KAMPUS AKADEMIK PUBLISING
Jurnal Multidisiplin Ilmu Akademik
Vol.2, No.1 Februari 2025
e-ISSN: 3032-7377; p-ISSN: 3032-7385, Hal 316-327
DOI: https://doi.org/10.61722/jmia.v2i1.3147

Penyalahgunaan Data Pribadi dalam Teknologi Transaksi Digital di Industri Perbankan Digital (Studi Kasus PT. Bank Syariah Indonesia)

Revalina Annisa Antoine
Universitas Negeri Semarang
Najalya Siti Farizqa
Universitas Negeri Semarang
Alifia Hafizha Hasna
Universitas Negeri Semarang
Masta Pasaribu
Universitas Negeri Semarang
Alamat: Fakultas Hukum, Universitas Semarang, Kota Semarang, Jawa Tengah
Korespondensi penulis: annisareva91@students.unnes.ac.id

Abstrak. *This article discusses the misuse of personal data in the use of digital transaction technology in the digital banking industry, with a case study of the customer data breach at PT Bank Syariah Indonesia (BSI) in 2023. Although regulations for personal data protection, such as Law Number 27 of 2022, have been implemented, weak enforcement and supervision have created opportunities for data misuse. The data breach case at BSI shows that human factors, cyberattacks, and non-compliance with security procedures can contribute to this issue. This research uses a normative legal method to evaluate the actions taken in response to the data breach by aligning them with applicable legal principles. The data used in this study is sourced from primary legal materials, including relevant laws and regulations, as well as secondary and tertiary legal materials to deepen the analysis. This study aims to identify the causes of personal data misuse and propose solutions, including strengthening security systems, updating regulations, and raising awareness about the importance of personal data protection. It is expected that the findings will serve as a reference for financial institutions to enhance customer data protection in the future and prevent similar incidents from recurring.*
Keywords: *Data Protection, Cybersecurity, Banking Regulations*

Abstrak. Artikel ini membahas tentang penyalahgunaan data pribadi dalam pemanfaatan teknologi transaksi digital di industri perbankan digital, dengan studi kasus kebocoran data nasabah PT. Bank Syariah Indonesia (BSI) pada 2023. Meskipun regulasi perlindungan data pribadi, seperti Undang-Undang Nomor 27 Tahun 2022, telah diterapkan, implementasi dan pengawasan yang lemah membuka peluang bagi penyalahgunaan data. Kasus kebocoran data di BSI menunjukkan bahwa faktor manusia, serangan siber, dan ketidakpatuhan terhadap prosedur keamanan dapat berkontribusi terhadap permasalahan ini. Penelitian ini menggunakan metode hukum normatif untuk mengevaluasi tindakan yang diambil terkait kasus kebocoran data dengan mencocokkannya dengan prinsip-prinsip hukum yang berlaku. Data yang digunakan berasal dari bahan hukum primer, termasuk undang-undang dan regulasi terkait, serta bahan hukum sekunder dan tersier untuk memperdalam analisis. Penelitian ini bertujuan untuk mengidentifikasi faktor penyebab penyalahgunaan data pribadi dan menawarkan solusi berupa penguatan sistem keamanan, pemutakhiran regulasi, serta peningkatan kesadaran akan pentingnya perlindungan data pribadi. Diharapkan, temuan ini dapat menjadi acuan bagi institusi keuangan dalam meningkatkan perlindungan data nasabah di masa depan dan mencegah kejadian serupa terulang kembali.
Kata Kunci: *Perlindungan Data, Keamanan Siber, Regulasi Perbankan*

PENDAHULUAN

Kemajuan dalam bidang teknologi informasi dan komunikasi telah menghadirkan transformasi yang bermakna di berbagai bidang, tidak terkecuali dalam sektor perbankan. Dalam upaya mendukung transformasi digital perbankan, Otoritas Jasa Keuangan (OJK) telah menerbitkan regulasi berupa Peraturan OJK No.12/POJK.03/2018 yang mengatur tentang implementasi Layanan Perbankan Digital untuk Bank Umum. Dalam peraturan tersebut, OJK

Received September 30, 2024; Revised Oktober 30, 2024;Desember 16, 2024
* Revalina Annisa Antoine, annisareva91@students.unnes.ac.id

mendefinisikan layanan perbankan digital sebagai sistem layanan perbankan elektronik yang dikembangkan dengan mengutamakan penggunaan optimal data nasabah, bertujuan untuk memberikan pelayanan yang lebih cepat, mudah, dan disesuaikan dengan kebutuhan nasabah, serta memungkinkan nasabah untuk melakukan transaksi secara mandiri dengan tetap memperhatikan aspek keamanan. Regulasi ini diharapkan dapat mendorong institusi perbankan untuk memaksimalkan penggunaan teknologi dalam rangka memenuhi kebutuhan dan memberikan kemudahan bagi para nasabah (Mutiasari, A. I. 2020). Meskipun demikian, kemudahan yang ditawarkan oleh layanan perbankan digital juga membawa konsekuensi berupa risiko keamanan data pribadi nasabah yang signifikan. Contoh konkretnya adalah kasus kebocoran data Bank Syariah Indonesia (BSI) pada tahun 2023. Pada bulan Mei 2023, BSI menghadapi permasalahan dalam mengakses sistem mereka dan diduga menjadi target serangan ransomware dari kelompok peretas yang dikenal sebagai LockBit 3.0. Serangan siber tersebut memberikan kesempatan bagi kelompok peretas untuk mengakses berbagai informasi nasabah, meliputi nama, konfigurasi host, informasi domain, konfigurasi local drive, berbagi jarak jauh, dan perangkat penyimpanan eksternal. Terlepas dari statusnya sebagai bank syariah terbesar di Indonesia, BSI tetap tidak luput dari tantangan yang umumnya dihadapi oleh industri perbankan, khususnya dalam hal pencurian data pribadi nasabah (Dwinanda, Duata, Ridanhus, dan Tarina 2023). Kasus pembobolan data yang terjadi di Bank Syariah Indonesia telah menimbulkan dampak yang signifikan, tidak hanya dari segi finansial dan reputasi bank, namun juga menciptakan kerentanan bagi nasabah terhadap berbagai bentuk penipuan dan pencurian identitas. Peristiwa ini telah menggarisbawahi berbagai tantangan dalam aspek keamanan siber yang membutuhkan penanganan serius, termasuk di dalamnya perlindungan data pribadi dan keuangan, pemutakhiran sistem keamanan, serta peningkatan kesadaran akan pentingnya keamanan siber (Hutagalung, Marendra, dan Hosnah 2024).

