Arus Jurnal Sosial dan Humaniora (AJSH)
Website: http://jurnal.ardenjaya.com/index.php/ajsh
Email: jurnal.ajsh@ardenjaya.com

Tanggung Jawab Hukum Pidana Penyelenggara Elektronik Perbankan terhadap Perlindungan Data Pribadi Nasabah

INFO PENULIS

Ruly Wahyu
Universitas Esa Unggul Jakarta
rulywhyu1911@gmail.com

Men Wih Widiatno
Universitas Esa Unggul Jakarta
dosen.menwih@gmail.com

INFO ARTIKEL

ISSN: 2808-1307
Vol. 5, No. 2, Agustus 2025
https://jurnal.ardenjaya.com/index.php/ajsh

Saran Penulisan Referensi:

Wahyu, R ., & Widiatno, M. W. (2025). Tanggung Jawab Hukum Pidana Penyelenggara Elektronik Perbankan terhadap Perlindungan Data Pribadi Nasabah. *Arus Jurnal Sosial dan Humaniora, 5* (2), 3190-3199.

Abstrak

Perkembangan teknologi informasi mendorong transformasi layanan perbankan menuju sistem elektronik yang memungkinkan transaksi lebih mudah dan efisien. Namun, hal ini memunculkan persoalan serius menyangkut upaya menjaga kerahasian infirmasi pribadi nasabah yang rentan terhadap penyalahgunaan dan kebocoran. Rumusan masalah dalam penelitian ini adalah mengenai bentuk pelanggran yang dilakukan oleh perbankan yang dapat dikategorikan sebagai pencurian data pribadi nasabah dan mengenai tanggung jawab hukum perbankan dalam melindungi data pribadi nasabah. Penelitian menggunakan metode yuridis normatif dengan pendekatan perundang-undangan, konseptual, dan studi kasus. Data diperoleh melalui studi kepustakaan dan dianalisis secara kualitatif. Hasil penelitian menunjukkan bahwa bentuk pelanggaran berupa pengungkapan data pribadi tanpa persetujuan merupakan pelanggaran serius, Kebocoran data elektronik akibat kelalaian penyelenggara sistem, khususnya perbankan, merupakan bentuk pelanggaran yang tidak dapat diabaikan, Penyalahgunaan data pribadi, seperti penggunaan informasi nasabah untuk promosi tanpa izin, sering terjadi dalam praktik perbankan dan bank memiliki tanggung jawab hukum berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, serta regulasi sektor keuangan dari Otoritas jasa keuangan serta Bank Indonesia. Meski demikian, perlindungan data di sektor perbankan masih menghadapi kendala, seperti lemahnya sistem keamanan, belum efektifnya otoritas pengawas data, dan rendahnya literasi hukum nasabah. Kondisi ini menimbulkan risiko kerugian hukum dan sosial, serta menurunkan tingkat kepercayaan publik terhadap perbankan digital. Penelitian ini merekomendasikan penguatan tata kelola keamanan data, pembentukan lembaga pengawas independen, dan edukasi hukum kepada masyarakat.

Kata Kunci: Tanggung Jawab Hukum, Perbankan, Perlindungan Data Pribadi, Sistem Elektronik Kebocoran Data

Abstract

The development of information technology has driven the transformation of banking services towards electronic systems that enable easier and more efficient transactions. However, this has raised serious issues regarding efforts to maintain the confidentiality of customers' personal information, which is vulnerable to misuse and leakage. The research problem formulation in this study concerns the forms of violations committed by banks that can be categorized as theft of customers' personal data and the legal responsibility of banks in protecting customers' personal data. The research uses a normative juridical method with a statutory, conceptual, and case study approach. Data were obtained through literature review and analyzed qualitatively. The research results show that the form of violation in the form of disclosure of personal data without consent is a serious violation. Electronic data leaks due to negligence of system administrators, especially banks, are a form of violation that cannot be ignored. Misuse of personal data, such as the use of customer information for promotions without permission, often occurs in banking practices and banks have legal responsibilities based on Law Number 27 of 2022 concerning Personal Data Protection, Law Number 11 of 2008 concerning Information and Electronic Transactions, and financial sector regulations from the Financial Services Authority and Bank Indonesia. However, data protection in the banking sector still faces obstacles, such as weak security systems, ineffective data supervisory authorities, and low customer legal literacy. These conditions pose a risk of legal and social losses, and reduce the level of public trust in digital banking. This study recommends strengthening data security governance, establishing an independent supervisory body, and legal education for the public.

Keywords: Legal Responsibility, Banking, Personal Data Protection, Electronic Systems, Data Leaks

A. Pendahuluan

Indonesia dikenal sebagai negara yang menjunjung tinggi aturan dan norma hukum dalam setiap aspek kehidupan, sudah sepatutnya setiap hubungan dalam kehidupan bermasyarakat diatur melalui ketentuan hukum yang berlaku. Permasalahan hukum akan selalu melekat pada aktifitas keseharian manusia, baik sebagai individu maupun dalam kapasitasnya sebagai warga negara. Setiap orang menginginkan kehidupan yang tenang, aman, dan Sejahtera. Namun, seiring dengan kemajuan hukum dan modernisasi diberbagai bidang kehidupan, tingkat keriminalitas ditengah Masyarakat juga menunjukkan peningkatan, termasuk di Indonesia.

Indonesia merupakan sebuah negara yang menerapkan Pokok-pokok ajaran yang menjadi landasan dalam Pancasila dan Undang-Undang 1945. Dalam sudut pandang sistem perekonomian, sektor perbankan berkontribusi signifikan terhadap proses pembangunan dan peningkatan ekonomi nasional. Perbankan menjadi pokok utama dalam menggerakkan roda perekonomian Indonesia, yang terus berkembang seiring dengan perkembangan global dan kemajuan teknologi.

