepentingan korporasi, serta masih

berkaitan dengan kegiatan usahanya (Undang-Undang (UU) Nomor 1 Tahun 2023 Kitab Undang-Undang Hukum Pidana, 2023).

Selain itu, Pasal 67 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi menegaskan bahwa apabila pelanggaran data pribadi dilakukan oleh suatu korporasi, maka sanksi pidana dapat dikenakan terhadap badan usaha tersebut maupun para pengurusnya, berupa pidana denda maupun sanksi administratif lain, termasuk penghentian kegiatan usaha atau pencabutan izin (Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang PDP, 2022).

Dengan demikian, bank sebagai badan usaha dapat dimintai pertanggungjawaban pidana apabila sistem keamanan yang digunakan terbukti tidak memenuhi standar kewajaran atau jika terdapat kelalaian struktural dan pembiaran terhadap praktik-praktik yang memungkinkan terjadinya kebocoran data, Baik dalam bentuk langsung maupun tidak langsung, sesuai dengan ketentuan yang berlaku dalam peraturan perundang-undangan.

Hal ini menunjukkan bahwa peran bank bukan hanya sebagai entitas ekonomi, tetapi juga sebagai subjek hukum yang bertanggung jawab atas dampak sosial dan hukum dari kegiatan operasionalnya. Di samping itu, masih terdapat celah dalam sistem perundang-undangan yang menyebabkan proses pembuktian dalam kasus pidana kebocoran data menjadi sulit dilakukan.

penelitian ini menjadi penting untuk menggali secara lebih mendalam bagaimana hukum pidana dapat diterapkan secara efektif terhadap institusi keuangan dalam konteks kebocoran data, serta bagaimana sistem pembuktian dapat diarahkan untuk menghadapi kompleksitas tindak pidana berbasis teknologi.

Metodologi

Metode adalah unsur krusial dalam penelitian karena setiap langkah penelitian tercermin melalui metode yang digunakan (Sudarto, 1996). Pemilihan metode yang sesuai dalam penelitian sangatlah penting untuk menggali kebenaran dalam karya ilmiah, sebab metode berperan sebagai landasan utama yang memengaruhi kualitas hasil penelitian.

Penulis dalam penelitian ini menggunakan pendekatan yuridis normatif dengan metode deduktif-sintesis. Pendekatan yuridis normatif berfokus pada kajian terhadap ketentuan hukum tertulis yang tercantum dalam peraturan perundang-undangan, putusan pengadilan, serta dokumen hukum resmi lainnya. Sementara itu, metode deduktif dipahami sebagai cara memperoleh pengetahuan ilmiah yang diawali dari hal-hal yang bersifat umum untuk kemudian ditarik menjadi kesimpulan yang bersifat khusus.

Dalam penelitian ini, penulis menggunakan 3 (tiga) pendekatan penelitian, yakni menggunakan Pendekatan Peraturan Perundang-Undangan *(Statuta Approach),* adalah suatu pendekatan penelitian yang dilakukan dengan menelaah suatu peraturan perundang-undangan yang berkaitan dengan permasalahan hukum yang sedang diteliti(Soekanto, 2009).

Untuk pendekatan kedua adalah pendekatan Konseptual, suatu pendekatan penelitian yang beranjak pada pandangan-pandangan dan doktrin-doktrin di dalam Ilmu Hukum(Rusdin Tahir, I Gde Pantja Astawa, Agus Widjajanto, Mompang L. Panggabean,

Moh. Mujibur Rohman, Ni Putu Paramita Dewi, Nandang Alamsah Deliarnoor, Muhamad Abas, Rizqa Febry Ayu, Ni Putu Suci Meinarni, Fatimah Hs, Ni Wayan Eka Sumartini, Dewi Kania Sugiha, 2023) . Pendekatan ketiga yang digunakan adalah **pendekatan historis**, yaitu suatu metode dalam penelitian hukum yang bertujuan untuk menelaah perjalanan perkembangan peraturan perundang-undangan, pemikiran doktrinal, maupun konsep-konsep hukum dari masa ke masa. Melalui cara ini, peneliti dapat menyingkap latar belakang lahirnya suatu norma hukum, memahami dinamika perubahannya, serta menggali maksud pembentuk undang-undang (legislative intent) dalam mengatur bidang tertentu. Misalnya, penelitian ini dapat menelusuri evolusi regulasi mengenai perlindungan data pribadi dan pertanggungjawaban pidana korporasi di Indonesia, mulai dari aturan-aturan awal yang belum secara eksplisit mengatur data pribadi, hingga ditetapkannya Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, serta melihat bagaimana regulasi tersebut beradaptasi dengan kemajuan teknologi informasi dan meningkatnya ancaman kejahatan siber.

Hasil dan Pembahasan

Bagaimana kronologi kasus kebocoran data bank BSI

Insiden peretasan data dialami oleh Bank Syariah Indonesia (BSI) pada Mei 2023. merupakan salah satu kasus siber terbesar yang menimpa industri perbankan di Indonesia. Kejadian ini bermula dari gangguan sistem yang dialami oleh nasabah, di mana layanan mobile banking tidak dapat diakses selama lebih dari tiga hari berturut-turut. Dalam kondisi normal, gangguan teknis mungkin saja terjadi, namun durasi gangguan ini memicu spekulasi luas akan adanya insiden siber besar(HUSAIN, 2025).