Perlindungan data pribadi telah diatur dalam beberapa regulasi. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi merupakan salah satu regulasi yang paling relevan, yang menyediakan landasan hukum untuk melindungi data pribadi masyarakat dari penyalahgunaan. Regulasi ini secara komprehensif mengatur hak-hak pemilik data, kewajiban pengendali data, dan konsekuensi hukum bagi para pelanggar. Meskipun kerangka hukum telah tersedia, implementasinya dalam praktik sehari-hari masih menghadapi berbagai kendala, terutama dalam sektor perbankan digital yang memiliki tingkat kompleksitas yang tinggi. Kasus kebocoran data nasabah Bank Syariah Indonesia menjadi bukti konkret bagaimana kelemahan dalam sistem keamanan dapat dieksploitasi oleh pihak-pihak yang tidak bertanggung jawab, yang mengakibatkan kerugian material maupun non-material bagi nasabah serta mencederai reputasi institusi perbankan.

Kemudian, penting untuk mengidentifikasi faktor-faktor yang menyebabkan data pribadi nasabah di industri perbankan digital dapat disalahgunakan. Faktor manusia seringkali menjadi penyebab utama kebocoran data, di mana karyawan yang kurang terlatih atau lalai dalam menjalankan protokol keamanan dapat menjadi titik kerentanan dalam sistem. Di samping itu, perkembangan serangan siber yang semakin canggih juga menjadi ancaman yang harus diwaspadai. Oleh karena itu, pemahaman mendalam mengenai penyalahgunaan data pribadi memerlukan analisis komprehensif terhadap berbagai faktor yang berkontribusi terhadap permasalahan ini.

Selanjutnya, pertanyaan yang muncul adalah bagaimana penyalahgunaan data pribadi dalam pemanfaatan teknologi transaksi digital di industri perbankan digital dapat terjadi, khususnya dalam konteks kasus bocornya data nasabah PT. Bank Syariah Indonesia. Kasus ini

mengindikasikan bahwa meskipun regulasi perlindungan data telah ada, implementasi dan pengawasan yang lemah dapat membuka celah bagi penyalahgunaan. Dalam berbagai kasus, kebocoran data terjadi akibat kombinasi serangan siber yang berhasil dan ketidakpatuhan terhadap prosedur keamanan yang berlaku. Selain itu, kurangnya transparansi dalam pengelolaan data dapat mengakibatkan nasabah tidak menyadari risiko yang mereka hadapi, sehingga mereka tidak mengambil langkah-langkah pencegahan yang diperlukan.

Penyalahgunaan data pribadi dalam pemanfaatan teknologi transaksi digital di industri perbankan digital merupakan permasalahan yang membutuhkan perhatian serius. Kasus kebocoran data nasabah PT Bank Syariah Indonesia menjadi pengingat bahwa perlindungan data pribadi harus menjadi prioritas utama bagi institusi keuangan. Melalui pemahaman yang lebih mendalam tentang faktor-faktor penyebab dan mekanisme penyalahgunaan data, didukung oleh regulasi yang kuat dan edukasi kepada nasabah, diharapkan kejadian serupa dapat diantisipasi dan dicegah di masa yang akan datang.

KAJIAN TEORI

Bagian Kajian teori dalam penelitian ini berfokus pada penyalahgunaan data pribadi dalam konteks pemanfaatan teknologi transaksi digital di industri perbankan, terutama terkait kebocoran data nasabah. Pertama, teori perlindungan data pribadi menekankan pentingnya perlindungan data sebagai hak fundamental yang harus dijamin oleh negara dan lembaga. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi menjadi dasar hukum yang mengatur hak-hak pemilik data dan kewajiban pengendali data, sehingga lembaga keuangan, termasuk bank, memiliki tanggung jawab untuk melindungi data nasabah dari penyalahgunaan.

Teori keamanan siber menjelaskan berbagai ancaman yang dihadapi oleh sistem digital, seperti serangan siber dan pencurian identitas. Peningkatan penggunaan teknologi dalam perbankan digital membuat pemahaman terhadap teori ini sangat penting untuk menyusun strategi mitigasi yang efektif. Selanjutnya, teori manajemen risiko berfokus pada identifikasi, analisis, dan mitigasi risiko yang terkait dengan penyalahgunaan data, di mana penerapan kebijakan dan prosedur keamanan yang ketat sangat diperlukan.

Teori kepatuhan hukum juga relevan, karena menjelaskan pentingnya kepatuhan terhadap regulasi yang ada. Meskipun regulasi perlindungan data sudah diterapkan, implementasinya sering kali lemah, dan penelitian ini akan mengeksplorasi bagaimana ketidakpatuhan terhadap regulasi dapat berkontribusi pada risiko penyalahgunaan data.

Penelitian sebelumnya menunjukkan bahwa kebocoran data di sektor perbankan sering disebabkan oleh kombinasi faktor manusia, kelemahan sistem keamanan, dan serangan siber. Selain itu, banyak penelitian mengungkapkan bahwa kurangnya pelatihan karyawan dan ketidakpatuhan terhadap prosedur keamanan menjadi penyebab utama kebocoran data. Dengan mengintegrasikan berbagai teori ini, penelitian ini bertujuan untuk mengidentifikasi faktor-faktor penyebab kebocoran data dan menawarkan solusi yang dapat meningkatkan perlindungan data nasabah di masa depan.