Perkembangan didalam teknologi informasi dan komunikasi, khususnya sistem elektronik, telah menciptakan gaya hidup dan pola komunikasi baru diantara masyarakat. Perubahan digital ini tidak hanya mempengaruhi aspek sosial, tetapi juga menjadi pemicu utama dalam pergeseran sistem ekonomi dari model tradisional berbasis industri manufaktur menuju aktivitas ekonomi melalui platform digital yang mengandalkan data atau keterangan, kreativitas daya pikir , dan wawasan keilmuan. Fenomena ini disebut sebagai ekonomi kreatif.

Namun, kemajuan teknologi juga membawa tantangan tersendiri, khususnya berrhubungan melalui perlindungan mengenai data pribadi. Di zaman digital saat ini, informasi pribadi memiliki nilai penting namun rawan terhadap ancaman, terutama dalam transaksi keuangan secara online. Pengamanan Data individu merupakan elemen hak asasi manusia yang harus dihormati, dijaga, dan tidak disalahgunakan.Beberapa negara juga telah memberikan pengakuan konstitusional terhadap hak atas perlindungan data melalui penerapan konsep habeas data, yaitu hak individu untuk mengakses, memperbaiki, dan melindungi informasi pribadinya.

Di Indonesia, pelindungan data pribadi telah menjadi perhatian, khususnya dalam sektor perbankan sebagai pengelola layanan yang bertanggung jawab atas data nasabah dalam jumlah yang melimpah. Dalam konteks ini, penyelenggara sistem elektronik perbankan diberi amanah upaya menjaga informasi pribadi tetap aman dan bersifat privat terhadapat data nasabah (Sumber Artikel Online).

Peraturan perbankan di Indonesia mencakup beberapa aspek penting, antara lain :

1. Ketentuan mengenai Bank Umum telah diterapkan melalui ketentuan sesuai dengan Peraturan Bank Indonesia Nomor 11/1/PBI/2009 yang berlaku, mengenai hal

menguraikan regulasi terkait operasional dan ketentuan hukum perbankan umum di Indonesia yang mengatur mengenai penguasaan saham, pengurusan lembaga, pendirian unit layanan, dan pengembangan cakupan layanan. Peraturan ini bertujuan untuuk meningkatkan dan memperkokoh ketahanan perbankan nasional.

2. Penerbitan Instrumen Pasar Uang: Regulasi yang diterapkan oleh Bank Indonesia Nomor 12 Tahun 2023 tentang Penertiban sarana transaksi keuangan yang berfokus pada pinjaman berjangka pendek dan pertukaran instrumen keuangan likuid dalam pasar uang, harga acuan, pelaku pasar, dan infrastruktur pasar keuangan.
3. Pengawasan: Bank Indonesia memiliki kewenangan untuk melakukan pengawasan terhadap bank-bank umum serta institusi keuangan lainnya untuk memastikan keseimbangan sistem keuangan dan melindungi konsumen.
4. Perlindungan Konsumen: Peraturan perbankan juga mengatur mengenai perlindungan konsumen, termasuk prinsip-prinsip perlindungan konsumen dan penerapatan prinsip kehati-hatian dalam kegiatan perbankan.
5. Kewajiban Bank: Bank-bank umur diwajibkan untuk memiliki SOP dalam bahasa indonesia, menyampaikan laporan kepada Bank Indonesia dalam bahasa Indoensia, dan memiliki struktur organisasi yang jelas.

Salah satu kasus yang mencuat merupakan insiden terbukanya data nasabah bank syariah indonesia (BSI) yang terjadinya pada tahun 2023. Peristiwa ini menimbulkan kekhawatiran besar di tengah masyarakat karena data pribadi nasabah yang sepatutnya memiliki sifat rahasia justru tersebar secara merata di internet. Kebocoran Ini termasuk informasi sensitif seperti nama lengkap, nomor rekening, nomor identitas, hingga riwayat transaksi nasabah.

Kebocoran informasi pribadi nasabah bank menjadi persoalan serius dalam industri perbankan, Pesatnya perkembangan teknologi digital telah memperbesar potensi terjadinya tindak kejahatan di sektor ini. Beberapa jenis informasi yang berkaitan dengan nasabah berupa data akun perbankan, detail fasilitas pembayaran berbasis kredit, informasi pribadi, hingga rincian finansial, apabila bocor, bisa menyebabkan kerugian yang sangat besar. Tindakan semacam ini memberikan dampak yang signifikan terhadapat sektor perbankan, mencakup tidak hanya insiden perlindungan data, tindakan penggelapan, dan pemanfaatan keuangan secara ilegal namun bisa memicu hilangnya kepercayaan konsumen jasa keuangan dengan sektor perbankan beserta menimbulkan penurunan kredibilitas secara substansial.

Berdasarkan pandangan Teguh Aprianto, seorang ahli keamanan diruang digital, melalui pernyataannya di media sosial Twitternya mengungkapkan bahwasanya informasi yang dimiliki oleh BSI dilaporkan telah disebarluaskan tanpa izin secara bertahap dilakukan oleh kelompok hacker dengan jumlah keseluruhan data yang diperkirakan mencapai 8133 data yang akan dibocorkan, ia melanjutkan keterangannya dengan menyatakan bahwa secara keseluruhan data prbadi yang dimaksud berjumlah 24,473 data milik karyawan BSI dan dokumen internalnya diketahui telah masuk dalam daftar data yang telah bocor sejak tahap awal serangan.

Ransomware LockBit 3.0, melalui keterangannya, mengungkapkan bahwa serangan tersebut telah berlangsung selama dua bulan. Bahwasanya mereka menyatakan diri sebagai aktor, peristiwa gangguan layanan BSI yang terjadi pada 8, Mei 2023 ternyata menyimpan fakta penting dibaliknya. Berdasarkan pernyataan dari kelompok peretas, mereka mengklaim telah mencuri sebanyak 15 juta catatan pelanggaran, termasuk data terkait pegawai serta sekitar 1,5 terabyte informasi internal perusahaan. Ransomware LockBit 3.0 juga memungkinkan terjadinya menyebarkan seluruh informasi tersebut pada situs ilegal apabila proses perundingan tidak mencapai kesepakatan.

