BAB I
PENDAHULUAN

1.1 Latar Belakang

Dalam era digitalisasi telah membawa transformasi besar dalam sektor perbankan. Transformasi digital di sektor perbankan telah berkembang pesat dalam dua dekade terakhir industri perbankan. Bank sebagai lembaga keuangan memiliki tanggung jawab besar dalam menjaga kerahasiaan dan keamanan data nasabah agar tidak disalahgunakan oleh pihak yang tidak bertanggung jawab.

Perbankan digital, dengan segala keunggulannya, telah menjadi tulang punggung transaksi ekonomi modern. Di Indonesia, transformasi digital di sektor perbankan terus menunjukkan tren peningkatan yang signifikan. Data Bank Indonesia menunjukkan bahwa nilai transaksi digital banking pada April 2024 mencapai Rp5.335,33 triliun, tumbuh 17,19% secara tahunan atau *year on year* (yoy),[1] mengindikasikan semakin tingginya ketergantungan masyarakat pada layanan perbankan daring.

Salah satu kasus yang menarik perhatian publik adalah kebocoran data nasabah yang dialami oleh Bank Syariah Indonesia (BSI), yang menimbulkan pertanyaan mengenai sejauh mana tanggung jawab bank dalam melindungi informasi pribadi para nasabahnya.

[1] Martha Herlinawati Simanjuntak. (2024, Februari 21). *BI: Nilai transaksi perbankan digital capai Rp5.335,33 triliun*. ANTARA News.

Bank Syariah Indonesia (BSI), sebagai salah satu bank syariah terbesar di Indonesia, mengalami gangguan sistem yang berujung pada dugaan kebocoran data nasabah pada Mei 2023. Kelompok peretas *LockBit* 3.0 mengklaim telah mencuri sekitar 1,5 *terabyte* data yang mencakup informasi pribadi nasabah, dokumen transaksi, hingga kredensial pegawai bank.[2]

Kejadian ini menimbulkan dampak serius, baik dari sisi operasional bank maupun kepercayaan publik terhadap keamanan sistem perbankan syariah di Indonesia. Dalam konteks hukum di Indonesia, perlindungan data pribadi dan pertanggungjawaban atas kebocoran data telah diatur melalui beberapa regulasi, termasuk Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang telah diperbarui melalui UU No. 19 Tahun 2016, dan Undang-Undang No. 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP).

UU PDP, khususnya Pasal 57 dan Pasal 67 sampai Pasal 70, mengatur sanksi administratif dan pidana atas pelanggaran perlindungan data pribadi.[3] Namun demikian, dalam praktiknya masih banyak kekosongan norma dan ketidakjelasan mekanisme pertanggungjawaban, khususnya terhadap entitas seperti perbankan digital yang memiliki risiko tinggi atas pelanggaran data tersebut.

Pasal 26 ayat (1) UU ITE memberikan hak kepada setiap orang atas perlindungan data pribadi dalam sistem elektronik, yakni “Kecuali ditentukan lain

[2] CNN Indonesia. (2023, Mei 13). *LockBit 3.0 diduga curi data dan password 15 juta nasabah BSI.*

[3] Lihat pasal 57 dan pasal 67-70 Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

oleh Peraturan Perundang- undangan, penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan Orang yang bersangkutan."[4] Ketentuan ini diperkuat dengan Pasal 14 dan 29 ayat 1 UU PDP Pengendali Data Pribadi wajib memastikan akurasi, kelengkapan, dan konsistensi Data Pribadi sesuai dengan ketentuan peraturan perundang-undangan.[5]

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.

Selain itu, Peraturan Otoritas Jasa Keuangan (POJK) No. 38/POJK.03/2016 tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi

[4] Lihat pasal 26 ayat (1) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

[5] Lihat pasal 29 ayat 1 Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

oleh Bank Umum secara umum mengatur kewajiban bank dalam menerapkan sistem keamanan yang memadai untuk melindungi data nasabah. Secara spesifik, Pasal 16 menyebutkan bahwa.