METODE PENELITIAN

Metode penelitian yang diterapkan adalah penelitian hukum normatif. Melalui metode ini, peneliti dapat melakukan evaluasi kritis terhadap tindakan yang dilakukan dengan cara mencocokkannya dengan prinsip-prinsip hukum yang berlaku. Dengan demikian, dapat diketahui apakah tindakan tersebut sudah sesuai dengan aturan hukum yang ada atau justru bertentangan. Dalam penelitian ini, data utama yang digunakan bersumber dari bahan hukum primer, yang mencakup Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, serta Undang-undang Nomor 10 Tahun 1998 Tentang Perbankan, dan regulasi terkait lainnya. Bahan hukum primer ini menyediakan landasan konkret yang diperlukan untuk melakukan analisis dan evaluasi terhadap berbagai tindakan yang berkaitan dengan kasus yang sedang diteliti.

Penelitian ini juga memanfaatkan bahan hukum sekunder dan tersier sebagai elemen pendukung dalam proses analisis. Berbagai sumber seperti artikel, jurnal, dan buku yang berkaitan dengan topik penelitian digunakan sebagai referensi tambahan untuk memperkuat dan memperdalam pemahaman terhadap isu hukum yang sedang dikaji. Bahan hukum sekunder ini membuka wawasan yang luas dan memungkinkan peneliti untuk mengamati permasalahan dari berbagai perspektif yang mungkin tidak tercakup dalam bahan hukum primer. Dalam pengumpulan data, penelitian ini menerapkan metodologi yang cermat dan sistematis, di mana proses identifikasi, pengumpulan, dan analisis data dilaksanakan dengan teliti untuk menjamin tingkat validitas dan reliabilitas yang tinggi.

HASIL PENELITIAN DAN PEMBAHASAN

1. Faktor Penyebab Penyalahgunaan Data Pribadi Nasabah di Industri Perbankan Digital

Uraian Di era digital kontemporer, informasi telah menjadi faktor krusial yang menentukan dinamika ekonomi negara, baik yang sedang berkembang maupun sudah maju. Meskipun pemerintah dan sektor swasta secara tradisional mengelola informasi individu, kemunculan teknologi digital telah menghadirkan ancaman yang lebih kompleks dan sistematis terhadap privasi personal. Ledakan pertumbuhan data pribadi yang disimpan dan ditransmisikan melalui komputer dan perangkat mobile telah menciptakan kerentanan baru. Kemajuan teknologi tidak hanya membuka peluang inovasi, tetapi juga menimbulkan risiko serius terhadap keamanan dan integritas informasi individu, dengan potensi kerugian yang jauh lebih besar akibat kebocoran atau penyalahgunaan data. Teknologi digital telah mentransformasi cara penyimpanan, distribusi, dan pemanfaatan informasi pribadi, membuat individu semakin rentan terhadap potensi pelanggaran privasi dan eksploitasi data yang tidak bertanggung jawab (Shinta Dewi 2009).

Perlindungan Data Pribadi adalah hal yang sangat penting bagi masyarakat untuk memperoleh perlindungan atas hak pribadinya. Hak atas perlindungan data pribadi secara khusus berhubungan dengan jaminan hak konstitusional yang tercantum dalam Pasal 28F Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, yang memberikan jaminan kepada setiap warga negara untuk memperoleh, mengolah, serta mengelola informasi yang berasal dari berbagai macam fasilitas (Aji 2023). Jaminan konstitusional ini menegaskan bahwa selain berhak untuk memperoleh, mengolah, dan mengelola informasi, setiap individu juga berhak mendapatkan perlindungan keamanan terkait data pribadi dalam proses pertukaran informasi.

Perusahaan pengelola data pribadi, khususnya penyedia layanan fintech sebagai pengendali data korporasi, memikul tanggung jawab penuh atas keamanan informasi. Mereka wajib mematuhi Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi untuk

menjamin keamanan dan privasi pengguna. Tanggung jawab ini mencakup pencegahan dan penanganan kebocoran data, baik yang disebabkan oleh pihak ketiga maupun yang terjadi secara disengaja. Kewajiban perlindungan data merupakan komitmen utama dalam menjaga kepercayaan dan kerahasiaan informasi konsumen. Sesuai dengan ketentuan dalam pasal 40 ayat (1) Undang-undang Nomor 10 Tahun 1998 Tentang Perbankan, bank diwajibkan menjaga kerahasiaan informasi nasabah penyimpan dan simpanannya. Pasal tersebut dengan tegas mengamanatkan bahwa bank harus menjaga kerahasiaan segala keterangan terkait identitas dan data nasabah. Sejalan dengan undang-undang tersebut, Otoritas Jasa Keuangan (OJK) mengeluarkan surat edaran Nomor 14/SEOJK.07/2014 tentang Kerahasiaan dan Keamanan Data dan/atau Informasi Pribadi Konsumen. Surat edaran ini mencakup Para Pelaku Usaha Jasa Keuangan (PUJK), termasuk bank, dalam menjaga kerahasiaan data konsumen. Kedua regulasi tersebut bertujuan melindungi kepentingan dan privasi nasabah di sektor perbankan, menegaskan tanggung jawab lembaga keuangan dalam menjaga kerahasiaan informasi pribadi (Bhoki, Aloysius, dan Bire 2024).