Isu - isu yang terjadi dalam masyarakat dalam kasus kebocoran data nasabah di Bank Syariah Indonesia pada tahun 2023 yaitu :

1. Skala Kebocoran & Tuntutan Ransom.
   Entitas peretas LockBit 3.0 diduga telah melakukan pencurian data elektronik sejumlah 1,5 terabyte, termasuk data pribadi milik 15 juta nasabah, dengan permintaan tebusan senilai 20 juta dolar AS sebagai bagian dari ancaman siber.(Kompas.com).
2. Gangguan Layanan BSI.
   Selama empat hari, tepatnya dari tanggal 8 hingga 11 Mei 2023, layanan perbankan seperti mobile banking, mesin ATM, dan layanan teller mengalami gangguan. Pada awalnya, gangguan ini diklaim sebagai bagian dari pemeliharaan sistem, namun kemudian diketahui bahwa penyebab utamanya adalah serangan ransomware (Kompas.com).
3. Keamanan Data & Kepercayaan Publik.

Kekhawatiran masyarakat meningkat akibat potensi terjadinya penipuan digital seperti phishing, tindak kecurangan, dan dugaan pengurangan saldo secara tidak sah. Kondisi ini memicu keraguan publik terhadap sistem keamanan perbankan digital. (Detik.com).

4. Respon Regulator & Pemerintah.
   Kominfo dan OJK tengah menyelidiki insiden ini dengan menekankan kepatuhan terhadap regulasi PSE dan UU Perlindungan Data Pribadi. BSSN turut melakukan audit sistem, sementara Wamen BUMN mengakui bahwa masih ada sistem lama yang belum diperbarui. (Detik.com).
5. Perlindungan Nasabah & Imbauan Mitigasi.
   Para ahli menyarankan agar nasabah segera mengganti PIN dan kata sandi, serta meningkatkan kewaspadaan terhadap tautan mencurigakan. Sementara itu, komunitas keamanan siber mendorong nasabah untuk lebih aktif dalam menjaga keamanan data pribadi mereka. (Detik.com)

Otoritas Jasa Keuangan (OJK) berperan menjadi institusi yang berwenang dalam mengawasi jasa disektor keuangan mempunyai peran sentral dalam menanggapi kasus ini. OJK menjalankan fungsi pengawasan, penyelidikan, serta dapat mengenakan sanksi administratif kepada pelaku jasa keuangan yang melanggar prinsip kerahasiaan data nasabah. Selain itu, Bank Syariah Indonesia sebagai pihak penyelenggara sistem elektronik bertanggung jawab secara hukum baik berdasarkan hubungan kontraktual dengan nasabah maupun berdasarkan prinsip tanggung jawab hukum umum non-kontraktual untuk memberikan perlindungan dan pemulihan atas dampak kebocoran data tersebut.

Berdasarkan uraikan yang terdapat dibagian pendahuluan, peneliti bermaksud menetapkan poin-poin permasalahan yang akan menjadi bahan analisis dalam penelitian ini, dengan mengkaji lebih mendalam mengenai tanggung jawab hukum penyelenggara elektronik perbankan terhadap perlindungan data pribadi nasabah yaitu sebagai berikut :

1. Apa bentu pelanggaran yang dilakukan oleh perbankan yang dapat dikategorikan sebagai pencurian data pribadi nasabah?
2. Bagaimana tanggung jawab hukum perbankan dalam melindungi data pribadi nasabah?

B. Metodologi

Berdasarkan apa yang telah dijabarkan diatas, penelitian yang akan dijadikan acuan sebagai dasar analisis dalam penelitian hukum ini yaitu dengan menerapkan metode penelitian normatif yang bersifat deskriptif analisis dan lebih condong mengarah menggunakan analisis. Pada penelitian ini Penulis akan menganalisi yaitu : Sumber Hukum Primer dengan berupa Undang-Undang Dasar 1945, Undang-Undang Nomor 27 Tahun 2022 yang mengatur mengenai Pelindungan identitas Pribadi, ketentuan dalam Undang-Undang Nomor 11 Tahun 2008 jo. Undang-Undang Nomor 19 Tahun 2016 yang mengatur berkaitan dengan Informasi dan Transaksi Elektronik, Undang-Undang Nomor 21 Tahun 2008 yang berfungsi sebagai pengatur mengenai sistem dan operasional perbankan syariah di Indonesia, Ketentuan Regulator Keuangan Nasional terkait upaya melindungi konsumen serta teknologi informasi, sumber Hukum Sekunder dengan Berupa sumber kepustakaan hukum, jurnal ilmiah, karya tulis akademik, serta laporan media yang membahas tanggung jawab hukum, perlindungan data, dan studi kasus kebocoran data nasabah, sumber Hukum Tersier dengan kamus hukum, ensiklopedia, serta literatur pendukung lainnya. Pendekatan yang diterapkan dalam kajian ini yaitu dengan menerapkan pendekatan berdasarkan peraturan perundang-undangan (Statute Approach) dan pendekatan berbasis konsep (Conceptual Approach). Penelitian ini akan menggambarkan atau menguraikan suatu masalah secara jelas dan tepat tentang permasalahan yang kemudian hasilnya akan dianalisis dan diurutkan secara sistematis, penelitian diperiksa dan kemudian ditarik kesimpulan berdasarkan topik yang akan diteliti.

C. Hasil dan Pembahasan

Bentuk pelanggaran yang dilakukan oleh perbankan yang dapat dikategorikan sebagai pencurian data pribadi nasabah

Sektor perbankan merupakan elemen krusial dalam sistem perekonomian nasional karena berperan sebagai penghimpun dan penyalur dana masyarakat dalam jumlah besar. Oleh sebab itu, perlindungan terhadap kepentingan nasabah menjadi prioritas utama. Luasnya cakupan layanan perbankan yang mencakup berbagai aspek keuangan dan pelayanan publik membuka

kemungkinan terjadinya berbagai tindakan merugikan, baik terhadap institusi perbankan maupun nasabah (Shinta Dewi 2009).