Kemudian terungkap bahwa insiden tersebut melibatkan kelompok peretas internasional bernama *LockBit*, yang diduga berhasil menyusup ke sistem BSI dan mengenkripsi data internal serta informasi pelanggan. Peretas meminta tebusan dan mengancam akan menyebarkan data jika permintaan mereka tidak dipenuhi. Aksi ini dikenal dengan istilah *ransomware attack*, sebuah metode kejahatan siber yang makin sering digunakan untuk menyerang institusi keuangan.

Kelompok *LockBit* mengklaim berhasil memperoleh lebih dari 15 juta data pelanggan, termasuk data pribadi seperti nama lengkap, nomor KTP, alamat, serta rincian transaksi. Data ini kemudian diklaim diunggah dalam forum gelap (*dark web*) dan ditawarkan kepada pihak ketiga jika tidak segera ditebus. Berdasarkan laporan CNN Indonesia, *LockBit* 3.0 diduga mencuri data dan *password* milik 15 juta nasabah Bank Syariah Indonesia (BSI) serta menuntut pembayaran tebusan dalam bentuk mata uang kripto untuk mencegah penyebaran data tersebut secara publik(CNN Indonesia, 2023).

Melalui keterangan resminya, BSI menyampaikan bahwa mereka telah berkoordinasi dengan Otoritas Jasa Keuangan (OJK), Bank Indonesia, serta Badan Siber dan Sandi Negara (BSSN) dalam menangani serangan tersebut. Namun, belum ada kejelasan terkait pembayaran tebusan. Sementara itu, masyarakat menekan pihak terkait untuk menunjukkan transparansi dan akuntabilitas atas insiden ini (Fatmala Putri & Ratna Sari, 2023).

Di ranah hukum, persoalan kebocoran data pribadi merupakan hal yang sangat penting karena dapat mencerminkan adanya kelemahan dalam sistem keamanan, yang menjadi tanggung jawab pokok pengendali data. Mengacu pada Pasal 1 angka 5 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, pengendali data pribadi adalah pihak yang berwenang menentukan tujuan serta mengendalikan proses pengelolaan data pribadi. Dengan demikian, Bank Syariah Indonesia (BSI) sebagai institusi yang mengolah dan menyimpan data nasabah, memiliki kewajiban hukum untuk menjamin keamanan serta perlindungan atas data yang dikelolanya.

Di samping UU PDP, perlindungan konsumen juga menjadi aspek yang terkena dampak. Berdasarkan Pasal 4 huruf a Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen, setiap konsumen memiliki hak atas rasa aman, nyaman, dan terlindungi ketika menggunakan barang maupun jasa, termasuk layanan di sektor perbankan. Apabila ketentuan ini dilanggar, maka dapat menimbulkan konsekuensi hukum baik dalam ranah perdata maupun pidana (Republik Indonesia, 1999).

Bank ini termasuk dalam jajaran lembaga keuangan terbesar di Indonesia seharusnya menerapkan sistem pengamanan yang mengacu pada standar internasional untuk menjaga kepercayaan publik. Berdasarkan hasil penelitian oleh Dewi Fatmala Putri dkk. Insiden gangguan layanan digital yang dialami Bank Syariah Indonesia (BSI) pada Mei 2023 menunjukkan masih lemahnya ketahanan terhadap serangan siber, termasuk minimnya kesiapan dalam menghadapi serangan ransomware dan potensi kebocoran data. Meski BSI mengklaim bahwa data nasabah tetap aman, kelompok ransomware LockBit mengaku telah mencuri 1,5 terabyte data dari BSI. Hal ini menunjukkan adanya potensi kegagalan dalam manajemen risiko serta terbatasnya investasi dalam penguatan keamanan digital(Fatmala Putri & Ratna Sari, 2023). ika tidak segera ditangani, kondisi ini dapat menciptakan preseden negatif bagi lembaga keuangan lainnya dan mengancam stabilitas sistem perbankan nasional secara keseluruhan.

Oleh karena itu, kronologi kebocoran data ini bukan sekadar narasi teknis, tetapi juga menjadi dasar analisis yuridis untuk menentukan sejauh mana kelalaian dapat diidentifikasi, dan bagaimana aspek pertanggungjawaban hukum dapat ditegakkan berlandaskan peraturan perundang-undangan yang berlaku di Indonesia.

Bagaimana Standar kemanan siber bank BSI bedasarkan POJK No. 38/POJK.03/2016

POJK No. 38/POJK.03/2016 mengenai Penerapan Manajemen Risiko pada Pemanfaatan Teknologi Informasi di Bank Umum berfungsi sebagai dasar hukum yang mewajibkan perbankan untuk menjalankan prinsip kehati-hatian serta pengendalian risiko TI secara menyeluruh. Aturan ini juga menegaskan peran direksi, kebijakan manajemen risiko, dan pelaksanaan kontrol internal atas penggunaan teknologi informasi sebagaimana diatur dalam Pasal 2 sampai Pasal 5 (Peraturan Otoritas Jasa Keuangan Nomor 38/POJK.03/2016 Tahun 2016, n.d.). Dalam konteks meningkatnya ketergantungan sektor perbankan terhadap sistem elektronik, peraturan ini menjadi penting dalam menghadapi kompleksitas ancaman siber.