Bank wajib memastikan pengamanan informasi dilaksanakan secara efektif dengan memperhatikan paling sedikit:

a. pengamanan informasi yang ditujukan agar informasi yang dikelola terjaga kerahasiaan (confidentiality), integritas (integrity), dan ketersediaan (availability) secara efektif dan efisien dengan memperhatikan kepatuhan terhadap ketentuan;

b. pengamanan informasi yang dilakukan terhadap aspek teknologi, sumber daya manusia, dan proses dalam penggunaan Teknologi Informasi;

c. pengamanan informasi yang diterapkan berdasarkan hasil penilaian terhadap risiko (risk assessment) pada informasi yang dimiliki Bank;

d. dan ketersediaan manajemen penanganan insiden dalam pengamanan informasi. [6]

Lebih lanjut, Pasal 19 mengatur mengenai pengembangan dan pengadaan Teknologi Informasi, di mana bank wajib melakukan langkah pengendalian untuk menghasilkan sistem dan data yang terjaga kerahasiaan dan integritas, yang

[6] Otoritas Jasa Keuangan. (2016). *Peraturan Otoritas Jasa Keuangan Nomor 38/POJK.03/2016 Tahun 2016 tentang Penerapan Manajemen Risiko Dalam Penggunaan Teknologi Informasi oleh Bank Umum*. Pasal 16

tentunya mencakup data nasabah. Selain itu, Pasal 22 mewajibkan bank untuk melakukan penilaian sendiri atas tingkat maturitas keamanan siber.

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.

Beberapa penelitian terdahulu telah menyoroti isu kebocoran data dan perlindungan hukum dalam sektor perbankan. Studi yang dilakukan oleh Muhammad Esza Maulana Firmanda, Taufik Kukuh Efendi, Fathor Rozy Alfarisy, Alfado Chievo Javantara, dan Rachma Indrarini (2024) membahas bagaimana kebijakan perlindungan nasabah diimplementasikan dalam bank digital syariah di Indonesia, terutama dari sudut pandang peraturan OJK, prinsip-prinsip

perlindungan konsumen syariah, serta efektivitas pengawasan internal bank dalam era digital, tetapi belum secara spesifik menyoroti tanggung jawab bank dalam kebocoran data. [7]

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.[8]

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.

Oleh karena itu, penelitian ini akan memberikan kontribusi akademik dengan mengkaji secara sistematis aspek hukum yang mengatur tanggung jawab bank dalam kasus kebocoran data nasabah. Penelitian ini menggunakan metode yuridis normatif**,** yaitu pendekatan yang berfokus pada analisis peraturan perundang-undangan yang berlaku.

[7] Firmanda, M. E. M., Efendi, T. K., Alfarisy, F. R., Javantara, A. C., & Indrarini, R. (2024). Analisis Kebijakan Perlindungan Nasabah pada Bank Digital Syariah di Indonesia. *Socius: Jurnal Penelitian Ilmu-ilmu Sosial*, *2*(4).

[8] Ramadhani, W. K. S., & Wiraguna, S. A. (2025). Implementasi pelindungan data pribadi dalam sistem informasi pada perusahaan jasa keuangan. *Perspektif Administrasi Publik dan hukum*, *2*(2), 158-175.

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[9].

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[10]. 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[11]. 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

[9] Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Lembaran Negara Republik Indonesia Tahun 2022 Nomor 200, Pasal 1 angka 4.

[10] Perbanas. 2025. *Bagaimana Regulasi OJK Mendukung Keamanan dan Pelindungan Data Nasabah*.

[11] Runtuwene, R. R. R. (2017). Pertanggungjawaban pidana korporasi sebagai suatu perkembangan tindak pidana. *Lex et Societatis*, *5*(2).

mekanisme pemulihan yang jelas ketika menjadi korban kebocoran data[12]. 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. Oleh karena itu, penelitian ini menjadi penting untuk 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 pendekatan *statute approach*, penelitian ini tidak hanya menganalisis aspek normatif, tetapi juga melihat sejauh mana regulasi yang ada mampu diterapkan secara konkret dalam kasus kebocoran data yang terjadi, khususnya pada institusi keuangan seperti Bank Syariah Indonesia. Selain ditinjau dari aspek hukum perdata dan administrasi, kasus kebocoran data nasabah bank seperti yang terjadi pada Bank Syariah Indonesia (BSI) juga relevan untuk dianalisis dari sudut pandang 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) sebagai subjek hukum pidana.

