Ranah Research
Journal of Multidisciplinary Research and Development
E-ISSN: 2655-0865
DINASTI RESEARCH
082170743613 ranahresearch@gmail.com https://jurnal.ranahresearch.com

DOI: https://doi.org/10.38035/rrj.v7i5

Analisis Hukum terhadap Kebocoran Data Pribadi dan Penyalahgunaan Identitas dalam Perbankan Berdasarkan Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi

Lenny Maria Aritonang[1], Zyetwill[2], Rara Handayani[3]
[1] Universitas Prima Indonesia, lennymaria90@yahoo.com
[2] Universitas Prima Indonesia, Zyetwil123@gmail.com
[3] Universitas Prima Indonesia, rarahandayani999@gmail.com

Corresponding Author: lennymaria90@yahoo.com [1]

Abstract: *This study aims to analyze and explain the legal certainty of personal data protection with reference to Article 65 of Law Number 27 of 2022, in order to provide an overview of the applicable regulations and their implementation. It also seeks to identify and describe the legal remedies available to bank customers to ensure the protection of their personal data, including mechanisms for prevention, supervision, and law enforcement. Furthermore, the study analyzes the impacts of personal data breaches on victims in financial, psychological, and social aspects, to understand the extent of risks and consequences faced by individuals whose data is compromised. This research employs a normative legal method. The results indicate that personal data breaches in the banking sector reflect the weak implementation of Law Number 27 of 2022 on Personal Data Protection (PDP Law), despite banks being obligated to safeguard such data. Affected customers are entitled to pursue legal action through the Financial Services Authority (OJK), the Ministry of Communication and Information (Kominfo), law enforcement, or civil lawsuits. The impacts include financial losses, psychological distress, and loss of trust and social reputation.*

Keywords: *legal analysis, personal data breach, identity misuse, banking, Law Number 27 of 2022*

Abstrak: Penelitian ini bertujuan untuk menganalisis dan menjelaskan kepastian hukum perlindungan data pribadi dengan merujuk pada Pasal 65 Undang-Undang No. 27 Tahun 2022, sehingga dapat memberikan gambaran tentang regulasi yang berlaku dan implementasinya, untuk mengidentifikasi dan menguraikan upaya-upaya hukum apa saja yang dapat dilakukan oleh nasabah untuk menjamin perlindungan data pribadinya, termasuk mekanisme pencegahan, pengawasan, dan penegakan hukum, serta untuk menganalisis dampak yang timbul akibat kebocoran data pribadi terhadap korban, baik dari segi finansial,

psikologis, maupun sosial, untuk memahami sejauh mana risiko dan konsekuensi yang dihadapi oleh individu yang datanya bocor. Peneliti menggunakan metode penelitian hukum yang bersifat normatif. Hasil penelitian menunjukkan bahwa Kebocoran data pribadi nasabah perbankan menunjukkan lemahnya implementasi UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), meskipun bank berkewajiban menjaga keamanan data. Nasabah yang dirugikan berhak menempuh upaya hukum melalui OJK, Kominfo, kepolisian, atau jalur perdata. Dampak kebocoran meliputi kerugian finansial, tekanan psikologis, serta hilangnya kepercayaan dan reputasi sosial korban.

Kata Kunci: analisis hukum, kebocoran data pribadi, penyalahgunaan identitas, perbankan, Undang Nomor 27 Tahun 2022

PENDAHULUAN

Dalam era digital yang semakin berkembang pesat, perlindungan data pribadi menjadi tantangan global yang mendesak. Di berbagai belahan dunia, instansi pemerintahan dan sektor swasta menghadapi risiko kebocoran data pribadi yang dapat mengancam privasi individu (Iswandari, 2021). Fenomena ini mendorong banyak negara untuk merumuskan undang-undang perlindungan data pribadi sebagai langkah proaktif untuk mengatasi tantangan tersebut. Indonesia, sebagai bagian dari komunitas global ini, juga merespons dengan mengeluarkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

Di Indonesia, perkembangan teknologi informasi dan penetrasi internet telah mencapai tingkat yang signifikan. Ketergantungan masyarakat terhadap layanan digital dan penggunaan data pribadi untuk keperluan administratif, bisnis, dan sosial semakin meluas. Namun, seiring dengan keuntungan tersebut, muncul tantangan baru terkait keamanan data pribadi. Kasus kebocoran data di berbagai sektor, termasuk instansi pemerintahan, menjadi perhatian serius yang memerlukan respons tegas dan efektif (E. F. Pakpahan, Chandra, & Dewa, 2020). Data pribadi adalah aset yang sangat berharga, hal tersebut dikarenakan data pribadi mengandung nilai ekonomi yang tinggi. Di era sekarang kita diharuskan untuk memberikan data pribadi jika ingin menggunakan layanan dari instansi pemerintahan maupun instansi swasta.