Berdasarkan Pasal 10 ayat (1) POJK No. 38/POJK.03/2016 tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum, Setiap bank harus menetapkan kebijakan, standar, serta prosedur terkait pengelolaan risiko teknologi informasi. Ketentuan ini menekankan pentingnya tata kelola yang terstruktur dalam pengelolaan risiko yang muncul akibat penggunaan teknologi informasi, termasuk risiko kebocoran data, gangguan sistem, maupun serangan siber.

Meskipun pasal ini tidak secara eksplisit menyebutkan prinsip kerahasiaan, integritas, dan ketersediaan data (*CIA triad*), substansi pengaturan tersebut mengarah pada kewajiban bank untuk menjaga keamanan sistem informasinya secara menyeluruh. Dalam praktiknya, kebijakan yang dirancang sesuai dengan pasal ini harus mencakup Upaya perlindungan, pendeteksian, dan penanggulangan terhadap ancaman di bidang keamanan siber yang dapat merugikan bank maupun nasabah. Oleh karena itu, implementasi pasal ini merupakan elemen penting dalam menilai kesesuaian dan ketepatan langkah pengamanan data yang diterapkan oleh suatu bank.

Pasal 15 POJK 38/POJK.03/2016 mewajibkan Setiap bank diwajibkan memiliki Disaster Recovery Plan yang efektif serta melakukan uji coba secara rutin minimal satu kali dalam setahun pada seluruh aplikasi dan infrastruktur penting, dengan melibatkan para pengguna teknologi informasi (Peraturan Otoritas Jasa Keuangan Nomor 38/POJK.03/2016 Tahun 2016, n.d.). Peraturan ini mengharuskan pihak bank untuk menjamin perlindungan informasi dengan cara yang optimal.

Sementara itu, Pasal 16 mewajibkan bank untuk memastikan pengamanan informasi secara efektif, meliputi aspek kerahasiaan, integritas, dan ketersediaan data (*confidentiality, integrity, availability*), serta pengamanan terhadap teknologi, SDM, dan proses berdasarkan hasil *risk assessment*. Ketentuan ini juga menekankan pentingnya tersedianya manajemen penanganan insiden sebagai bagian dari sistem pengamanan informasi.

Namun demikian, hingga saat ini tidak ditemukan bukti publik terkait pelaksanaan audit eksternal keamanan siber yang dilakukan secara berkala oleh BSI, sebagaimana diamanatkan dalam kedua pasal tersebut. Ketiadaan dokumentasi atau laporan transparan mengenai uji coba dan evaluasi sistem pemulihan bencana, serta penanganan insiden, dapat menunjukkan ketidaksiapan bank dalam merespons ancaman siber, dan berpotensi mengindikasikan adanya kelalaian dalam memenuhi kewajiban regulasi yang berdampak hukum.

Ketiadaan transparansi atas hasil audit dan evaluasi risiko TI ini memperlihatkan potensi **kelalaian dalam manajemen risiko teknologi informasi.** Kelalaian tersebut diperparah oleh fakta bahwa serangan *ransomware* yang menimpa BSI berlangsung dalam waktu yang cukup lama, berdampak pada sistem layanan digital perbankan, dan disinyalir melibatkan pencurian data dalam jumlah besar. Dalam konteks ini, kegagalan untuk mendeteksi dan merespons secara cepat menunjukkan lemahnya **resiliensi siber** dan kemampuan mitigasi risiko bank terhadap ancaman digital yang semakin kompleks.

Lebih lanjut, dalam konteks hukum pidana, Pasal 15 ayat (1) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) menyatakan bahwa "Setiap Penyelenggara Sistem Elektronik harus menyelenggarakan Sistem

Elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya Sistem Elektronik sebagaimana mestinya." Ketentuan ini mencerminkan prinsip tanggung jawab objektif, di mana penyelenggara system termasuk bank sebagai badan hukum wajib menjamin keandalan dan keamanan sistem elektronik yang mereka operasikan.

Apabila kelalaian dalam sistem pengamanan ini menyebabkan kebocoran data atau kerugian bagi konsumen, maka penyelenggara dapat dimintai pertanggungjawaban secara hukum. Dalam konteks ini, Bank Syariah Indonesia (BSI) sebagai korporasi penyelenggara sistem elektronik dapat dimintai pertanggungjawaban apabila terbukti lalai dalam menjamin keamanan data pribadi nasabah. Hal ini sejalan dengan ketentuan UU ITE dan diperkuat oleh Pasal 70 UU PDP, yang memungkinkan pemidanaan terhadap korporasi yang melakukan pelanggaran atas kewajiban pengendalian data pribadi.