[12] CNN Indonesia, "BSI Kena Ransomware Lockbit, 15 Juta Data Nasabah Bocor?", 15 Mei 2023,

Dalam hukum pidana modern, termasuk di Indonesia, telah berkembang doktrin pertanggungjawaban pidana korporasi yang memungkinkan badan hukum, seperti bank, untuk dimintai pertanggungjawaban pidana apabila terbukti melakukan atau turut serta dalam suatu tindak pidana. Hal ini tercermin dalam Pasal 46 ayat (1) dan (2) UU Nomor 1 Tahun 2023 yang menyatakan bahwa korporasi dapat dijatuhi pidana apabila tindak pidana dilakukan untuk dan atas nama korporasi, serta tindak pidana tersebut berada dalam lingkup usahanya.[13]

Lebih lanjut, Pasal 67 UU Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) secara tegas menyatakan bahwa jika tindak pidana pelanggaran data dilakukan oleh korporasi, maka pidana dapat dijatuhkan terhadap korporasi dan/atau pengurusnya, termasuk pidana denda dan tindakan administratif lain seperti pembekuan usaha atau pencabutan izin.[14]

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 secara langsung maupun tidak langsung, sebagaimana diatur 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

[13] Undang-Undang Republik Indonesia Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana, Lembaran Negara Republik Indonesia Tahun 2023 Nomor 1, Pasal 46.

[14] Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Lembaran Negara Republik Indonesia Tahun 2022 Nomor 213, Pasal 67.

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.

1.2 Rumusan Masalah

Dari latar belakang di atas dirumuskan masalah sebagai berikut :

1. Apakah Bank BSI telah memenuhi standar keamanan siber yang ditetapkan oleh OJK dan peraturan terkait dalam melindungi data nasabah?

1.3 Tujuan Penelitian

1. Untuk mengetahui dan menganalisis apakah Bank Syariah Indonesia (BSI) telah memenuhi standar keamanan siber sebagaimana yang ditetapkan oleh Otoritas Jasa Keuangan (OJK) dan peraturan perundang-undangan terkait dalam upaya melindungi data nasabah

1.4 Manfaat penelitian

Penelitian ini diharapkan dapat memberikan manfaat baik dari segi teoritis maupun praktis.

1.4.1 Manfaat Teoritis

1. Pengembangan Ilmu Hukum

Menambah wawasan akademis dalam bidang hukum perbankan dan perlindungan data pribadi, terutama terkait dengan kebocoran data di sektor perbankan syariah.

2. Kontribusi terhadap Kajian Hukum Perlindungan Data

   Memberikan kajian akademis mengenai implementasi Undang-Undang Perlindungan Data Pribadi (UU PDP) dan regulasi perbankan terkait keamanan informasi.

3. Analisis terhadap Tanggung Jawab Hukum Perbankan

   Menganalisis tanggung jawab hukum bank dalam konteks kebocoran data dan menjelaskan sejauh mana bank dapat dimintai pertanggungjawaban secara perdata, pidana, dan administratif.

1.4.2 Manfaat Praktis

1. Bagi Perbankan Syariah (Bank BSI dan Lembaga Keuangan Lainnya)

   Memberikan rekomendasi terkait peningkatan sistem keamanan data dan kepatuhan terhadap regulasi perlindungan data pribadi.

2. Bagi Nasabah yang Terdampak

   Memberikan pemahaman mengenai hak-hak hukum nasabah serta langkah-langkah yang dapat ditempuh dalam mencari perlindungan hukum jika data pribadinya mengalami kebocoran.

3. Bagi Regulator (OJK, Bank Indonesia, dan Pemerintah)

   Menjadi referensi dalam penguatan kebijakan dan regulasi terkait perlindungan data di sektor perbankan guna mencegah insiden serupa di masa depan.