Dari berbagai kasus kebocoran data pribadi yang terjadi, salah satu Instansi Pemerintahan yang memiliki kasus kebocoran yang sering terjadi adalah Instansi Perbankan, saat ingin memiliki rekening maka masyarakat diharuskan untuk memberikan beberapa data penting sebagai persyaratan, seperti KTP (Kartu Tanda Penduduk), Kartu Keluarga, Nama Ibu dan lain-lain. Menjaga kerahasiaan data pribadi nasabah merupakan tanggung jawab dan kewajiban dari bank, namun tak jarang bank gagal menjaga data pribadi nasabahnya dari kebocoran. Terkait kebocoran data pribadi di bank adalah suatu masalah yang sangat serius karena sangat merugikan nasabah dan juga bank itu sendiri, kebocoran data yang terjadi dapat merusak kepercayaan nasabah kepada bank karena merugikan nasabah secara finansial, psikologi dan sosial. Hal tersebut juga berarti bank gagal dalam menjalankan kewajibannya sebagai Instansi yang harus menjamin keamanan informasi nasabah dan integritas sistem keuangan.

Kasus-kasus kebocoran data pribadi di Indonesia menunjukkan kompleksitas dan dampak yang dapat merugikan masyarakat secara luas. Salah satu kasus kebocoran data yang terjadi pada seorang nasabah Bank Rakyat Indonesia (BRI) yang selanjutnya disebut bank menunjukkan kelemahan dalam sistem keamanan informasi dan pengawasan internal bank, berdasarkan kronologi yang terjadi bahwa data pribadi nasabah bocor dan disalahgunakan oleh pegawai internal bank untuk membuat kartu kredit tanpa sepengetahuan pemilik data, akibat dari penyalahgunaan tersebut, nasabah yang tidak pernah mengajukan kartu kredit tercatat dalam Sistem Layanan Informasi Keuangan (SLIK) OJK sebagai debitur yang bermasalah dengan status kolektibilitas (Coll 5). Nasabah dalam hal ini baru mengetahui

adanya kartu kredit fiktif setelah mengajukan Kredit Kepemilikan Rumah (KPR) ke bank lain dan ditolak karena status Coll 5 tersebut, proses penyelesaian masalah yang lambat dan tidak transparan oleh pihak bank menunjukkan kurangnya akuntabilitas dan tanggung jawab pengendali data pribadi sebagaimana yang diatur dalam Pasal 65 Undang-Undang Perlindungan Data Pribadi yang selanjutnya disebut UU PDP (Leonard, Sitompul, Tanjaya, & Esther, 2023). Kasus ini juga menyoroti ketidakmampuan sistem keamanan yang dapat dieksploitasi oleh pihak yang tidak bertanggung jawab, serta menimbulkan kekhawatiran terkait privasi dan keamanan data.

Menghadapi tren kebocoran data yang semakin meningkat, pemerintah Indonesia mengambil langkah serius untuk melindungi hak privasi warganya dengan meratifikasi Undang-Undang Nomor 27 Tahun 2022 (Irmawati, 2023). Undang-undang ini tidak hanya menetapkan standar perlindungan data yang tinggi, tetapi juga memberikan dasar hukum bagi pemerintah untuk mengatasi dan mencegah kebocoran data pribadi. Tetapi berdasarkan kasus kebocoran data yang terjadi dapat disimpulkan bahwa implementasi Pasal 65 UU PDP di sektor perbankan masih lemah, terutama dalam hal keamanan informasi, pengawasan internal dan akuntabilitas pengendali data pribadi. Oleh karena itu, diperlukan reformasi dalam sistem keamanan data perbankan dan pengawasan yang lebih ketat oleh OJK untuk mencegah terjadinya kebocoran data pribadi di masa mendatang (OJK, 2020).

METODE

Penelitian ini menggunakan metode penelitian hukum normatif, yaitu penelitian yang berfokus pada studi dokumen dengan mengkaji norma-norma hukum tertulis yang berlaku, seperti peraturan perundang-undangan, putusan pengadilan, kontrak, teori hukum, dan pendapat para ahli. Sumber data yang digunakan berupa data sekunder yang terdiri dari tiga jenis bahan hukum: bahan hukum primer (peraturan perundang-undangan, putusan pengadilan, dokumen resmi negara), bahan hukum sekunder (buku hukum, jurnal, doktrin ahli), dan bahan hukum tersier (kamus hukum, ensiklopedia, indeks, dan sumber internet). Teknik pengumpulan data dilakukan melalui studi pustaka, studi dokumen, dan studi arsip dengan menelusuri bahan hukum dari berbagai media tertulis dan digital. Seluruh data yang diperoleh dianalisis secara kualitatif dengan metode interpretasi hukum untuk menafsirkan dan memahami substansi hukum, mengidentifikasi kekosongan, pertentangan, atau ketidakjelasan norma hukum yang relevan dengan permasalahan yang diteliti.