Kepatuhan terhadap POJK No. 38/POJK.03/2016 Ketentuan ini tidak hanya dimaksudkan sebagai formalitas administratif, melainkan juga berfungsi sebagai tolok ukur minimum dalam penerapan manajemen risiko teknologi informasi yang harus dipatuhi setiap bank. Sesuai Pasal 2 ayat (1), bank diwajibkan untuk menerapkan manajemen risiko terkait penggunaan teknologi informasi secara menyeluruh dan berkesinambungan, yang meliputi aspek strategi, struktur organisasi, kebijakan, hingga prosedur pengelolaan risiko. Jika bank tidak memiliki sistem tersebut atau lalai menyesuaikan kebijakan keamanannya dengan perkembangan ancaman, maka hal itu dapat dianggap sebagai pengabaian terhadap kewajiban hukum yang bersifat pencegahan.

Selain itu, Pasal 4 dan Pasal 5 POJK No. 38/2016 menetapkan tanggung Dewan Komisaris dan Direksi memiliki peran penting dalam menjamin penerapan manajemen risiko teknologi informasi berjalan secara optimal dan efisien, khususnya terkait insiden siber yang menimpa Bank Syariah Indonesia (BSI).

Hal ini juga sejalan dengan ketentuan Pasal 70 Undang-Undang No. 27 Tahun 2022 tentang Pelindungan Data Pribadi, yang menyatakan bahwa pertanggungjawaban pidana dapat dikenakan terhadap korporasi dan/atau pengurusnya jika terbukti melakukan pelanggaran hukum dalam pengendalian data pribadi.

Bagaimana Tanggung Jawab Hukum Pidana terhadap Bank Syariah Indonesia (BSI)

Tanggung jawab pidana korporasi dalam konteks kebocoran data menjadi isu krusial, terutama dalam era digital saat ini yang sangat bergantung pada keamanan informasi. Insiden kebocoran data yang melibatkan institusi keuangan seperti Bank Syariah Indonesia (BSI) bukan hanya mencerminkan kegagalan teknis, tetapi juga dapat menunjukkan kelalaian struktural dalam tata kelola dan sistem pengawasan internal.

Dalam hukum pidana korporasi Indonesia, doktrin vicarious liability dipahami sebagai konsep pertanggungjawaban pidana yang dialihkan, yakni ketika pihak atasan—baik perusahaan maupun pengelolanya—dapat dimintai tanggung jawab atas tindak pidana yang dilakukan oleh bawahan, sepanjang terdapat hubungan kerja dan perbuatan tersebut dilakukan dalam lingkup pekerjaannya (Hendriawan, 2022).

Setiap pelanggaran atas aturan perlindungan data pribadi dapat dikenakan sanksi pidana, dan tanggung jawab hukum bisa dibebankan kepada korporasi, pengurusnya, atau

keduanya sekaligus. Hal ini menunjukkan pengakuan tegas bahwa korporasi termasuk subjek hukum pidana yang dapat dimintai pertanggungjawaban, baik secara langsung maupun melalui tanggung jawab pengganti *vicarious*.

Selain itu, ketentuan Pasal 46 UU PDP mewajibkan pengendali data melaporkan insiden kebocoran data paling lambat 3x24 jam. Ketidakpatuhan terhadap kewajiban ini, seperti dugaan yang terjadi dalam kasus BSI, dapat dikategorikan sebagai tindak pidana. Maka, pertanggungjawaban tidak hanya dibebankan pada pelaku peretasan, melainkan juga pada institusi yang lalai memenuhi kewajiban hukumnya(Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang PDP, 2022).

Dalam regulasi perbankan di Indonesia, POJK No. 38/POJK.03/2016 menetapkan bahwa setiap bank harus mengimplementasikan manajemen risiko secara optimal dalam pemanfaatan teknologi informasi (TI). Kewajiban tersebut mencakup keterlibatan aktif Direksi serta Dewan Komisaris sebagaimana diatur pada Pasal 2 ayat (2) huruf a. Selanjutnya, Pasal 4 sampai Pasal 6 memberikan penguatan dengan menegaskan peran strategis dan fungsi pengawasan pengurus bank dalam penerapan manajemen risiko TI(Peraturan Otoritas Jasa Keuangan Nomor 38/POJK.03/2016 Tahun 2016, n.d.).

Secara normatif, POJK tersebut tidak secara eksplisit mengatur pertanggungjawaban pidana personal, namun Pasal 36 memberikan sanksi administratif yang dapat dikenakan secara individual kepada pengurus, termasuk pencantuman dalam daftar tidak lulus uji kemampuan dan kepatutan (*fit and proper test*). Ini menandakan perluasan pertanggungjawaban dari kelembagaan ke personalia, khususnya jika terjadi kegagalan pengawasan.(Peraturan Otoritas Jasa Keuangan Nomor 38/POJK.03/2016 Tahun 2016, n.d.)

Meskipun tidak secara langsung merujuk pada doktrin *corporate criminal liability*, struktur tanggung jawab yang dibangun POJK ini selaras dengan pendekatan pertanggungjawaban dalam hukum pidana korporasi, di mana individu dalam posisi pengawasan dapat dimintakan pertanggungjawaban jika lalai menjalankan fungsi pengendalian risiko.