Penyalahgunaan data pribadi nasabah di industri perbankan digital semakin menjadi perhatian utama di tengah pesatnya perkembangan teknologi. Banyak nasabah yang kurang memahami risiko yang terkait dengan penyampaian informasi pribadi mereka, seperti nomor rekening dan kata sandi. Kejahatan siber, termasuk penipuan dan pencurian identitas, sering kali terjadi akibat lemahnya sistem keamanan yang diterapkan oleh bank. Data yang seharusnya dilindungi dengan baik dapat dengan mudah diakses oleh pihak yang tidak bertanggung jawab, menyebabkan kerugian finansial yang signifikan bagi nasabah. Selain itu, kejadian semacam ini juga dapat merusak reputasi lembaga keuangan dan menurunkan kepercayaan masyarakat terhadap layanan perbankan digital. Untuk itu, penting bagi bank dan penyedia layanan digital untuk terus meningkatkan sistem keamanan mereka, dengan menerapkan teknologi terbaru dan memastikan kebijakan perlindungan data pribadi sesuai dengan regulasi yang berlaku. Keamanan data pribadi yang lebih kuat tidak hanya akan melindungi nasabah, tetapi juga membantu menjaga keberlanjutan bisnis di tengah meningkatnya ancaman siber (Romadhonia, Nahdliyin, dan Janah 2024).

Di sisi lain, kurangnya regulasi yang tegas dan pemahaman tentang pentingnya perlindungan data pribadi menjadi tantangan besar bagi industri perbankan. Banyak nasabah tidak mendapatkan informasi yang cukup mengenai cara melindungi data mereka saat bertransaksi secara online. Oleh karena itu, penting bagi bank untuk memperkuat sistem keamanan dan menerapkan kebijakan perlindungan data yang lebih ketat. Edukasi kepada nasabah mengenai langkah-langkah pencegahan juga harus menjadi prioritas utama. Dengan upaya ini, diharapkan nasabah dapat lebih sadar akan pentingnya menjaga data pribadi mereka, serta meningkatkan kepercayaan terhadap layanan perbankan digital. Selain itu, bank juga perlu bekerja sama dengan otoritas terkait untuk memastikan bahwa regulasi yang ada dapat diterapkan secara efektif, serta menciptakan lingkungan yang lebih aman bagi nasabah. Keberhasilan dalam meningkatkan perlindungan data pribadi tidak hanya bergantung pada teknologi, tetapi juga pada kesadaran bersama antara lembaga keuangan dan nasabah dalam menjaga privasi informasi yang bersifat sensitif (Hisbulloh t.t.). Terdapat 2 faktor yang menyebabkan penyalahgunaan data pribadi nasabah di industri perbankan digital, yaitu:

a) Faktor Internal

Faktor internal penyebab penyalahgunaan data pribadi berasal dari dalam lembaga, seperti kelemahan dalam sistem keamanan, kelalaian atau tindakan tidak sah dari karyawan, serta kurangnya pengawasan dan audit yang efektif.

Penyebab lain terjadinya faktor internal :

1. Lemahnya Sistem Keamanan Internal

Salah satu faktor internal utama penyebab penyalahgunaan data pribadi adalah lemahnya sistem keamanan yang diterapkan oleh lembaga perbankan. Meski banyak bank menggunakan teknologi seperti enkripsi dan otentikasi dua faktor, sistem ini bisa memiliki celah jika tidak diperbarui atau diawasi secara terus-menerus. Sistem yang tidak cukup kuat dapat memberikan peluang bagi pihak yang tidak berwenang untuk mengakses data pribadi nasabah, baik melalui peretasan (hacking) atau penyalahgunaan sistem yang ada.

2. Kebocoran Data dari Karyawan atau Pihak Internal

Penyalahgunaan data pribadi tidak selalu berasal dari pihak eksternal. Seringkali, data nasabah bocor karena kelalaian atau tindakan yang disengaja dari pihak internal, seperti karyawan bank yang memiliki akses langsung ke data tersebut. Tanpa pengawasan yang ketat, karyawan atau pihak internal bisa saja menyalahgunakan data pribadi nasabah untuk keuntungan pribadi atau bahkan menjual data tersebut kepada pihak ketiga. Kebocoran data internal ini bisa sangat merugikan, karena pihak bank sendiri memiliki akses penuh terhadap informasi sensitif nasabah.

3. Kurangnya Pengawasan dan Audit Keamanan

Faktor internal lainnya adalah kurangnya pengawasan yang memadai terhadap sistem perlindungan data dan kebijakan yang diterapkan. Tanpa audit rutin dan evaluasi yang tepat, celah keamanan dalam sistem digital dapat terlewatkan. Pengawasan yang lemah bisa menyebabkan potensi penyalahgunaan data oleh pihak internal yang tidak terdeteksi. Oleh karena itu, bank perlu melakukan pemeriksaan dan audit berkala untuk memastikan bahwa kebijakan dan prosedur keamanan data berjalan sesuai dengan standar yang berlaku.

4. Penerapan Kebijakan yang Tidak Konsisten

Internal bank yang tidak memiliki kebijakan perlindungan data yang jelas dan konsisten juga dapat menyebabkan penyalahgunaan data. Kebijakan yang tidak tegas atau berubah-ubah dalam mengelola data pribadi nasabah dapat menciptakan kebingungannya pengelola data internal serta memberi ruang bagi kebocoran atau penyalahgunaan data pribadi. Tanpa adanya regulasi yang kuat, implementasi kebijakan perlindungan data bisa menjadi tidak efektif.

b) Faktor Eksternal

Dalam konteks penyalahgunaan data pribadi nasabah di industry perbankan digital, faktor eksternal memiliki peran signifikan yang mencakup beberapa dimensi penting. Pertama, lingkungan teknologi yang semakin kompleks dan rentan terhadap serangan siber menjadi faktor eksternal utama, di mana kemajuan teknologi informasi telah membuka celah keamanan yang dapat dimanfaatkan oleh pihak-pihak yang tidak bertanggung jawab. Hal ini terjadi karena ekosistem digital perbankan yang terintegrasi secara global menciptakan jaringan komunikasi dan transaksi yang sangat luas, memungkinkan pelaku kejahatan untuk menemukan kerentanan keamanan dengan lebih mudah. Kedua, aspek regulasi dan penegakan hukum yang belum sepenuhnya komprehensif turut berkontribusi terhadap risiko penyalahgunaan data, di mana kerangka hukum yang ada belum mampu sepenuhnya melindungi data pribadi nasabah dari potensi pelanggaran. Ketidakselarasan regulasi antarwilayah dan lambatnya proses adaptasi hukum terhadap perkembangan teknologi digital semakin memperparah situasi, menciptakan ruang abu-abu yang dapat dieksploitasi oleh pelaku kejahatan siber.