Tindakan tersebut dapat berupa tindak pidana seperti pemalsuan, penggelapan, penipuan, hingga pencurian yang secara langsung berkaitan dengan aktivitas operasional perbankan. Situasi ini menuntut adanya regulasi yang ketat dan sistem penegakan hukum yang efektif demi menjaga integritas sektor perbankan dan memelihara kepercayaan masyarakat terhadap institusi keuangan. Dalam konteks hukum, berkembang dua konsep penting yang berkaitan dengan pelanggaran dalam sektor ini, yaitu tindak pidana perbankan dan tindak pidana di bidang perbankan. Menurut Moh. Anwar, perbedaan di antara keduanya terletak pada dasar hukum yang digunakan. Tindak pidana perbankan adalah pelanggaran terhadap standar yang diterapkan khusus berdasarkan Undang-Undang Perbankan, di mana sanksi hukum pidana juga disebutkan dalam perundang-undangan tersebut. Sebaliknya, tindak hukum pidana di bidang perbankan mencakup perbuatan melawan hukum yang terjadi dalam aktivitas perbankan, tetapi tunduk pada ketentuan hukum di luar Undang-Undang Perbankan (Gulo et al., 2021).

Di era digital, tantangan dalam sektor perbankan semakin kompleks dengan meningkatnya ketergantungan pada teknologi informasi. Salah satu masalah signifikan yang perlu ditangani secara serius adalah perlindungan data nasabah. Pengelolaan data nasabah secara digital menuntut sistem keamanan informasi yang andal, untuk mencegah kebocoran, penyalahgunaan, atau pencurian data pribadi yang dapat merugikan nasabah dan mencederai reputasi bank. Oleh karena itu, lembaga perbankan wajib mematuhi prinsip kehati-hatian serta peraturan yang mengatur perlindungan terhadap data pribadi, sebagaimana diatur dalam peraturan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Penerapan perlindungan data digital mencakup kewajiban bank untuk mengadopsi metode keamanan mutakhir, salah satunya enkripsi data, otentikasi ganda, serta pengawasan sistem secara berkala.

Di samping itu, transparansi kepada nasabah mengenai penggunaan data mereka serta mekanisme pengaduan bila terjadi pelanggaran, juga menjadi bagian integral dari perlindungan hukum. Dengan demikian, integritas sektor perbankan dapat terjaga tidak hanya melalui pengawasan terhadap tindak pidana konvensional, tetapi juga dengan penguatan keamanan dan keandalan sistem digital dalam menjaga kerahasiaan dan hak-hak nasabah.

Beberapa bentuk pelanggaran yang sering terjadi dalam praktik perbankan antara lain, pada sektor perbankan digital, perlindungan informasi pribadi pelanggan menjadi kewajiban hukum yang harus dijalankan secara konsisten oleh lembaga perbankan serta pihak ketiga yang berkolaborasi dengan bank. Pelanggaran terhadap prinsip-prinsip perlindungan data tidak hanya menimbulkan risiko hukum, tetapi juga berdampak pada reputasi dan kepercayaan publik terhadap lembaga keuangan. Terdapat beberapa bentuk pelanggaran yang sering terjadi dan memiliki konsekuensi hukum yang jelas antara lain (Roy, 2022):

Pertama, pengungkapan data pribadi tanpa persetujuan merupakan pelanggaran serius. Apabila bank atau pihak ketiga yang menjadi mitranya membagikan atau mengungkapkan data nasabah tanpa persetujuan eksplisit dari pemilik data, tindakan tersebut dianggap melanggar ketentuan yang tercantum dalam Pasal 26 Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) serta Pasal 39 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), sehingga dapat dikenakan sanksi hukum sesuai peraturan yang berlaku. Kami bertanggungjawab sepenuhnya atas terjadinya pelanggaran yang melibatkan penyebaran data pribadi tanpa persetujuan sah dari pemilik informasi tersebut. Tindakan ini bertentangan dengan UU ITE Pasal 26 dan UU PDP Pasal 39. Sebagai bentuk tanggung jawab, kami berkomitmen: Menyampaikan permintaan maaf, Memperbaiki sistem perlindungan data, Mencegah kejadian serupa di masa depan.

Kedua, Kebocoran data elektronik akibat kelalaian penyelenggara sistem, khususnya perbankan, merupakan bentuk pelanggaran yang tidak dapat diabaikan. Apabila sistem keamanan digital yang digunakan tidak sejalan dengan prinsip tata kelola teknologi informasi yang baik, sebagaimana diatur dalam POJK Nomor 38/POJK.03/2016 dan PBI Nomor 23/6/PBI/2021, maka hal tersebut dapat digolongkan sebagai kelalaian administratif dan etik. Kegagalan dalam melindungi data nasabah juga berpotensi melanggar Pasal 26 Undang Undang Nomor. 11 Tahun 2008 tentang ITE, yang menekankan perlindungan data pribadi. Tanggung jawab sepenuhnya berada pada pihak bank, yang wajib menerapkan manajemen risiko teknologi informasi secara optimal. Jika lalai, sanksi administratif dapat dijatuhkan sesuai Pasal 39 POJK 38/2016, termasuk peringatan tertulis hingga pembatasan kegiatan usaha.

Ketiga, Penyalahgunaan data pribadi, seperti penggunaan informasi nasabah untuk promosi tanpa izin, sering terjadi dalam praktik perbankan. Tindakan ini melanggar hak privasi dan tidak sesuai dengan prinsip pemrosesan data yang sah dan terbatas, sebagaimana diatur

dalam Pasal 26 Undang-undang ITE dan Pasal 20–39 Undang-undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Kami bertanggung jawab atas pelanggaran ini dan berkomitmen untuk menghentikan praktik yang tidak sesuai tersebut, memperbaiki sistem perlindungan data, serta memastikan kepatuhan terhadap peraturan yang berlaku di masa mendatang.