Dengan demikian, pengurus bank harus menyadari bahwa kelalaian dalam pengawasan TI tidak hanya berdampak pada reputasi institusi, tetapi juga menimbulkan implikasi hukum administratif, dan dalam konteks tertentu, potensi pertanggungjawaban pidana.

Beberapa hambatan penerapan pertanggungjawaban pidana korporasi di Indonesia adalah lemahnya sumber daya penegak hukum serta tumpang tindih regulasi. Oleh karena itu, perlu harmonisasi regulasi dan penguatan kapasitas lembaga penegak hukum agar korporasi benar-benar dapat dimintai pertanggungjawaban secara efektif (Dr. H. Joko Sriwidodo, SH.MH.M.Kn.CLA, 2021).

Dengan demikian, pengurus korporasi, khususnya di sektor perbankan, harus menyadari bahwa kelalaian dalam pengawasan TI dapat berujung pada sanksi administratif hingga pidana. Untuk mendukung efektivitas penerapan pertanggungjawaban pidana korporasi, diperlukan harmonisasi regulasi serta penguatan kapasitas penegak hukum di Indonesia.

Sebagai penyelenggara sistem elektronik (PSE), Bank Syariah Indonesia (BSI) tunduk pada Undang-Undang Nomor 11 Tahun 2008 mengenai Informasi dan Transaksi Elektronik, yang kemudian mengalami perubahan melalui Undang-Undang Nomor 19 Tahun 2016, memuat aturan mengenai kewajiban serta tanggung jawab dari penyelenggara sistem elektronik (PSE). Hal ini secara khusus tercantum dalam Pasal 15 UU ITE disebutkan bahwa:

"Setiap Penyelenggara Sistem Elektronik wajib menyelenggarakan Sistem Elektronik secara andal dan aman serta bertanggung jawab atas berfungsinya Sistem Elektronik sebagaimana mestinya."(Undang-Undang (UU) Nomor 11 Tahun 2008 Informasi Dan Transaksi Elektronik, 2008)

Ketentuan ini menekankan kewajiban PSE termasuk bank, untuk menjamin keamanan, keandalan, dan integritas sistem informasi yang digunakan. Dalam konteks ini, kegagalan sistem akibat serangan siber, kebocoran data, atau gangguan layanan mencerminkan tidak terpenuhinya prinsip-prinsip keandalan dan keamanan sistem sebagaimana diwajibkan oleh UU ITE.

Kasus kebocoran data yang menimpa BSI pada tahun 2023 menjadi ilustrasi konkret dari dugaan pelanggaran terhadap Pasal 15 ini. Gangguan layanan dan dugaan kebocoran data yang berlangsung selama berhari-hari menunjukkan potensi kegagalan sistemik dalam infrastruktur digital bank tersebut. Hal ini menimbulkan pertanyaan serius mengenai kepatuhan BSI terhadap standar perlindungan data dan keamanan informasi yang diatur oleh hukum positif.

Lebih lanjut, Pasal 36 UU ITE menyatakan bahwa:

"Setiap orang yang dengan sengaja dan tanpa hak atau melawan hukum melakukan perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 34 yang mengakibatkan kerugian bagi orang lain dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah)."

Berikut juga unsur unsur utama dari ketentuan pasal 36:

1. Subjek Hukum

   Unsur ini menunjukkan bahwa subjek hukum yang dapat dimintai pertanggungjawaban tidak terbatas hanya pada warga negara Indonesia, tetapi juga termasuk badan hukum, organisasi, atau bahkan warga negara asing yang melakukan perbuatan tersebut dalam yurisdiksi hukum Indonesia.
2. Perbuatan Dengan Unsur Kesengajaan

   Unsur ini menegaskan bahwa tindak pidana dilakukan secara sadar, direncanakan, atau setidak-tidaknya dikehendaki oleh pelaku. Ini berarti, pelaku mengetahui bahwa tindakannya dapat menimbulkan akibat hukum dan tetap memilih untuk melakukannya.
3. Tanpa Hak atau Melawan Hukum

   Frasa ini menunjukkan bahwa perbuatan tersebut tidak didasarkan pada kewenangan hukum yang sah atau dilakukan dengan cara yang bertentangan dengan norma hukum, etika, atau kepatutan.
4. Perbuatan Pokok

Unsur ini mengacu pada tindakan-tindakan yang dikualifikasikan sebagai tindak pidana dalam pasal-pasal sebelumnya, seperti penyebaran konten bermuatan melanggar kesusilaan (Pasal 27), penghinaan/pencemaran nama baik (Pasal 27 ayat 3), intersepsi ilegal (Pasal 31), atau akses ilegal ke sistem elektronik (Pasal 30). Dengan kata lain, Pasal 36 bersifat pelengkap atau pemberat atas perbuatan yang telah dikualifikasi sebelumnya.

5. Akibat Hukum

Peraturan ini dijadikan landasan untuk pemberian sanksi pidana apabila terdapat tindakan melawan hukum dalam penyelenggaraan sistem elektronik yang menimbulkan kerugian bagi pihak lain. Dalam perkara BSI, apabila terbukti bahwa pengelolaan sistem elektronik tidak dilakukan secara andal maupun aman hingga merugikan nasabah (baik secara materiel maupun immateriel), maka bank dapat dimintai pertanggungjawaban sesuai dengan ketentuan Pasal 36.