HASIL DAN PEMBAHASAN

Kepastian Hukum Perlindungan Data Pribadi Berdasarkan Pasal 65 Undang-Undang No. 27 Tahun 2022

Kasus kebocoran atau penyalahgunaan data pribadi di bank mencerminkan lemahnya perlindungan data dan ketidakpatuhan terhadap regulasi yang berlaku. Kejadian ini bermula ketika seorang nasabah menerima pesan dari seseorang yang mengaku sebagai debt collector terkait tagihan kartu kredit yang tidak pernah diajukan. Awalnya, pesan tersebut dianggap sebagai penipuan dan diabaikan. Namun, ketika korban mengajukan Kredit Pemilikan Rumah (KPR) di bank lainnya, ia mendapati bahwa namanya tercatat dalam BI Checking dengan status kolektibilitas 5 akibat tunggakan kartu kredit sebesar Rp27.000.000 (dua puluh tujuh juta rupiah) sejak 2021. Hal ini mengejutkan karena ia sama sekali tidak pernah mengajukan kartu kredit, terutama dari bank (F. Manurung, Tarigan, Brahmana, & Alendra, 2023).

Menanggapi hal ini, korban mencoba menghubungi call center bank, namun jawaban yang diberikan kurang memuaskan. Ia kemudian mendatangi Kantor Cabang Bank Bagan Batu untuk meminta klarifikasi (E. A. P. Manurung & Thalib, 2022). Pihak bank mengonfirmasi bahwa memang ada tagihan tersebut dan menyampaikan bahwa mereka akan melakukan pengecekan lebih lanjut ke Kantor Pusat Bank Pekanbaru. Dalam proses ini, bank meminta berbagai dokumen seperti KTP (Kartu Tanda Penduduk), foto diri dengan KTP

(Kartu Tanda Penduduk), surat izin usaha, serta surat kronologi sebagai syarat verifikasi kepemilikan kartu kredit. Setelah dokumen diberikan, pihak bank meminta waktu untuk menyelidiki kasus ini, namun tanggapan yang diberikan terkesan lambat dan kurang transparan.

Setelah tekanan dari pihak nasabah, termasuk ancaman untuk menyebarkan kasus ini ke media sosial dan wacana menggunakan bantuan hukum, akhirnya bank mengeluarkan Surat Keterangan Lunas Sementara, yang menyatakan bahwa kewajiban kartu kredit tersebut telah diselesaikan. Namun, penghapusan nama dari BI Checking tetap memerlukan waktu satu bulan setelah surat tersebut diterbitkan. Meskipun bank memberikan solusi berupa surat tersebut, lambatnya respons dan minimnya transparansi dalam penanganan kasus ini menunjukkan masih adanya celah dalam penerapan perlindungan data pribadi sesuai dengan UU PDP (Mochtar, 2023).

Pasal 65 UU PDP menegaskan tanggung jawab penyelenggara data dalam melindungi data pribadi yang berada di bawah penguasaannya. Dalam konteks kebocoran atau penyalahgunaan data, pasal ini memberikan landasan hukum yang mengatur hak-hak subjek data pribadi, kewajiban pengendali data, serta mekanisme pengawasan dan penegakan hukum untuk memastikan perlindungan data pribadi secara memadai.

Undang-Undang ini memberikan jaminan bahwa setiap pengendali data pribadi wajib menjaga keamanan data untuk mencegah akses ilegal, manipulasi, atau pencurian data (Ardini, 2022). Apabila terjadi kebocoran data, pengendali data wajib segera memberitahukan subjek data dalam waktu 72 jam sejak kebocoran diketahui. Dalam kasus kebocoran data yang dialami oleh nasabah bank, terdapat indikasi pelanggaran kewajiban tersebut karena pihak bank tidak segera memberikan pemberitahuan maupun solusi konkret atas kebocoran yang terjadi.

Pasal 65 juga menegaskan bahwa subjek data pribadi memiliki hak untuk mendapatkan akses, perbaikan, atau penghapusan data pribadi yang telah disalahgunakan. Dalam kasus ini, korban sebagai subjek data berhak menuntut penghapusan nama dari BI Checking yang diakibatkan oleh penyalahgunaan data. Hal ini tidak hanya bertujuan untuk memulihkan nama baik subjek data, tetapi juga untuk mengembalikan kepercayaan masyarakat terhadap institusi pengelola data pribadi. Selanjutnya, UU PDP menekankan kewajiban pengendali data untuk mengelola data secara transparan dan akuntabel. Keterlambatan atau pengabaian pihak bank dalam menanggapi aduan nasabah, seperti yang dialami dalam kasus ini, mencerminkan lemahnya akuntabilitas pengelola data. Hal ini menjadi perhatian serius karena menunjukkan adanya potensi pelanggaran terhadap prinsip-prinsip pengelolaan data yang diatur dalam Pasal 65 UU PDP.