Keempat, kegagalan bank dalam memberikan notifikasi atas kebocoran data juga merupakan pelanggaran. Dalam hal terjadi insiden keamanan siber atau kebocoran data, bank wajib menyampaikan informasi kepada nasabah dalam jangka waktu tertentu. Kewajiban ini diatur dalam Pasal 46 Undang-Undang Nomor 27 Tahun 2022. Apabila bank lalai dalam menyampaikan notifikasi, maka dapat dikenai sanksi administratif dan dianggap melanggar etika perlindungan konsumen. Sebagai bentuk tanggung jawab, bank wajib segera memberikan pemberitahuan kepada nasabah ketika terjadi kebocoran data, melakukan investigasi dan perbaikan sistem keamanan, serta memastikan bahwa kejadian serupa tidak terulang di masa mendatang. Bank juga harus bekerja sama dengan otoritas terkait dan menjaga transparansi dalam proses penanganan insiden demi melindungi hak-hak nasabah.

Kelima, pelanggaran juga dapat terjadi karena ketiadaan rencana pemulihan dan mekanisme pengawasan keamanan data. Kewajiban bank untuk memiliki business continuity plan serta melakukan audit keamanan informasi secara berkala diatur dalam Peraturan Pemerintah (PP) Nomor 71 Tahun 2019 serta Peraturan Menteri Komunikasi dan informatika Nomor 20 Tahun 2016. Tidak tersedianya rencana kontinjensi dan lemahnya pengawasan membuat sistem bank rentan diretas, dan ini dapat dianggap sebagai pelanggaran kewajiban hukum dalam menjaga keamanan data pribadi nasabah. Bank berkewajiban untuk menyediakan rencana pemulihan yang handal serta melaksanakan audit keamanan secara rutin guna menjaga keandalan sistem dan perlindungan data. Upaya ini sangat penting untuk memastikan keamanan data pribadi nasabah tetap terjaga dan mengurangi potensi terjadinya kebocoran informasi.

Keenam, pelanggaran terhadap informasi perbankan sebagaimana telah ditetapkan dalam Pasal 40 ayat (1) Undang-Undang Perbankan juga merupakan bentuk pelanggaran hukum yang dapat menimbulkan akibat hukum secara perdata. Dalam konteks ini, apabila rahasia nasabah dibocorkan atau diakses secara tidak sah, nasabah berhak Mengajukan tuntutan ganti rugi dengan dasar adanya perbuatan yang melanggar ketentuan hukum. Bank memiliki tanggung jawab untuk memastikan keamanan dan kerahasiaan data nasabah secara optimal, menerapkan langkah-langkah pengamanan yang efektif, dan memberikan kompensasi jika terjadi pelanggaran yang disebabkan oleh kelalaian pihak bank.

Dengan demikian, lembaga perbankan wajib memastikan bahwa seluruh mekanisme perlindungan data pribadi dilaksanakan secara menyeluruh, mulai dari aspek teknis, administratif, hingga hukum. Kepatuhan terhadap peraturan perundang-undangan menjadi syarat mutlak dalam menjaga kepercayaan publik serta menjamin hak-hak nasabah atas data pribadinya.

Pelanggaran-pelanggaran tersebut menunjukkan bahwa keamanan digital merupakan tanggung jawab penting yang harus dipikul oleh perbankan. Selain memastikan perlindungan secara teknis, bank juga dituntut untuk menerapkan kebijakan perlindungan data yang transparan dan patuh terhadap ketentuan hukum yang berlaku, termasuk di dalamnya Undang-Undang Perlindungan Data Pribadi. Dengan demikian, perlindungan terhadap data nasabah bukan hanya berperan sebagai aspek teknis, sekaligus berperan sebagai bagian dari upaya memperkuat integritas dan akuntabilitas lembaga perbankan di mata publik.

Seperti pada kasus (BSI) Bank Syariah Indonesia merupakan salah satu bank syariah utama di Indonesia telah menyediakan layanan perbankan digital yang memudahkan nasabah mengakses berbagai produk dan layanan melalui perangkat elektronik. Namun, seiring dengan meningkatnya pemanfaatan teknologi informasi, risiko terhadap keamanan data pribadi nasabah juga semakin besar. Ancaman seperti serangan siber, phishing, malware, dan denial of service (DoS) menjadi tantangan serius dalam menjaga kepercayaan nasabah. Kasus gangguan layanan digital yang dialami BSI pada 8 Mei 2023 menjadi ilustrasi nyata. Selain karena pemeliharaan sistem, terdapat dugaan upaya peretasan yang menyebabkan nasabah kesulitan mengakses layanan seperti BSI Mobile, ATM, dan teller. Meskipun pihak bank menyatakan bahwa data dan dana nasabah tetap aman, kejadian tersebut memicu instruksi Otoritas Jasa Keuangan (OJK) untuk memastikan pemulihan layanan serta peningkatan ketahanan digital seluruh lembaga perbankan.

Pelanggaran terhadap data pribadi nasabah dalam layanan perbankan digital umumnya dipicu oleh dua penyebab utama, yakni dari dalam dan luar institusi. Dari sisi internal, hal ini