Ketentuan ini menjadi dasar untuk menjatuhkan sanksi pidana apabila terdapat perbuatan melawan hukum dalam sistem elektronik yang mengakibatkan kerugian bagi pihak lain. Dalam kasus BSI, jika terbukti bahwa sistem elektronik dikelola secara tidak andal dan tidak aman hingga menyebabkan kerugian nasabah (baik materiel maupun immateriel), maka pihak bank dapat dimintai pertanggungjawaban berdasarkan ketentuan Pasal 36 tersebut.

Dengan demikian, jika dapat dibuktikan adanya kelalaian atau pelanggaran kewajiban oleh pengelola sistem (BSI), maka terdapat potensi penegakan hukum baik dalam bentuk sanksi administratif, perdata, maupun pidana. Hal ini juga membuka ruang untuk pendekatan *corporate criminal liability*, di mana korporasi sebagai badan hukum dapat dimintai pertanggungjawaban pidana atas tindak pidana yang terjadi melalui atau dalam lingkup operasionalnya.

Sebagai entitas yang mengelola dan menentukan tujuan pemrosesan data nasabah, Bank BSI berperan sebagai Pengendali Data Pribadi sebagaimana dimaksud dalam Pasal 1 angka 4 UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP). Posisi ini memberikan beban tanggung jawab hukum yang signifikan dalam menjamin pelindungan data nasabah.

Sebagai pengendali data, bank memiliki kewajiban bukan hanya dalam pengumpulan dan penyimpanan data, tetapi juga dalam menjamin akuratnya data, keamanan sistem, dan kesesuaian penggunaan data dengan prinsip-prinsip pelindungan data pribadi. Pasal 20 hingga Pasal 30 UU PDP menetapkan sejumlah kewajiban substantif yang meliputi keabsahan dasar pemrosesan, transparansi, pembatasan tujuan, dan akuntabilitas pengelolaan data.

Lebih lanjut, Pasal 35 UU PDP mengharuskan pengendali data untuk melakukan evaluasi berkala terhadap sistem keamanan, termasuk pengujian atas kerentanan yang berpotensi dimanfaatkan oleh pihak yang tidak bertanggung jawab. Dalam konteks ini, audit sistem dan pengawasan internal merupakan komponen kunci dari manajemen risiko yang wajib dijalankan secara rutin.

Selain itu, Menurut Pasal 39 ayat (1) Undang-Undang Perlindungan Data Pribadi (UU PDP), pengendali data memiliki kewajiban untuk melindungi data dari akses maupun pemrosesan yang tidak sah. Jika kewajiban ini diabaikan, maka dapat menimbulkan akibat hukum yang berat, sebagaimana ditegaskan dalam Pasal 57 dan Pasal 67 yang memuat ketentuan mengenai sanksi administratif maupun pidana atas pelanggaran tersebut.

Kewajiban ini semakin diperkuat dalam Pasal 46 UU PDP, yang menyatakan bahwa pengendali data harus melaporkan insiden kegagalan pelindungan data pribadi kepada subjek data dan otoritas pelindungan data paling lambat 3 x 24 jam setelah insiden diketahui. Dalam kasus kebocoran data yang menimpa Bank BSI, pelaporan yang cepat dan transparan menjadi tolok ukur kepatuhan bank terhadap UU PDP.

Dalam sektor perbankan, pelaksanaan kewajiban ini juga bersinggungan dengan prinsip kehati-hatian (*prudential principle*) dan asas fidusia (*fiduciary duty*), yang menuntut bank untuk menjaga kepercayaan nasabah sebagai bagian dari perlindungan konsumen. Seiring dengan percepatan digitalisasi layanan keuangan, kelalaian dalam perlindungan data pribadi dapat menimbulkan risiko sistemik, merusak reputasi institusi, dan bahkan mengancam stabilitas sektor keuangan.

Sebagai konsekuensi, Bank BSI wajib menyusun kebijakan internal dan prosedur teknis yang mengacu pada standar nasional maupun internasional, serta menunjuk pejabat pelindungan data pribadi, sesuai dengan Pasal 53 dan Pasal 54 UU PDP. Ketidakpatuhan terhadap ketentuan tersebut membuka ruang diterapkannya prinsip strict liability, di mana bank tetap dapat dimintai pertanggungjawaban meskipun tidak ada unsur kesengajaan.

Oleh karena itu, pemahaman yang komprehensif dan pelaksanaan nyata terhadap kewajiban sebagai pengendali data pribadi menjadi aspek krusial dalam membangun ekosistem keuangan digital yang akuntabel dan melindungi hak-hak digital masyarakat.