Selain itu, faktor lingkungan eksternal seperti meningkatnya aktivitas kejahatan siber internasional dan kompleksitas jaringan kriminal digital turut memperburuk situasi keamanan data. Karakteristik kejahatan siber yang bersifat lintas batas negara dan menggunakan teknologi canggih membuat proses pelacakan dan penindakan menjadi sangat sulit. Ketidakmampuan

lembaga perbankan untuk selalu beradaptasi dengan cepat terhadap modus operandi baru para pelaku kejahatan siber menjadi tantangan tersendiri, di mana setiap inovasi keamanan selalu diikuti oleh metode peretasan baru yang lebih kompleks. Faktor eksternal lainnya termasuk kurangnya kesadaran masyarakat akan pentingnya keamanan data pribadi, yang membuat nasabah rentan terhadap praktik penipuan dan manipulasi digital. Praktik perdagangan data ilegal yang masih marak terjadi di pasar gelap internet semakin memperburuk situasi, di mana data pribadi dapat dengan mudah diperjualbelikan kepada pihak-pihak yang tidak bertanggung jawab. Keterbatasan infrastruktur teknologi keamanan informasi yang memadai di tingkat nasional turut berkontribusi terhadap risiko penyalahgunaan data, mengingat tidak semua lembaga perbankan memiliki kemampuan teknologi dan sumber daya yang sama untuk mengimplementasikan sistem keamanan mutakhir.

Dampak dari faktor-faktor eksternal tersebut tidak hanya berdimensi teknologi, tetapi juga meliputi aspek sosial, ekonomi, dan hukum. Kompleksitas ancaman terhadap keamanan data pribadi nasabah menuntut pendekatan komprehensif dan kolaboratif dari seluruh pemangku kepentingan, mulai dari lembaga perbankan, pemerintah, penegak hukum, hingga masyarakat umum.

2. Penyalahgunaan Data Pribadi Dalam Pemanfaatan Teknologi Transaksi Digital di Industri Perbankan Digital dapat Terjadi dalam Kasus Data Nasabah PT. Bank Syariah Indonesia

Perbankan digital semakin diminati karena memberikan kenyamanan dan efisiensi waktu. Namun, perlindungan terhadap nasabah saat menggunakan layanan perbankan digital menjadi isu yang sangat penting, mengingat adanya berbagai ancaman keamanan seperti pencurian identitas, penipuan, gangguan transaksi, serangan malware yang dapat merusak sistem keamanan perbankan digital, serta kebocoran data pribadi. Oleh karena itu, melakukan analisis terhadap perlindungan nasabah di Bank Syariah Indonesia (BSI) dalam penggunaan layanan perbankan digital bukan hanya penting, tetapi juga sangat krusial. Digitalisasi di sektor keuangan telah meningkatkan kemungkinan terjadinya serangan siber hingga 86,70%. Menurut IMF (International Monetary Fund), total kerugian tahunan rata-rata yang dialami oleh sektor jasa keuangan di seluruh dunia akibat serangan siber diperkirakan mencapai USD100 miliar, yang setara dengan lebih dari Rp1.433 triliun. Di Asia Tenggara, Indonesia menempati peringkat kelima dalam hal keamanan siber. Melihat kondisi ini, penting bagi institusi keuangan untuk memperkuat sistem perlindungan nasabah agar dapat memitigasi risiko yang muncul akibat penggunaan teknologi digital dalam transaksi perbankan.

Bank Syariah Indonesia (BSI) menyediakan layanan perbankan digital yang memungkinkan nasabah untuk mengakses berbagai layanan perbankan melalui perangkat digital seperti smartphone, tablet, atau komputer. Secara umum, nasabah menghadapi beragam risiko keamanan saat menggunakan layanan perbankan digital, termasuk risiko keamanan siber, phishing, malware, dan serangan denial of service (DoS) (Nadzirin Anshari Nur dkk. 2022) . Risiko keamanan siber mencakup ancaman dari individu atau kelompok yang tidak bertanggung jawab yang berusaha untuk mengakses, merusak, atau mencuri data serta informasi penting dari sistem perbankan digital. Dengan meningkatnya penggunaan teknologi dalam perbankan, penting bagi BSI untuk menerapkan langkah-langkah keamanan yang efektif guna melindungi nasabah dari risiko-risiko tersebut.

Pada 8 Mei 2023, Bank Syariah Indonesia (BSI) mengalami disrupsi layanan digital yang berlangsung selama beberapa hari. Gangguan ini tidak hanya disebabkan oleh perawatan sistem yang terjadwal, tetapi juga terdapat indikasi adanya upaya peretasan. Para nasabah BSI menghadapi berbagai kendala dalam mengakses layanan perbankan, termasuk ketidakmampuan untuk melakukan transaksi melalui BSI Mobile, kesulitan menggunakan ATM, serta hambatan dalam pelayanan teller (Ayu Andreana Beru Tarigan dan Hartono Paulus t.t.) BSI kemudian memberikan klarifikasi pada 16 Mei 2023, menegaskan bahwa meskipun terjadi gangguan layanan, keamanan data nasabah dan dana mereka tidak terkompromikan. Menanggapi insiden tersebut, Otoritas Jasa Keuangan (OJK) menginstruksikan BSI untuk memastikan normalisasi seluruh layanannya. Lebih lanjut, OJK juga mengeluarkan himbauan kepada seluruh institusi keuangan di sektor perbankan untuk meningkatkan kapabilitas ketahanan digital mereka.