Selain itu, undang-undang ini memberikan perlindungan hukum terhadap subjek data dengan adanya sanksi administratif maupun pidana bagi pelanggaran yang dilakukan oleh pengendali data. Dalam kasus ini, apabila terbukti terjadi kelalaian atau pelanggaran dalam pengelolaan data pribadi, subjek data berhak untuk mengajukan gugatan melalui jalur hukum atau melibatkan lembaga terkait seperti Otoritas Jasa Keuangan (OJK). Tindakan ini bertujuan untuk memberikan efek jera kepada pihak yang lalai.

Pasal 65 UU PDP juga menegaskan bahwasanya perlindungan data merupakan salah satu bagian terpenting dalam hak asasi manusia. Dalam kasus ini, pelanggaran perlindungan data tidak hanya berdampak pada kerugian finansial, tetapi juga psikologis bagi subjek data. Hal ini menyoroti urgensi implementasi UU PDP yang efektif dan tegas untuk memastikan tidak ada institusi yang dapat mengabaikan kewajibannya dalam menjaga data pribadi masyarakat (E. F. Pakpahan, Chandra, & Tanjaya, 2020).

Secara keseluruhan, kepastian hukum perlindungan data pribadi berdasarkan Pasal 65 UU PDP menekankan tanggung jawab pengendali data, hak-hak subjek data, dan mekanisme penegakan hukum yang jelas. Namun, dalam praktiknya, seperti yang terlihat dalam kasus kebocoran data di bank, masih terdapat celah dalam penerapan undang-undang ini. Oleh

karena itu, diperlukan penguatan pengawasan dan penegakan hukum yang lebih ketat agar tujuan dari UU PDP dapat tercapai secara maksimal.

Dengan demikian, hasil penelitian menunjukkan bahwa harusnya mengenai perihal perlindungan data pribadi yang ada di Indonesia, sebagaimana tertulis dan diatur dalam Pasal 65 UU PDP, masih menghadapi tantangan besar dalam implementasinya. Kasus kebocoran data pada Bank menjadi contoh nyata di mana prinsip-prinsip perlindungan data, seperti transparansi, akuntabilitas, dan kewajiban pemberitahuan, belum sepenuhnya diterapkan secara efektif.

Studi ini mengungkapkan bahwa hak-hak subjek data, seperti hak atas pemberitahuan kebocoran data, hak untuk mengajukan keberatan, dan hak untuk penghapusan data yang disalahgunakan, sering kali tidak dipenuhi dengan baik oleh pengendali data. Selain itu, lambannya penanganan kasus oleh pihak terkait menunjukkan adanya kelemahan dalam sistem pengawasan dan mekanisme penegakan hukum yang seharusnya memberikan perlindungan yang lebih tegas kepada subjek data (Raineven, 2023).

Fakta bahwa korban dalam kasus ini mengalami kerugian finansial, psikologis, dan reputasi juga menunjukkan kurangnya perlindungan preventif dalam pengelolaan data pribadi. Hal ini menjadi bukti bahwa pengendali data, seperti institusi perbankan, belum menjalankan tanggung jawabnya secara optimal dalam memastikan keamanan data yang dipercayakan oleh masyarakat.

Penelitian ini juga menegaskan pentingnya penguatan penerapan UU PDP melalui pengawasan yang lebih ketat, peningkatan kapasitas pengendali data, erta melalui edukasi terstruktur terhadap publik terkait hak yang harusnya mereka dapat atas data pribadi mereka. Di sisi lain, sanksi yang lebih tegas terhadap pelanggaran perlu diterapkan untuk menciptakan efek jera dan meningkatkan kepatuhan terhadap regulasi yang ada.

Dengan adanya UU PDP, diharapkan kepastian hukum perlindungan data pribadi dapat terwujud secara efektif di masa depan. Namun, untuk mencapai hal tersebut, diperlukan komitmen yang kuat dari semua pihak, termasuk pengendali data, pemerintah, dan masyarakat, agar kasus serupa tidak terulang kembali. Hasil penelitian ini memberikan kontribusi penting untuk meningkatkan kesadaran akan urgensi mengenai perlindungan data pribadi yang merupakan salah satu bagian dalam hak asasi manusia.

Upaya Hukum untuk Menjamin Perlindungan Data Pribadi Nasabah Dalam kasus kebocoran data di Bank Rakyat Indonesia (BRI)

Perlindungan data pribadi merupakan aspek krusial dalam era digital, terutama dalam sektor perbankan yang menyimpan informasi sensitif milik nasabah. Keamanan data menjadi perhatian utama mengingat banyaknya kasus kebocoran data yang dapat menyebabkan kerugian finansial, pencurian identitas, dan penurunan kepercayaan masyarakat terhadap institusi keuangan. Pemerintah Indonesia telah mengesahkan UU PDP sebagai landasan hukum dalam mengatur kewajiban pengendali data serta hak-hak subjek data agar terhindar dari penyalahgunaan informasi pribadi mereka.