Penyelesaian permasalahan hukum terkait kebocoran data di Indonesia umumnya dapat ditempuh melalui dua mekanisme, yaitu ranah pidana dan ranah perdata. Akan tetapi, dalam kasus kebocoran data berskala besar seperti yang dialami Bank Syariah Indonesia (BSI), jalur pidana sering dipandang lebih efektif dibandingkan dengan perdata. Efektivitas ini didorong oleh beberapa alasan: hukum pidana memiliki kekuatan pemaksaan yang lebih kuat, proses pembuktiannya lebih menekankan pada kesalahan pelaku, serta keberadaan sanksi pidana yang mampu memberikan efek jera baik kepada individu maupun lembaga.

Efektivitas jalur pidana dalam penyelesaian sengketa kebocoran data sangat bergantung pada keberadaan instrumen hukum yang tegas, dapat diimplementasikan, dan memiliki kekuatan memaksa. UU Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) memberikan kerangka hukum yang kuat untuk menindak pelanggaran, baik yang dilakukan oleh individu maupun oleh korporasi.

Dalam konteks pertanggungjawaban pidana korporasi, Pasal 67 ayat (1) dan (2) UU PDP menyebutkan bahwa:

"(1) Dalam hall Tindak Pidana sebagaimana dimaksud pasal 65 dan pasal 66 dilakukan oleh korporasi, pidana dijatuhkan kepada korporasi, dan/atau orang yang memberi perintah atau orang yang bertindak sebagai pemimpin kegiatan korporasi tersebut"

"(2) Pidana terhadap Korporasi dikenakan berupa pidana denda dan dapat dikenai tindakan tambahanberupa:

a. perampasan keuntungan dan/atau harta kekayaan yang diperoleh dari Tindak Pidana
b. pembekuan seluruh atau sebagian usaha Korporasi
c. pelarangan permanen melakukan perbuatan tertentu
d. menempatkan Korporasi di bawah pengawasan paling lama 3 (tiga) tahun; atau
e. pencabutan seluruh atau sebagian izin usaha."

Ketentuan tersebut menampilkan dengan tegas bahwa badan hukum berupa korporasi bisa dikenakan pertanggungjawaban pidana secara langsung. Tidak hanya sanksi berupa pidana denda, UU PDP juga memberikan ruang untuk tindakan tambahan berupa pembekuan usaha dan pencabutan izin operasional. Hal ini memberikan landasan hukum yang kuat untuk menindak lembaga keuangan seperti bank, apabila terbukti melakukan pelanggaran serius terhadap kewajiban pelindungan data.

Keberhasilan penerapan sanksi pidana terhadap korporasi dalam kasus penyalahgunaan data pribadi sangat ditentukan oleh efektivitas aparat penegak hukum dalam membuktikan unsur kesalahan, kesiapan regulasi prosedural seperti Perma No. 13 Tahun 2016, serta peran aktif lembaga pengawas seperti Badan Pelindungan Data Pribadi (BPDP). Meskipun ketentuan hukum substantif telah diatur dalam UU No. 27 Tahun 2022, tanpa penegakan hukum yang konsisten dan dukungan kelembagaan yang kuat, perlindungan terhadap data pribadi tidak akan mampu menjamin rasa aman dan keadilan bagi Masyarakat (Falevi, 2024).

Dengan demikian, Pasal 67 UU PDP merupakan bentuk konkret dari pengakuan sistem hukum Indonesia terhadap doktrin *corporate criminal liability*, dan memberikan ruang yang luas untuk menindak pelaku kebocoran data, baik perseorangan maupun korporasi.

Kesimpulan

Merujuk pada latar belakang serta hasil analisis yang telah dipaparkan, penelitian ini menyimpulkan bahwa Bank Syariah Indonesia (BSI) dapat dimintai pertanggungjawaban pidana atas terjadinya kebocoran data nasabah. Peristiwa tersebut mencerminkan adanya kelalaian dalam menerapkan standar keamanan sebagaimana yang diamanatkan dalam UU Perlindungan Data Pribadi, UU ITE, serta peraturan OJK. Kebocoran data tersebut mengandung unsur tindak pidana karena secara nyata menimbulkan kerugian pada pemilik data. Dalam perspektif hukum pidana modern, korporasi termasuk lembaga perbankan dapat dijatuhi sanksi pidana apabila lalai menjaga keamanan sistem informasi. Sebagai pihak pengendali data, BSI memiliki kewajiban mencegah terjadinya akses ilegal, dan kegagalan dalam menjalankan kewajiban ini dapat digolongkan sebagai perbuatan pidana. Pasal 67 UU PDP serta Pasal 36 UU ITE menegaskan adanya ancaman pidana bagi penyelenggara sistem elektronik maupun korporasi yang lalai. Kasus ini menegaskan relevansi doktrin *corporate criminal liability*, yaitu pertanggungjawaban bukan hanya dibebankan pada individu, tetapi juga kepada korporasi

untuk menciptakan efek jera, memperbaiki tata kelola keamanan digital, serta melindungi hak-hak nasabah. Penegakan transparansi dan akuntabilitas dalam penanganan perkara menjadi penting agar kepercayaan publik tetap terjaga. Oleh karena itu, BSI patut dipandang sebagai subjek hukum pidana yang bertanggung jawab atas kelalaiannya. Perlindungan hukum pidana terhadap data pribadi merupakan bagian dari hak asasi digital yang harus dijamin keberlangsungannya.