Seiring dengan pesatnya perkembangan era digital, masalah kebocoran data telah menjadi tantangan krusial yang dihadapi berbagai sektor, khususnya industri perbankan. Meskipun bukan fenomena baru, kebocoran data pribadi tetap menjadi persoalan yang mengkhawatirkan dan membutuhkan perhatian serius. Ketika informasi sensitif nasabah terekspos, seperti nomor rekening, detail kartu kredit, data identitas personal, dan catatan keuangan, konsekuensinya bisa sangat merugikan. Kebocoran semacam ini dapat terjadi melalui beragam cara, mulai dari serangan siber yang terencana, pelanggaran protokol keamanan oleh pihak internal, hingga ketidakcermatan dalam manajemen data. Dampak dari kebocoran data perbankan tidak hanya terbatas pada risiko langsung seperti pencurian identitas, aktivitas penipuan, dan penyalahgunaan keuangan. Lebih jauh lagi, insiden semacam ini dapat mengikis kepercayaan nasabah terhadap lembaga perbankan yang terdampak dan mengakibatkan kerusakan reputasi yang substansial bagi institusi tersebut.

Pada hakikatnya, perlindungan hukum merupakan perwujudan dari pemenuhan hak-hak yang semestinya diterima oleh konsumen. Kewajiban dalam memberikan perlindungan kepada konsumen bukan hanya menjadi beban pemerintah semata, tetapi juga merupakan tanggung jawab yang harus dipikul oleh para pelaku usaha, termasuk di dalamnya institusi perbankan seperti PT. Bank Syariah Indonesia. Lingkup perlindungan konsumen mencakup berbagai dimensi hukum yang komprehensif, meliputi aspek hukum perdata, hukum administrasi, dan hukum pidana. Perlindungan ini tidak semata-mata terbatas pada pemberian kompensasi atau pengenaan sanksi terhadap pelaku usaha yang melakukan pelanggaran, melainkan mencakup spektrum yang lebih luas dalam upaya menjamin hak-hak konsumen.

Bank Syariah Indonesia (BSI) telah menerapkan serangkaian langkah pengamanan untuk melindungi kepentingan nasabahnya. Dalam menghadapi ancaman ransomware, institusi yang menjadi target serangan perlu berkoordinasi dengan aparat penegak hukum, institusi penanggulangan darurat siber, maupun perusahaan yang bergerak di bidang keamanan siber. BSI menggunakan beragam teknologi pengamanan, termasuk sistem enkripsi data, verifikasi dua tahap, serta berbagai sistem keamanan tambahan. Sebagai respons terhadap insiden gangguan layanan dan potensi kebocoran data yang terjadi sebelumnya, BSI telah menganggarkan dana sebesar Rp 580 miliar untuk memperkuat aspek digitalisasi dan keamanan data nasabah. BSI menegaskan bahwa alokasi anggaran tersebut akan difokuskan pada penguatan sistem pengamanan data dan layanan perbankan. Dalam upaya pencegahan, BSI melakukan penguatan sistem

keamanan teknologi informasi untuk mengantisipasi potensi gangguan data melalui peningkatan sistem proteksi dan ketahanan. BSI juga menjalin koordinasi dengan berbagai lembaga terkait, termasuk Badan Siber dan Sandi Negara (BSSN), Otoritas Jasa Keuangan (OJK), dan Bank Indonesia (BI).

Transformasi digital dalam industri perbankan telah meningkatkan eksposur bank terhadap risiko keamanan siber. Meningkatnya frekuensi serangan siber telah menciptakan urgensi untuk memperkuat ketahanan siber (cyber resilience) melalui peningkatan keamanan siber (cyber security). Penguatan sistem keamanan siber telah memicu berbagai inisiatif di berbagai sektor industri, terutama di sektor perbankan, dimana regulator di berbagai negara berupaya mengatasi risiko siber (cyber risk). Bank Syariah Indonesia dan institusi perbankan lainnya di Indonesia perlu memprioritaskan penguatan sistem pertahanan digital mereka, mengingat sektor keuangan, khususnya perbankan, menjadi target utama serangan siber baik dalam skala global maupun nasional. Berbagai langkah strategis yang perlu diimplementasikan mencakup pengembangan kebijakan pengelolaan keamanan siber, implementasi sistem penilaian risiko siber, pelaksanaan uji kerentanan teknologi informasi, evaluasi tingkat maturitas siber, serta pelaksanaan pengujian keamanan siber yang mengacu pada praktik terbaik yang telah teruji di berbagai negara.

Walaupun telah dilakukan peningkatan keamanan jaringan dan sistem melalui implementasi firewall, sistem enkripsi data, dan monitoring secara aktif untuk mencegah serangan siber, tidak ada sistem yang dapat menjamin keamanan sepenuhnya dari ancaman ransomware. Dengan demikian, menjadi sangat krusial untuk menerapkan strategi mitigasi yang tepat dan melakukan persiapan yang matang. Bank Syariah Indonesia sebaiknya mempertimbangkan untuk mengadopsi praktik-praktik terbaik yang telah terbukti efektif dan diterapkan di berbagai negara, dalam upaya memitigasi potensi ancaman dan kerentanan siber yang dapat membahayakan keamanan sistem digital mereka.

Bank Syariah Indonesia memiliki kewajiban pertanggungjawaban atas insiden kebocoran data nasabah, yang didasarkan pada prinsip-prinsip yang tertuang dalam Undang-Undang Perlindungan Konsumen (UUPK) (Anon t.t.-a) Tanggung jawab ini merupakan bagian integral dari prinsip pertanggungjawaban perdata yang meliputi:

1. Prinsip kesalahan merupakan dasar pertanggungjawaban hukum. Artinya, seseorang wajib mengganti kerugian yang ditimbulkannya jika terbukti secara hukum bahwa tindakannya melanggar hukum, sebagaimana diatur dalam Pasal 1365 KUHPerdata.
2. Prinsip praduga bersalah membebankan tanggung jawab pembuktian pada tergugat. Tergugat dianggap bertanggung jawab atas suatu kerugian hingga ia dapat membuktikan bahwa dirinya tidak bersalah. Prinsip ini bertujuan untuk memastikan bahwa setiap pihak yang menyebabkan kerugian harus bertanggung jawab.
3. Prinsip bahwa konsumen tidak selalu bisa meminta ganti rugi kepada penjual hanya berlaku dalam situasi tertentu, terutama dalam transaksi sehari-hari yang masuk akal.
4. Prinsip tanggung jawab mutlak atau strict liability menyatakan bahwa seseorang dapat dibebankan tanggung jawab atas kerugian yang ditimbulkan tanpa perlu membuktikan adanya unsur kesalahan. Meskipun demikian, terdapat pengecualian dalam keadaan kahar atau force majeure.