4. Bagi Masyarakat Umum

Meningkatkan kesadaran tentang pentingnya perlindungan data pribadi serta memberikan wawasan mengenai risiko kebocoran data dalam dunia digital.

1.5 Metode Penelitian

1.5.1 Metode Pendekata Penelitian

Dalam penelitian ini, penulis menggunakan 3 (tiga) pendekatan penelitian, yakni :

1.5.1.1 Pendekatan Peraturan Perundang-Undangan (Statute Approach) adalah suatu pendekatan penelitian yang dilakukan dengan menelaah secara mendalam peraturan perundang-undangan yang berkaitan dengan permasalahan hukum yang sedang diteliti. Dalam konteks penelitian ini, pendekatan tersebut digunakan untuk mengkaji ketentuan yang terdapat dalam Undang-Undang Informasi dan Transaksi Elektronik, Undang-Undang Perlindungan Data Pribadi, dan Peraturan Otoritas Jasa Keuangan Nomor 38/POJK.03/2016 tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum.

Melalui pendekatan ini, penelitian berupaya menemukan dasar normatif mengenai kewajiban pengendali data pribadi dan kewajiban bank dalam menjaga keamanan, kerahasiaan, dan keakuratan data pribadi nasabah. Selain itu, pendekatan perundang-undangan juga memungkinkan untuk melihat sejauh mana harmonisasi antar-regulasi

tersebut mampu memberikan perlindungan hukum yang komprehensif terhadap data pribadi masyarakat.

1.5.1.2 Pendekatan Konseptual, (Conceptual Approach) adalah suatu pendekatan penelitian yang beranjak pada pandangan-pandangan dan doktrin-doktrin di dalam Ilmu Hukum. Sehingga penulis akan menggunakan teori-teori hukum, doktrin para ahli, dan prinsip-prinsip umum perlindungan data pribadi sebagai landasan dalam menganalisis permasalahan yang diteliti.

Dengan menggunakan pendekatan ini, penulis dapat menafsirkan norma-norma hukum tidak hanya berdasarkan teks peraturan perundang-undangan, tetapi juga dari kerangka pemikiran konseptual yang lebih luas. Misalnya, penerapan prinsip confidentiality, integrity, dan availability (CIA) dalam keamanan informasi yang banyak diadopsi dalam praktik internasional, serta doktrin mengenai kewajiban pengendali data dalam menjaga keakuratan, kerahasiaan, dan keamanan data pribadi. Dengan demikian, pendekatan konseptual ini memberikan dasar teoritis yang memperkaya analisis normatif dan membantu memberikan argumentasi hukum yang lebih mendalam.

1.5.2 Jenis dan Sifat Penelitian

Jenis penelitian yang digunakan dalam skripsi ini adalah penelitian hukum normatif**.** Penelitian hukum normatif merupakan jenis penelitian yang menitikberatkan pada studi terhadap norma-norma hukum positif, baik yang tertulis dalam peraturan perundang-undangan maupun dalam doktrin hukum.

Tujuan dari penelitian ini adalah untuk menemukan kaidah-kaidah hukum, asas-asas hukum, dan konsep-konsep yang relevan guna menjawab permasalahan hukum yang telah dirumuskan dalam rumusan masalah.

Menurut Peter Mahmud Marzuki, penelitian hukum normatif dilakukan untuk mengkaji hukum sebagai norma yang tertuang dalam sistem peraturan perundang-undangan, bukan hukum sebagai realitas sosial yang hidup dalam masyarakat[15]. Oleh karena itu, data utama dalam penelitian ini bersumber dari bahan hukum primer seperti undang-undang, serta bahan hukum sekunder dan tersier yang mendukung interpretasi norma hukum.

Adapun sifat dari penelitian ini adalah deskriptif-analitis. Penelitian deskriptif bertujuan untuk memberikan gambaran secara sistematis, faktual, dan akurat mengenai fakta-fakta hukum dan karakteristik dari fenomena hukum tertentu.[16] Sementara itu, pendekatan analitis digunakan untuk menginterpretasikan ketentuan hukum yang ada dalam kaitannya dengan praktik serta penerapannya dalam konteks kebocoran data pribadi oleh lembaga keuangan.