dapat terjadi karena sistem keamanan yang tidak memadai, keteledoran atau penyimpangan yang dilakukan oleh pegawai, minimnya proses pengawasan dan audit, serta ketidakkonsistenan dalam penerapan kebijakan perlindungan data. Kurangnya pembaruan rutin pada sistem keamanan dapat membuka peluang bagi pihak yang tidak bertanggung jawab untuk mengakses data pribadi secara ilegal. Di samping itu, pegawai yang memiliki wewenang terhadap informasi sensitif berisiko menyalahgunakannya apabila tidak diawasi secara optimal. Lemahnya pengawasan dan proses audit juga berkontribusi terhadap sulitnya mendeteksi pelanggaran, sementara kebijakan internal yang tidak tegas memperbesar kemungkinan terjadinya kebocoran data. Di sisi lain, faktor eksternal muncul dari perkembangan teknologi yang semakin rumit namun belum sepenuhnya dijangkau oleh regulasi yang memadai. Ketidaksempurnaan sistem hukum, perbedaan kebijakan antar wilayah, serta lambannya adaptasi regulasi terhadap dinamika digital membuka celah bagi penyalahgunaan data pribadi. Selain itu, kejahatan siber yang bersifat lintas negara dan semakin canggih menjadi tantangan tersendiri dalam proses penegakan hukum. Selain itu, minimnya pemahaman masyarakat mengenai pentingnya menjaga data pribadi menjadikan nasabah lebih mudah menjadi korban penipuan digital. Maraknya jual beli data pribadi secara ilegal di pasar gelap, ditambah dengan lemahnya infrastruktur keamanan siber nasional, semakin memperparah kondisi tersebut.(Santoso 2019).

Dengan demikian, upaya melindungi data pribadi dalam layanan perbankan digital harus dilakukan secara komprehensif. Teknologi saja tidak cukup; diperlukan kerja sama antara institusi keuangan, regulator, aparat penegak hukum, serta partisipasi aktif dari masyarakat. Kolaborasi lintas sektor ini merupakan elemen penting dalam membangun ekosistem perbankan digital yang aman, dapat dipercaya, dan berkelanjutan di tengah dinamika ancaman yang terus berkembang.

Dalam konteks tanggung jawab hukum perbankan terhadap perlindungan data pribadi nasabah, kasus kebocoran data pada Bank Syariah Indonesia (BSI) tahun 2023 bukanlah satu-satunya insiden yang menunjukkan lemahnya tata kelola data pribadi di sektor jasa keuangan. Sebelumnya, terjadi pula kasus kebocoran data nasabah Kreditplus pada tahun 2020 yang melibatkan hampir 896 ribu data nasabah tersebar di forum hacker internasional. Peristiwa ini menegaskan bahwa penyelenggara sistem elektronik di sektor keuangan belum sepenuhnya menerapkan standar keamanan digital sesuai dengan ketentuan peraturan perundang-undangan.

Demikian pula kasus kebocoran 91 juta data pengguna Tokopedia pada tahun 2020, meskipun tidak secara langsung berkaitan dengan perbankan, tetap relevan karena menunjukkan lemahnya perlindungan data dalam ekosistem digital nasional. Bahkan di tingkat internasional, kasus Equifax pada tahun 2017 yang mengakibatkan kebocoran 147 juta data pribadi di Amerika Serikat berujung pada denda sebesar USD 700 juta, menjadi pembelajaran bahwa korporasi dapat dimintai pertanggungjawaban hukum secara serius jika lalai menjaga keamanan data.(Demak 2020)

Secara teoritis, pembahasan ini dapat dijelaskan melalui beberapa teori. Pertama, Teori Tanggung Jawab Hukum sebagaimana dikemukakan Hans Kelsen, menegaskan bahwa setiap pelanggaran norma hukum menimbulkan konsekuensi sanksi. Dalam hal ini, bank sebagai penyelenggara sistem elektronik berkewajiban secara hukum apabila lalai menjaga kerahasiaan data nasabah. Kedua, Teori Perlindungan Hukum dari Philipus M. Hadjon yang membagi perlindungan hukum menjadi preventif dan represif. Perlindungan preventif dapat diwujudkan melalui sistem keamanan, audit berkala, dan transparansi, sedangkan perlindungan represif dilakukan melalui mekanisme sanksi dan pemulihan hak nasabah setelah terjadinya kebocoran data. Ketiga, Teori Hak Privasi yang dipelopori Samuel D. Warren dan Louis D. Brandeis dengan konsep the right to be let alone, menegaskan bahwa setiap individu berhak atas kerahasiaan data pribadinya.

Dengan demikian, setiap kebocoran data pribadi nasabah perbankan merupakan bentuk pelanggaran atas hak privasi yang fundamental. Keempat, Teori Pertanggung jawaban Pidana Korporasi sebagaimana dijelaskan Rusianto, bahwa korporasi dapat dimintai pertanggungjawaban pidana apabila terjadi tindak pidana atau kelalaian serius. Hal ini menegaskan bahwa bank, sebagai badan hukum, tidak hanya memiliki tanggung jawab administratif dan perdata, tetapi juga dapat dimintai pertanggungjawaban pidana atas kelalaian dalam menjaga data pribadi nasabah.

Tanggung Jawab Hukum Perbankan Dalam Melindungi Data Pribadi Nasabah

Aktivitas perbankan di Indonesia yang beroperasi dalam sistem demokrasi ekonomi bertumpu pada prinsip kehati-hatian sebagai fondasi utamanya. Prinsip ini bukan hanya aspek teknis semata, tetapi juga mencerminkan nilai-nilai yang sejalan dengan ideologi Pancasila dan tujuan nasional sebagaimana diatur dalam Undang-Undang Dasar Negara Republik Indonesia Tahun 1945. Perbankan yang berlandaskan pada prinsip demokrasi ekonomi mencerminkan keterlibatan masyarakat secara aktif dalam pembentukan arah dan kebijakan sektor perbankan. Dalam hal ini, pemerintah memegang peran penting untuk memberikan panduan dan dukungan guna mendorong perkembangan sektor perbankan, sekaligus menciptakan iklim usaha yang kondusif dan berkelanjutan dalam konteks pembangunan ekonomi.