5. Prinsip pembatasan tanggung jawab mengharuskan adanya batasan yang jelas terhadap kewajiban pihak yang bertanggung jawab, dengan tetap mengutamakan perlindungan konsumen dan kepatuhan terhadap peraturan perundang-undangan.

   Berdasarkan Undang-Undang Perlindungan Konsumen (UUPK), PT. Bank Syariah Indonesia memiliki tanggung jawab mutlak terhadap kebocoran data nasabah, yang berarti bank harus memberikan pertanggungjawaban tanpa perlu adanya pembuktian kesalahan terlebih dahulu. UUPK mengatur berbagai bentuk kompensasi untuk perbuatan melawan hukum, mencakup ganti rugi nominal, kompensasi, dan ganti rugi penghukuman (Anon t.t.-b) Hal ini sejalan dengan ketentuan dalam Undang-Undang Nomor 21 Tahun 2008 Pasal 47 ayat (1) tentang perbankan syariah, yang mewajibkan bank syariah untuk menjaga kerahasiaan data dan informasi nasabah. Ketika terjadi kebocoran data nasabah, bank syariah bertanggung jawab atas kerugian yang muncul, kecuali dapat membuktikan bahwa kebocoran tersebut terjadi di luar kesalahan bank syariah. Lebih lanjut, Pasal 48 ayat (1) undang-undang tersebut menetapkan kewajiban bank syariah untuk memberikan ganti rugi atas kerugian yang dialami nasabah akibat perbuatan melawan hukum, baik yang dilakukan oleh bank syariah maupun pegawainya. Bentuk ganti rugi yang dapat diberikan meliputi ganti rugi nominal, kompensasi, dan ganti rugi penghukuman.

   Terkait insiden kebocoran data nasabah Bank Syariah Indonesia yang diduga merupakan hasil peretasan, prinsip-prinsip hukum yang berlaku mengharuskan BSI untuk memberikan kompensasi kepada para nasabah yang terkena dampak. Mengingat kejadian ini telah menimbulkan kerugian bagi nasabah, pihak bank memiliki kewajiban untuk memberikan ganti rugi sesuai dengan ketentuan hukum yang berlaku. Para nasabah memiliki hak untuk mengajukan tuntutan ganti rugi melalui mekanisme hukum yang telah ditetapkan dalam peraturan yang berlaku, dimana beban pembuktian dalam kasus ini menjadi tanggung jawab nasabah yang mengalami kerugian. Seiring dengan pesatnya perkembangan ekonomi digital, kebutuhan akan perlindungan data nasabah dalam layanan perbankan digital semakin mendesak. Untuk membangun kepercayaan dan memastikan keberlangsungan bisnis di era digital, bank syariah harus memprioritaskan keamanan data nasabah. Implementasi kebijakan dan regulasi yang kuat serta penerapan teknologi keamanan mutakhir menjadi kunci utama dalam menjaga kerahasiaan dan integritas data nasabah.

KESIMPULAN

Penyalahgunaan data pribadi nasabah di industri perbankan digital merupakan isu penting yang semakin mendapat perhatian seiring dengan pesatnya perkembangan teknologi. Faktor penyebabnya terbagi menjadi dua kategori utama: faktor internal dan eksternal. Faktor internal mencakup kelemahan dalam sistem keamanan perbankan, kelalaian atau tindakan tidak sah dari karyawan, serta kurangnya pengawasan yang memadai. Sedangkan faktor eksternal berkaitan dengan ancaman siber global, kurangnya regulasi yang memadai, serta meningkatnya kesadaran yang rendah dari masyarakat tentang pentingnya perlindungan data pribadi.

Perlindungan data pribadi nasabah sangat penting, baik dalam konteks hukum maupun teknologi. Dalam hal ini, bank sebagai pengelola data harus mematuhi regulasi yang berlaku, seperti Undang-Undang Perlindungan Data Pribadi dan peraturan Otoritas Jasa Keuangan (OJK), untuk menjaga kepercayaan dan privasi nasabah. Kejadian kebocoran data, seperti yang terjadi di

Bank Syariah Indonesia, menegaskan perlunya penguatan sistem keamanan dan kesadaran tentang potensi risiko yang bisa terjadi akibat serangan siber.

Tanggung jawab hukum atas kebocoran data pribadi sangat jelas, di mana bank diharuskan memberikan kompensasi kepada nasabah yang dirugikan, sesuai dengan prinsip hukum perlindungan konsumen. Upaya untuk mengatasi penyalahgunaan data pribadi harus mencakup tidak hanya peningkatan teknologi, tetapi juga pemahaman dan kesadaran yang lebih tinggi dari pihak bank dan nasabah. Mengingat ancaman yang terus berkembang, penting bagi industri perbankan untuk terus berinovasi dan memperkuat sistem keamanan serta bekerjasama dengan pihak berwenang guna menciptakan lingkungan yang lebih aman bagi nasabah.

DAFTAR PUSTAKA

Adolph, Ralph. 2016. "Perlindungan Hukum Penyalahgunaan Data Pribadi Nasabah Sebagai Konsumen Perbankan Berkaitan Dengan Rahasia Bank (Studi Kasus Di PT Bank Muamalat KC Surabaya)," 1–23.