Penelitian ini secara khusus bertujuan untuk menggambarkan dan menganalisis norma-norma hukum yang berkaitan dengan pertanggungjawaban pidana dalam kasus kebocoran data pribadi nasabah yang terjadi pada Bank Syariah Indonesia (BSI). Dengan demikian, jenis dan sifat penelitian ini

[15] Peter Mahmud Marzuki, *Penelitian Hukum*, Jakarta: Kencana Prenada Media Group, 2017, hlm. 35.

[16] Beni Ahmad Saebani, *Metode Penelitian Hukum*, (Bandung: Pustaka Setia, 2021), hlm. 61.

mendukung upaya untuk membangun argumentasi hukum secara komprehensif dan sistematis dalam menjawab persoalan hukum yang diangkat.

1.5.3 Bahan Hukum

Penelitian ini menggunakan tiga jenis bahan hukum yang relevan dalam studi yuridis normatif, yaitu bahan hukum primer, sekunder, dan tersier.

1. Bahan Hukum Primer

Bahan hukum primer merupakan sumber hukum utama yang menjadi landasan analisis dalam penelitian ini. Bahan ini terdiri atas:

- Kitab Undang-Undang Hukum Pidana (KUHP);
- Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP);
- Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dan perubahannya melalui Undang-Undang Nomor 19 Tahun 2016;
- Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan;
- Peraturan Otoritas Jasa Keuangan (POJK) Nomor 38/POJK.03/2016;

Bahan hukum ini digunakan untuk mengkaji tanggung jawab pidana yang dapat dikenakan kepada institusi perbankan dalam kasus kebocoran data pribadi.

2. Bahan Hukum Sekunder

Bahan hukum sekunder meliputi literatur hukum seperti buku ajar, jurnal hukum, hasil penelitian hukum terdahulu, dan pendapat para ahli hukum yang membahas konsep-konsep seperti *corporate criminal liability, strict liability*, dan perlindungan data pribadi.

Literatur tersebut digunakan untuk mendukung interpretasi terhadap ketentuan normatif dalam bahan hukum primer, sekaligus sebagai dasar pengembangan argumentasi dalam penelitian ini.

3. Bahan Hukum Tersier

Bahan hukum tersier mencakup sumber-sumber penunjang seperti kamus hukum, ensiklopedia hukum, glosarium istilah, serta panduan metodologi penelitian hukum. Bahan ini berguna untuk memperjelas definisi dan konsep yang digunakan dalam penelitian.

1.5.4 Teknik Analisa Bahan Hukum

Teknik analisis yang digunakan dalam penelitian ini adalah teknik analisis kualitatif, yaitu menganalisis bahan hukum dengan mengutamakan logika dan penalaran hukum secara sistematis. Analisis ini dilakukan terhadap bahan hukum primer seperti undang-undang, peraturan pelaksana, dan putusan pengadilan, serta bahan hukum sekunder berupa doktrin hukum dari literatur akademik, jurnal ilmiah, dan pandangan para ahli.

Melalui teknik ini, penulis berupaya untuk menginterpretasikan norma-norma hukum yang relevan dengan isu tanggung jawab pidana atas kebocoran data

pribadi oleh lembaga perbankan. Setiap ketentuan hukum yang dikaji akan ditelaah dari segi struktur normatif dan aplikasinya dalam konteks konkret, seperti kasus kebocoran data pada Bank Syariah Indonesia (BSI).

Penekanan diberikan pada bagaimana peraturan perundang-undangan dan doktrin hukum membentuk dasar pertanggungjawaban pidana korporasi dalam kejahatan siber, khususnya pelanggaran terhadap perlindungan data pribadi. Teknik ini juga memungkinkan penulis untuk mengidentifikasi kesenjangan normatif (legal gap) maupun tumpang tindih pengaturan yang dapat memengaruhi efektivitas penegakan hukum di Indonesia.