Dalam konteks hukum, upaya perlindungan data pribadi melibatkan berbagai mekanisme seperti kewajiban pengendali data untuk menjaga keamanan informasi, pemberian hak kepada subjek data untuk mengakses dan mengontrol datanya, serta adanya sanksi administratif maupun pidana bagi pelanggar. UU PDP mewajibkan pengendali data untuk segera melaporkan kebocoran dalam waktu 72 jam dan memberikan solusi konkret kepada subjek data yang terdampak. Namun, dalam praktiknya, banyak kasus menunjukkan bahwa implementasi perlindungan data masih lemah, dengan banyaknya pelanggaran yang tidak ditindak secara tegas (Keliat, Siregar, Zulkifli, & Purba, 2023).

Salah satu kasus yang mencerminkan lemahnya perlindungan data pribadi adalah kebocoran data nasabah di Bank. Kasus ini berawal dari dugaan penggunaan data nasabah tanpa izin, yang berakibat pada pencatatan kredit fiktif dalam sistem BI Checking. Akibatnya,

nasabah mengalami kesulitan dalam mengakses layanan keuangan akibat reputasi kredit yang tercemar. Dalam menghadapi kasus seperti ini, nasabah memiliki berbagai upaya hukum yang dapat ditempuh, baik melalui jalur administratif, perdata, maupun pidana, guna memastikan perlindungan hak-haknya serta berdampak signifikan kepada pihak yang bertanggung jawab (M. E. Pakpahan, Zulkifli, & Sunarto, 2022).

Perlindungan data pribadi nasabah merupakan aspek krusial dalam menjaga kepercayaan publik terhadap institusi perbankan. Untuk menjamin perlindungan data tersebut, UU PDP menjadi landasan hukum utama. Undang-undang ini mewajibkan pengendali data, termasuk bank, untuk melindungi data pribadi nasabah dari kebocoran, akses tidak sah, atau penyalahgunaan. Dalam kasus kebocoran data, pengendali data wajib memberikan pemberitahuan kepada nasabah dalam waktu 72 jam dan menyelesaikan permasalahan secara cepat dan akuntabel.

Langkah hukum yang dapat diambil nasabah mencakup pengaduan ke lembaga terkait, seperti Otoritas Jasa Keuangan (OJK). OJK memiliki peran penting dalam mengawasi kepatuhan bank terhadap regulasi perlindungan data. Apabila nasabah merasa dirugikan, mereka dapat melaporkan pelanggaran ini untuk mendorong investigasi dan penerapan sanksi administratif terhadap bank yang melanggar. Selain itu, nasabah juga memiliki hak untuk mengajukan gugatan perdata guna mendapatkan ganti rugi atas kerugian yang dialami akibat penyalahgunaan data.

Mekanisme penyelesaian sengketa melalui mediasi atau arbitrase juga dapat menjadi alternatif bagi nasabah untuk mendapatkan keadilan. Proses ini biasanya melibatkan negosiasi antara nasabah dan bank dengan bantuan pihak ketiga yang netral. Jika penyelesaian ini tidak membuahkan hasil, nasabah dapat mengajukan gugatan ke pengadilan berdasarkan UU PDP maupun aturan perlindungan konsumen.

Dalam konteks pidana, UU PDP memberikan sanksi tegas bagi pihak yang secara sengaja atau lalai menyebabkan kebocoran data pribadi. Nasabah yang menjadi korban dapat melaporkan kasus ini ke pihak kepolisian untuk dilakukan penyidikan lebih lanjut. Sanksi pidana terhadap pelaku pelanggaran bertujuan memberikan efek jera dan memperkuat kepatuhan terhadap regulasi perlindungan data.

Upaya hukum ini harus diimbangi dengan penguatan sistem pengawasan dan regulasi oleh pemerintah, termasuk penerapan teknologi keamanan data yang lebih canggih oleh institusi keuangan. Edukasi kepada nasabah tentang hak-hak mereka juga penting untuk mendorong kesadaran akan perlindungan data pribadi. Dengan kombinasi langkah-langkah hukum dan preventif ini, perlindungan data nasabah dapat dijamin secara lebih efektif (Keliat, 2024).