Aji, Muhammad Prakoso. 2023. "Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi) [Cyber Security System and Data Sovereignty in Indonesia in Political Economic Perspective]." *Jurnal Politica Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional* 13 (2): 222–38. https://doi.org/10.22212/jp.v13i2.3299.

Dewi, S. (2009). *Perlindungan Privasi Atas Informasi Pribadi dalam E-Commerce Menurut Hukum Internasional.* Cyber Law.

Dwinanda, Arya m, dan ilham muhammad duata. 2023. "Nusantara: Jurnal Ilmu Pengetahuan Sosial Perlindungan Hukum Terhadap Data Diri Nasabah Bank Pada Kasus Bank Syariah Indonesia 1." *Jurnal Ilmu Pengetahuan Sosial* 11 (11): 4979–89. http://jurnal.um-tapsel.ac.id/index.php/nusantara/index.

Efendi, Taufik Kukuh, Muhammad Esza, Maulana Firmanda, Fathor Rozy Alfarisy, Alfado Chievo Javantara, and Rachma Indrarini. 2024. "Analisis Kebijakan Perlindungan Nasabah Pada Bank Digital Syariah Di Indonesia" 2 (November): 1–7.

Fadhlina, Amilah, Regina Resentia, Syarifah Fatimahtazzuhrah Rukhsal, Herpandu Hadiwibowo, dan Alicia Shafa Azzahra. 2024. "Perlindungan Data Pribadi Nasabah dalam Transaksi Central Bank Digital Currency (CBDC) dalam Rupiah Digital" 7 (1): 307–17.

Fakultas, Jurnal, and Hukum Unsrat. 2024. "Jurnal Fakultas Hukum Unsrat Lex Privatum. Vol 13. No. 01. 2024" 13 (01): 1–17.

Fatmala Putri, Dewi, dan Widya Ratna Sari. 2023. "Analisis Perlindungan Nasabah BSI Terhadap Kebocoran Data Dalam Menggunakan Digital Banking." *Jurnal Ilmiah Ekonomi dan Manajemen* 1 (4): 173–81. https://doi.org/10.61722/jiem.v1i4.331.

Hijriani, Hijriani, Muh. Nadzirin Anshari Nur, Adnan Ali, Azis Ali, dan Winner A. Siregar. 2023. "Literasi Digital Perlindungan Hukum Terhadap Data Pribadi Nasabah Pengguna Electronic Wallet." *Sultra Research of Law* 5 (2): 85–95.

https://doi.org/10.54297/surel.v5i2.59.

Keliat, Venia Utami, Andini Pratiwi Siregar, Suhaila Zulkifli, and Iin Purba. 2023. "Analisis Upaya Dan Peran Perlindungan Hukum Terhadap Kasus Peretasan Data Bank Syariah Indonesia." *Ilmu Hukum Prima (IHP)* 6 (2): 182–90. https://doi.org/10.34012/jihp.v6i2.4251.

Kesuma, A. A. Ngurah Deddy Hendra, I Nyoman Putu Budiartha, and Puru Ayu Sriasih Wesna. 2021. "Perlindungan Hukum Terhadap Keamanan Data Pribadi Konsumen Teknologi Finansial Dalam Transaksi Elektronik." *Jurnal Preferensi Hukum* 2 (2): 411–16. https://doi.org/10.22225/jph.2.2.3350.411-416.

Kurnianingrum, Trias Palupi. 2020. "Urgensi Pelindungan Data Pribadi Konsumen Di Era Ekonomi Digital." *Kajian* 25 (3): 197–216. https://www.

Monica Pertiwi, Herbasuki Nurcahyanto Departemen. 2011. "Efektivitas Program Bpjs Kesehatan Di Kota Semarang (Studi Kasus pada Pasien Pengguna Jasa BPJS Kesehatan di Puskesmas Srondol) Oleh : Monica Pertiwi , Herbasuki Nurcahyanto Departemen Administrasi Publik Fakultas Ilmu Sosial dan Ilmu Politik Universita." *Departemen Administrasi Publik Fakultas Ilmu Sosial dan Ilmu Politik Universitas Diponegoro*, 1–14.

Muhammad, Anggi, Chandraca Hutagalung, Nadia Rhaesa Marendra, dan Asmak Ul. 2024. "Perlindungan Terhadap Konsumen Dalam Kasus Kebocoran Data Bank Syariah Indonesia." *Jurnal Ilmu Hukum, Sosial, dan Humaniora* 2 (1): 156–65.

Mutiasari, Annisa Indah. 2020. "Perkembangan Industri Perbankan Di Era Digital." *Jurnal Ekonomi Bisnis Dan Kewirausahaan* 9 (2): 32–41. https://doi.org/10.47942/iab.v9i2.541.

Putusan, Analisis, Pengadilan Tata, Usaha Negara, D I Desa, Tanah Merah, dan Kabupaten Kupang. 2023. "Petitum LawJournal" 1 (1): 177–88.

Romadhonia, Annisa, Sukma Hidayatun Nahdliyin, dan Miftakhul Janah. 2024. "Peran Literasi Digital Bagi Masyarakat Dalam Mengurangi Dampak Kejahatan Transaski Elektronik Illegal." *Jurnal Hukum Ius Publicum* 5 (1): 176–201. https://doi.org/10.55551/jip.v5i1.96.

Soemitra, Andri, and Adlina. 2022. "Perlindungan Konsumen Terhadap Kebocoran Data Pada Jasa Keuangan Di Indonesia." *Jurnal Insitusi Politeknik Ganesha Medan Juripol* 5: 288–303.

Tambunan, Lambok. 2014. "Jurnal Hukum" 37 (2): 24.

Tarigan, Herdian Ayu Andreana Beru, dan Darminto Hartono Paulus. 2019. "Perlindungan Hukum Terhadap Nasabah Atas Penyelenggaraan Layanan Perbankan Digital." *Jurnal Pembangunan Hukum Indonesia* 1 (3): 294–307. https://doi.org/10.14710/jphi.v1i3.294-307.