Referensi

Anggraini, N. F., & Wiraguna, S. A. (2025, Mei). *Tanggung jawab hukum platform pinjaman online terhadap penyalahgunaan dan penyebaran data pribadi konsumen secara ilegal*. Riset Sosial Humaniora dan Pendidikan, 3(3), 144–167. https://doi.org/10.62383/risoma.v3i3.767 ResearchGate

Antoine, R. A., Farizqa, N. S., Hasna, A. H., & Pasaribu, M. (2025, Februari). *Penyalahgunaan data pribadi dalam teknologi transaksi digital di industri perbankan digital (Studi kasus PT. Bank Syariah Indonesia)*. Jurnal Multidisiplin Ilmu Akademik (JMIA), 2(1), 316–327. https://doi.org/10.61722/jmia.v2i1.3147

Amoraga, P., & Widiyaati, N. (2002). *Dinamika Koperasi.* Jakarta: Rineka Cipta Bina Adiaksara.

Andjar Pachta W, d. (2005). *Hukum Koperasi Indonesia Pemahaman, Regulasi, Pendirian dan Modal Usaha.* Jakarta: Kencana Jakarta.

Dimyati, & Mudjiono. (2012). *Belajar dan Pembelajaran.* Jakarta: Rineka Cipta.

Dinas Perindustrian Koperasi UKM Kulon Progo. (2024). *Sejarah dan Latar Belakang Koperasi*. Retrieved November 10, 2024, from Koperasi Kulon Progo: https://koperasi.kulonprogokab.go.id

Erlin Kurniati, d. (2024, November). Peran Pemerintah dalam Pembangunan Ekonomi Daerah. *JIIC : Jurnal Intelek Insan Cendekia, I*(9), 60-65.

Firdaus, M., & Santoso, A. E. (2002). *Perkoperasian, Sejarah, Teori dan Praktek.* Jakarta: Ghalia Indonesia.

Firmanda, M. E. M., Efendi, T. K., Alfarisy, F. R., Javantara, A. C., & Indrarini, R. (2024, November). *Analisis kebijakan perlindungan nasabah pada bank digital syariah di Indonesia*. Socius: Jurnal Penelitian Ilmu-Ilmu Sosial, 2(4), 1–7. https://doi.org/10.5281/zenodo.13998659

Hadhikusuma, S. R. (2000). *Hukum Koperasi Indonesia.* Jakarta: Rajawali Press.

Herawati, Y. (2014). Konsep Keadilan Sosial dalam Bingkai Sila Kelima Pancasila. *UPN Veteran Yogyakarta*, 20.

Hidayat, R., & Abdillah. (2019). *Ilmu Pendidikan Komsep, Teori, dan Aplikasinya.* Medan: LPPI.

Manurung. (2000). Perkoperasian Di Indonesia : Masalah, Peluang dan Tantangannya di Masa Depan. *Economics E-Journal*.

Marzuki, P. M. (2016). *Penelitian Hukum.* Jakarta: Kencana Prenada Media Group.

Muchsin. (2003). *Perlindungan dan Kepastian Hukum Bagi Investor di Indonesia.* Surakarta: Magister Ilmu Hukum Program Pascasarjana Universitas Sebelas Maret.

Muhammad Taufiq, A. (n.d.). *Pengantar Ekonomi Koperasi.* Purbalingga: Eurekamediaaksara.

Rineska, O. L., & Wulandari, B. T. (2020). Perlindungan Hukum Terhadap Penerima Pinjaman Terkait Penetapan Tingkat SUku Bunga Yang Tinggi Oleh Perusahaan Peer To Peer Lending yang Terdaftar Pada Otoritas Jasa Keuangan. *Selisik*.

Salim, H. (2008). *Pengantar Hukum Perdata Tertulis (BW)* (Vol. Cetakan 5). Jakarta: Sinar Grafika.

Saputra, A., & Ardiansyah, M. R. (2021, Juni). Strategi Pengembangan Koperasi Serba Usaha (KSU) di Kota Medan. *Jurnal Administrasi Publik dan Kebijakan (JAPK), 1*(1), 3.

Setiono. (2004). *Rule Of Law (Supremasi Hukum).* Surakarta: Magister Ilmu Hukum Program Pascasarjana Universitas Sebelas Maret.

Sitio, A., & Tamba, H. (2001). *Koperasi Teori dan Praktek.* Jakarta: Erlangga.

Solihin, S. A. (2023). Peran Koperasi Bagi Anggota Dan Harapan Anggota Terhadap Koperasi. *Jurnal Ilmiah Ekonomi dan Keuangan Syariah, 4*(2), 118.

Sulistiyani, & Teguh, A. (2004). *Kemitraan dan Model-Model Pemberdayaan.* Yogyakarta: Gaya Media.

Syarif, T. (2002). *Koperasi Menuju Otonomi Yang Berdaya Saing.* Jakarta: Kementerian Koperasi Republik Indonesia.

Tutik, T. T. (2008). *Hukum Perdata Dalam Sistem Hukum Nasional.* Jakarta: Perada Media Group