Kasus kebocoran data yang dialami oleh nasabah Bank, sebagaimana dijelaskan dalam kronologis, menunjukkan adanya kelemahan dalam perlindungan data pribadi yang seharusnya dijamin oleh pengendali data sesuai dengan UU PDP. Dalam kasus ini, data pribadi nasabah digunakan untuk pengajuan kartu kredit secara ilegal tanpa sepengetahuan atau persetujuan yang bersangkutan. Pelanggaran ini mencerminkan kurangnya penerapan prinsip keamanan data dan kewajiban akuntabilitas oleh pihak bank dalam melindungi data pribadi nasabah.

Sebagai upaya hukum, nasabah memiliki hak untuk melaporkan kejadian tersebut kepada Otoritas Jasa Keuangan (OJK) sebagai pengawas sektor perbankan dan lembaga lain yang berwenang menangani pelanggaran data pribadi, seperti Komisi Informasi atau bahkan pihak kepolisian untuk proses hukum pidana. Dalam hal ini, Bank sebagai pengendali data wajib memberikan penjelasan transparan, menyelesaikan masalah secara tuntas, dan memberikan ganti rugi kepada nasabah yang dirugikan. Selain itu, nasabah bisa melakukan aju gugatan dalam bentuk perdata untuk mendapatkan ganti rugi atas keruskan material maupun immaterial yang dialami akibat pencemaran nama baik di BI Checking.

Kasus ini juga menyoroti pentingnya penerapan teknologi keamanan data yang lebih baik dan komitmen institusi keuangan dalam melindungi data pribadi nasabah. Dalam perspektif UU PDP, Bank memiliki tanggung jawab untuk memberikan pemberitahuan dalam waktu 72 jam terkait kebocoran data dan menyelesaikan permasalahan secara cepat. Namun, lambannya respons dari pihak Bank menunjukkan kurangnya mekanisme penanganan yang efektif. Oleh karena itu, kasus ini menjadi momentum untuk memperkuat pengawasan dan kepatuhan terhadap regulasi perlindungan data pribadi di sektor perbankan.

Hasil penelitian menunjukkan bahwa perlindungan data pribadi nasabah di sektor perbankan, seperti dalam kasus kebocoran data di Bank, masih menghadapi berbagai tantangan signifikan. Salah satu temuan utama adalah adanya kelemahan dalam mekanisme pengamanan data dan minimnya transparansi serta respons cepat dari pihak bank ketika terjadi pelanggaran. Hal ini terlihat dari lambannya penyelesaian kasus, kurangnya pemberitahuan sesuai waktu yang diatur dalam UU PDP, dan kurangnya penanganan yang memadai terhadap keluhan nasabah.

Selain itu, penelitian ini mengungkapkan bahwa pemahaman nasabah terhadap hak-hak mereka dalam perlindungan data pribadi masih terbatas. Hal ini menyebabkan nasabah kurang proaktif dalam menuntut keadilan atau melaporkan kasus kebocoran data ke lembaga yang berwenang, seperti Otoritas Jasa Keuangan (OJK). Dalam kasus ini, meskipun nasabah telah mendesak penyelesaian masalah secara intensif, pihak bank tampaknya tidak memiliki sistem yang efektif untuk merespons dan menindaklanjuti keluhan secara cepat dan akurat.

Secara keseluruhan, hasil penelitian menyoroti perlunya peningkatan sistem pengamanan data, implementasi teknologi perlindungan data yang lebih canggih, serta pengawasan yang lebih ketat oleh regulator. Penelitian ini juga menunjukkan bahwa perlindungan data pribadi harus menjadi prioritas utama di sektor perbankan untuk menjaga kepercayaan nasabah dan mematuhi ketentuan hukum yang berlaku. Kasus Bank ini menjadi pelajaran penting untuk meningkatkan kesadaran dan tanggung jawab baik di pihak bank maupun nasabah dalam melindungi data pribadi.

Dampak Kebocoran Data Pribadi Terhadap Korban dari Segi Finansial, Psikologis dan Sosial

Berdasarkan Pasal 65 Undang-Undang No.27 Tahun 2022 Tentang Perlindungan Data Pribadi, perusahaan termasuk bank dan penyedia layanan fintech sebagai pengendali data pribadi berbentuk korporasi, memiliki kewajiban untuk menjaga dan melindungi data-data tersebut. Maka kebocoran data yang terjadi, apapun penyebabnya sudah seharusnya menjadi tanggung jawab perusahaan. Dengan terjadinya kebocoran data pribadi pada korban menunjukkan bahwa bank gagal dan melakukan pelanggaran terhadap kewajibannya dalam hal menjaga kerahasiaan dan keamanan pemilik data pribadi tersebut. Terjadinya insiden kebocoran data merupakan bukti kelemahan dalam sistem keamanan, pengawasan, penyimpanan dan pengelolaan keamanan informasi data (Edbert & Putra, 2023).