Pasal 1 ayat (3) Undang-Undang Dasar 1945 menegaskan bahwa Indonesia merupakan negara yang berdasarkan hukum, sehingga semua kegiatan ekonomi perbankan di tanah air harus dijalankan sesuai dengan prinsip-prinsip hukum yang berlaku dan tidak melanggar peraturan yang ada. Selain itu, ketentuan serupa juga diatur dalam Pasal 1 angka (28) Undang-Undang Nomor 10 Tahun 1998 yang merevisi Undang-Undang Nomor 7 Tahun 1992 tentang perbankan. Rahasia bank mencakup seluruh informasi yang berkaitan dengan identitas nasabah serta detail simpanan yang tersimpan di bank. Penjelasan ini menegaskan pentingnya menjaga dan melindungi kerahasiaan data pribadi nasabah. Ketentuan ini juga diatur dalam Pasal 40 ayat (1) Undang-Undang Perbankan, yang mewajibkan bank untuk menjaga kerahasiaan informasi nasabah beserta simpanannya.

Pasal 26 ayat (1) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik menyatakan bahwa penggunaan data pribadi melalui perangkat elektronik harus mendapat persetujuan dari pemilik data, kecuali jika ada ketentuan khusus yang diatur dalam peraturan perundang-undangan lainnya. Aturan ini juga diperkuat oleh regulasi Bank Indonesia Nomor 7/PBI/2005, yang menjadi landasan bagi ketentuan dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Tujuan dari regulasi ini adalah agar nasabah dapat memahami risiko yang terkait dengan produk perbankan yang ditawarkan, sekaligus memastikan perlindungan data pribadi nasabah tetap terjaga.

Merujuk pada insiden kebocoran data pribadi yang menimpa BSI, pihak bank memiliki tanggung jawab untuk menjaga kerahasiaan serta keamanan data nasabah. Meski demikian, penting untuk dicatat bahwa Indonesia telah menetapkan regulasi terkait perlindungan data pribadi sejak September tahun sebelumnya. Seperti yang disampaikan oleh Pratama Persadha, apabila Bank Syariah Indonesia terbukti melakukan pelanggaran, maka akan dikenai sanksi administratif sesuai dengan ketentuan yang tercantum dalam Pasal 57 Undang-Undang Perlindungan Data Pribadi. Namun, implementasi undang-undang tersebut baru akan berlaku efektif pada Oktober 2024, sementara hingga kini, otoritas yang bertugas untuk mengawasi dan menegakkan perlindungan data pribadi masih belum dibentuk.

insiden tersebut diharapkan menjadi momentum untuk mendorong perbaikan nyata dalam sistem pencegahan dan penanganan kebocoran data pribadi. Dengan penegakan kebijakan perlindungan data yang ketat, pemanfaatan teknologi yang andal, serta transparansi dalam merespons insiden, sektor perbankan dituntut untuk memulihkan kepercayaan nasabah dan memastikan perlindungan atas kerahasiaan data mereka, Dengan demikian, diharapkan potensi kebocoran informasi di sektor ini dapat dicegah. Risiko dalam industri perbankan perlu ditekan seminimal mungkin agar para pengguna layanan merasa lebih aman, nyaman, dan terlindungi secara optimal.Kasus kebocoran data nasabah Bank Syariah Indonesia (BSI) tahun 2023 menunjukkan bahwa bank sebagai pengendali data pribadi belum sepenuhnya memenuhi kewajibannya sesuai dengan ketentuan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Kegagalan BSI dalam menjamin keamanan informasi pribadi nasabah bukan sekadar persoalan teknis, tetapi juga merupakan bentuk kelalaian hukum yang dapat dimintai pertanggungjawaban pidana, perdata, maupun administratif.

Dari perspektif Teori Tanggung Jawab Hukum Hans Kelsen, peristiwa ini mencerminkan adanya pelanggaran norma hukum yang mengikat bank sebagai penyelenggara sistem elektronik, sehingga secara yuridis dapat dikenakan sanksi sebagai konsekuensi logis dari pelanggaran tersebut. Selain itu, jika ditinjau melalui Teori Perlindungan Hukum Philipus M. Hadjon, kasus BSI memperlihatkan lemahnya perlindungan preventif karena tidak adanya sistem keamanan siber yang memadai, dan sekaligus lemahnya perlindungan represif karena bank terlambat memberikan notifikasi kepada nasabah atas insiden kebocoran data. Kondisi ini menimbulkan kerugian ganda, yakni hilangnya hak nasabah atas kerahasiaan data sekaligus menurunnya tingkat kepercayaan publik terhadap sistem perbankan digital. Lebih jauh lagi, kasus ini juga dapat dikaitkan dengan Teori Hak Privasi Warren dan Brandeis, bahwa setiap individu berhak untuk dilindungi dari intervensi pihak lain terkait data pribadinya, Dengan

bocornya data 15 juta nasabah BSI, hak privasi tersebut telah dilanggar secara serius. Terakhir, dalam kerangka Teori Pertanggungjawaban Pidana Korporasi Rusianto, bank sebagai badan hukum dapat dimintai pertanggungjawaban pidana karena kelalaian atau kesengajaan dalam menjaga data pribadi nasabah termasuk ke dalam kategori perbuatan melawan hukum yang merugikan masyarakat luas. Dengan demikian, kasus BSI merupakan cerminan nyata perlunya penegakan hukum yang tegas serta penguatan regulasi dalam rangka menjamin kepastian hukum dan perlindungan hak fundamental nasabah.

D. Kesimpulan

Berbagai bentuk pelanggaran dalam sektor perbankan digital, seperti pengungkapan data pribadi tanpa persetujuan, kebocoran data akibat kelalaian sistem, penyalahgunaan data untuk kepentingan komersial, keterlambatan notifikasi kepada nasabah, hingga ketiadaan rencana pemulihan keamanan, secara yuridis dapat dikategorikan sebagai tindak pencurian maupun penyalahgunaan data pribadi nasabah. Seluruh perbuatan tersebut jelas bertentangan dengan ketentuan dalam UU ITE, UU PDP, POJK, PBI, serta UU Perbankan, dan mencerminkan lemahnya penerapan prinsip kehati-hatian serta akuntabilitas bank sebagai penyelenggara sistem elektronik. Pelanggaran ini tidak hanya menimbulkan kerugian finansial bagi nasabah, tetapi juga merusak hak fundamental atas privasi dan menurunkan kepercayaan publik terhadap integritas lembaga perbankan. Dengan demikian, dapat ditegaskan bahwa setiap kelalaian dalam menjaga data pribadi nasabah merupakan bentuk perbuatan melawan hukum yang harus dipertanggung jawabkan secara administratif, perdata, maupun pidana.