Kebocoran data pribadi akan memberikan dampak yang signifikan bagi banyak individu yang data pribadinya telah tersebar. Selain gangguan privasi, mereka dapat menjadi sasaran kejahatan siber, seperti pemalsuan, penipuan, pemerasan, atau doxing, yang merupakan tindakan membongkar serta menyebarluaskan informasi target oleh pihak yang tidak berwenang (Hisbulloh, 2021).

Dengan perkembangan zaman yang sangat pesat, saat ini perbankan sudah mengadopsi sistem digital, tentu hal ini mempermudah nasabah yang akan melakukan berbagai kegiatan perbankan, seperti pembukaan rekening dan transaksi keuangan digital tanpa harus datang secara fisik ke kantor cabang. Tetapi dengan mudahnya melakukan kegiatan digital juga menjadi pedang bermata dua bagi nasabah, karena hal tersebut mempermudah bocornya data pribadi nasabah karena kurangnya edukasi akan bahaya dan pentingnya dalam menjaga data pribadi dan lemahnya sistem keamanan bank.

Otoritas Jasa Keuangan (OJK) adalah lembaga yang dipercaya untuk menjaga keamanan nasabah dalam bertransaksi di seluruh lembaga keuangan yang terdaftar di bawahnya. Terdaftar di OJK memastikan bahwa lembaga keuangan tersebut sudah memiliki legalitas yang sah di bawah hukum. Oleh karena itu, guna mencegah terjadinya penipuan dalam transaksi keuangan, selalu pastikan bahwa lembaga keuangan seperti perbankan yang akan digunakan sudah sah dan terdaftar di OJK.

Dengan maraknya kebocoran data pribadi yang terjadi seiring berkembangnya zaman menjadikan lembaga keuangan seperti perbankan harus selalu meningkatkan keamanan sistem teknologi informasinya dari waktu ke waktu dalam menjaga data-data penting nasabahnya, antara lain bank dapat menggunakan beberapa cara:

1. Menggunakan dan Meningkatkan Sistem Otentikasi Ganda (*Multi-Factor Authentication*) implementasi dua atau lebih langkah agar akses ke data sensitif dapat terlindungi secara maksimal.
2. Meningkatkan Keamanan Jaringan dengan cara menggunakan *firewall* canggih dan perangkat lunak anti *malware.*
3. Pemantauan real-time 24/7 berbasis AI untuk memantau dan mencegah adanya kegiatan mencurigakan (Irsyad, Siregar, Marbun, & Hasyim, 2024).

Tetapi kasus bocornya data pribadi yang terjadi kepada korban, dapat disimpulkan bahwa sistem keamanan pihak bank tidak cukup ketat. Hal ini tentu mengakibatkan hilangnya rasa percaya nasabah yang sebelumnya memiliki kepercayaan kepada bank sebagai lembaga keuangan yang seharusnya dapat menjaga data-data pribadinya. Berdasarkan Pasal 65 UU PDP, bank sebagai pengendali data pribadi telah gagal melaksanakan kewajibannya dalam menjaga kerahasiaan dan keamanan data pribadi nasabah dan berdampak negatif bagi korban yang dapat dikategorikan ke dalam tiga aspek utama, yaitu finansial, psikologis dan sosial:

a. Dampak Finansial

   Kebocoran data pribadi seperti informasi nomor rekening bank, data kartu kredit, atau informasi keuangan lainnya sering kali merugikan korban secara finansial yang sangat signifikan (Sugiarto, Lie, & Putra, 2024). Beberapa bentuk kerugian finansial yang terjadi kepada nasabah antara lain:

   1) Tercatat Sebagai Nasabah Dengan Kolektibillitas Yang Buruk (Coll 5)
      Nama korban tercatat dalam Sistem Layanan Informasi Keuangan (SLIK) Otoritas Jasa Keuangan (OJK) sebagai debitur yang bermasalah akibat tunggakan kartu kredit sebesar Rp27.000.000 (dua puluh tujuh juta rupiah) yang tidak pernah diajukan. Ini berdampak negatif kepada korban karena akan kesulitan dalam mengakses layanan keuangan lainnya, seperti pengajuan Kredit Kepemilikan Rumah (KPR) yang ditolak.
   2) Kesulitan Mendapatkan Pinjaman atau Kredit di Masa Depan Karena nama korban sudah masuk ke dalam daftar hitam BI Checking (Coll 5), korban akan kesulitan untuk mengajukan KPR, Kredit Kendaraan atau Pinjaman lainnya karena akan dianggap beresiko dengan adanya riwayat buruk yang dapat mempengaruhi penilaian perbankan di masa mendatang.
   3) Potensi Kewajiban Membayar Tagihan Yang Tidak Sah
      Meskipun korban tidak pernah mengajukan kartu kredit, bank awalnya menganggap bahwa tagihan tersebut sah. Jika tidak adanya langkah hukum yang tepat, korban bisa saja terpaksa untuk membayar tagihan utang yang bukan miliknya.
   4) Biaya Tambahan Untuk Penyelesaian Kasus
      Untuk menghapus catatan buruk dalam BI Checking, korban mungkin perlu mengeluarkan biaya tambahan seperti untuk konsultasi hukum atau bahkan menyewa jasa pengacara jika kasus ini tidak kunjung selesai.
   5) Kerugian Akibat Penundaan Transaksi Keuangan