Bank sebagai pengendali data pribadi memiliki tanggung jawab hukum yang bersifat menyeluruh, baik secara administratif, perdata, maupun pidana, sebagaimana diatur dalam UU PDP, UU ITE, dan regulasi sektor keuangan (POJK dan PBI). Kasus kebocoran data BSI 2023 menunjukkan bahwa kelalaian bank dalam menjaga keamanan data nasabah bukan sekadar persoalan teknis, tetapi merupakan pelanggaran hukum yang menuntut pertanggungjawaban nyata.

Saran

Untuk mencegah terulangnya pelanggaran berupa kebocoran, penyalahgunaan, dan pengungkapan data pribadi tanpa izin, bank perlu memperkuat sistem keamanan siber melalui penerapan teknologi enkripsi, otentikasi berlapis, dan audit keamanan secara berkala. Selain itu, bank wajib membentuk prosedur notifikasi cepat kepada nasabah setiap kali terjadi insiden keamanan, agar nasabah dapat segera melakukan langkah mitigasi. Dengan cara ini, risiko kerugian finansial maupun kerugian atas hak privasi nasabah dapat diminimalisir sejak dini.

Agar tanggung jawab hukum perbankan dapat berjalan efektif, bank perlu membentuk unit khusus perlindungan data (Data Protection Officer/DPO) yang berfungsi mengawasi kepatuhan terhadap UU PDP dan regulasi OJK-BI. Selain itu, bank harus menyusun kebijakan internal yang transparan terkait pengelolaan data, melakukan pelatihan privasi bagi karyawan, serta memperkuat mekanisme pengawasan pihak ketiga (vendor/mitra teknologi), contohnya kaya Bank, OJK, Dan BI Dengan demikian, tanggung jawab hukum perbankan tidak hanya bersifat normatif di atas kertas, tetapi benar-benar terlaksana dalam praktik untuk melindungi hak-hak nasabah secara nyata.

E. Referensi

Dewi, S. (2023). Perlindungan Hukum Data Pribadi Nasabah Dalam CBDC. Review UNES, 6(4), 10661–10675.

Haryanto, S. (2023). Perlindungan Hukum Nasabah Dalam Internet Banking. Jurnal Magister Hukum Udayana, Universitas Warmadewa.

Katiandagho, V., Putong, D. D., & Melo, I. J. (2023). UU PDP Memperkuat UU Perbankan Dalam Melindungi Data Nasabah. Jurnal Hukum to-ra, 9(1), 106–114.

Kurniawan, A. (2023). Perlindungan Data Pribadi Konsumen Dalam Transaksi Elektronik. Jurnal Rechtsvinding, 12(1), 1285–1329.

Maisah, S. P. S., Sudiarni, & Ompusunggu, H. P. (2023). Analisis Hukum Perlindungan Data Pribadi Nasabah Dalam Perbankan Digital. Aufklarung: Jurnal Pendidikan, 3(3), 285–290.

Nasution, R. A., Ginting, B., & Siregar, M. (2024). Perlindungan Hukum Terhadap Data Pribadi Nasabah Layanan Perbankan Setelah Berlakunya POJK No. 6/POJK.07/2022. JEHSS, 7(1), 71–78.

Prayogo, P. (2023). Perlindungan Hukum Data Pribadi Nasabah Pada Internet Banking. Nuansa Akademik, 1(2), 2089–2101.
Priowirjanto, S., & Dewantara, R. (2022). Pemanfaatan AI dalam Aktivitas Perbankan dan Perlindungan Data. Jurnal Komunikasi Hukum, 7(2), 663–677.
Juanda, F. M. (2019). Tanggung Jawab Penyelenggara Sistem Elektronik. Skripsi, UIN Syarif Hidayatullah Jakarta.
Yudistira, I. G. W. (2023). Tanggung Jawab Hukum Bank terhadap Kebocoran Data Pribadi Nasabah. Jurnal Ilmiah Mahasiswa, Universitas Mataram.
Gulo, A. S., Lasmadi, S., & Nawawi, K. (2021). Cyber Crime dalam Bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik. PAMPAS: Journal of Criminal Law, 1(2), 32-41
Dewi, S. (2009). Perlindungan Privasi Atas Informasi Pribadi dalam E-Commerce Menurut Hukum Internasional. Cyber Law, 10-12
Mahesa Jati Kusuma S.H, M.H. (2015). Hukum Perlindungan Nasabah Bank.
Rusianto, A. (2016). Tindak Pidana dan Pertanggungjawaban Pidana. Kencana.
Utami, A. S. S. (2023). Hukum Perlindungan Data Pribadi: Cerdas dan Bijak Menggunakan Media Sosial untuk Melindungi Data Pribadi.
Santosa, B. (2019). Data Mining: Teknik Pemanfaatan Data untuk Keperluan Bisnis. Graha Ilmu.
Pratama, M. A. M., & Suryokencono, P. (2024). Tanggung Jawab Bank BSI Atas Kebocoran Data Nasabah. Indonesian Journal of Law and Justice (IJLJ), 3(1), 45–60. https://doi.org/10.47134/ijlj.v3i1.4804
Suwardi, S. H., M. H. (2018). Hukum Dagang: Suatu Pengantar.
Roy, D. S. (2022). Cyber Law. Bandung: CV. Cakra.
Santoso, T. (2019). Manajemen Keuangan dan Hukum Perbankan. Jakarta: Erlangga.
https://repository.uinjkt.ac.id/dspace/bitstream/123456789/47272/1/FAJAR%20MUHAMMAD%20JUANDA-FSH.pdf
https://ifrelresearch.org/index.php/Doktrin-widyakarya/article/download/3202/3041/12696