Karena masalah ini, rencana korban untuk mengajukan KPR harus tertunda dan jika korban membutuhkan dana cepat untuk investasi atau kebutuhan lain, maka penundaan ini bisa menyebabkan peluang finansial yang hilang.

b. Dampak Psikologis

Kebocoran data pribadi tidak hanya berdampak pada aspek finansial, tetapi juga menyebabkan tekanan mental yang cukup besar bagi korban. Beberapa dampak psikologis yang di alami oleh korban:

1) Stres dan Frustasi
Korban harus menghadapi penagihan dari pihak bank yang tidak dikenal, tanpa mengetahui bagaimana data pribadinya bisa disalahgunakan. Ketidakjelasan penyelesaian kasus oleh bank juga memperburuk kondisi emosionalnya.
2) Kemarahan dan Rasa Tidak Berdaya
Ketika korban mencoba untuk menghubungi pihak bank untuk melakukan klarifikasi, ia mendapatkan respons yang lambat dan berbelit-belit. Hal ini tentu menyebabkan frustrasi dan kemarahan karena seolah-olah pihak bank tidak serius dalam menanggapi masalah ini.
3) Kecemasan dan Ketidakpastian
Ketidakjelasan dalam penyelesaian masalah dan ketakutan akan memberikan dampak jangka panjang (misalnya, kesulitan dalam mengakses dalam mengakses layanan keuangan) menyebabkan kecemasan yang berkepanjangan. Apalagi, pihak bank terus meminta waktu tambahan tanpa kepastian penyelesaian.
4) Trauma Terhadap Layanan Perbankan dan Keuangan
Setelah mengalami kejadian ini, korban bisa menjadi lebih takut untuk berinteraksi dengan bank atau lembaga keuangan lainnya. Korban juga dapat mengalami perasaan takut yang menyebabkan korban cenderung menghindari penggunaan kartu kredit atau layanan pinjaman.
5) Gangguan Tidur dan Kesehatan Mental
Gangguan tidur (Insomnia) dapat terjadi kepada korban karena terus-menerus memikirkan masalah ini, terutama jika terus mendapat tekanan dan tagihan dari *debt collector* atau pihak bank.

c. Dampak Sosial

Dampak sosial dari kebocoran data pribadi sering kali diabaikan, tetapi dalam beberapa kasus, efeknya bisa sangat merugikan korban. Beberapa dampak sosial yang dialami oleh korban meliputi:

1) Penurunan Kepercayaan terhadap Lembaga Keuangan
Setelah mengalami kasus ini, korban merasa bahwa bank tidak memiliki sistem keamanan yang baik dan tidak peduli terhadap perlindungan akan data nasabah. Hal ini bisa berdampak pada keengganan menggunakan layanan perbankan di masa depan (Sugiarto et al., 2024).
2) Stigma Negatif di Lingkungan Sosial
Nama korban yang tercatat dalam daftar hitam perbankan dapat menimbulkan stigma negatif. Terutama jika ada pihak yang lain yang mengetahui status kreditnya. Ini dapat mempengaruhi interaksi sosial dan kepercayaan dalam lingkungan kerja atau bisnis.
3) Gangguan dalam Aktivitas Sehari-hari
Korban harus menghabiskan waktu yang cukup lama untuk menyelesaikan kasus ini, mulai dari menghubungi call center, mendatangi bank, hingga berusaha mendapatkan kejelasan dari pihak terkait. Hal ini tentu sangat mengganggu aktivitas sehari-hari dan menurunkan produktivitas.
4) Dampak Terhadap Kehidupan Profesional

Jika informasi mengenai hutang fiktif ini tersebar, bisa berdampak buruk pada reputasi profesional korban. Jika korban memiliki bisnis atau usaha sendiri, maka kepercayaan pelanggan atau mitra bisnis bisa menurun karena melihat adanya masalah keuangan yang terkait dengan namanya.

5) Isolasi Sosial
Jika kasus ini tersebar luas, dapat muncul stigma dari teman atau rekan kerja yang menganggap korban sebagai orang yang tidak bisa mengelola keuangan dengan baik, meskipun sebenarnya ia adalah korban dari pencurian identitas. Bahkan korban bisa merasa malu untuk menceritakan kejadian ini baik kepada teman atau keluarganya yang bisa membuat dirinya semakin terisolasi.

Kasus kebocoran data pribadi yang berujung pada penyalahgunaan kartu kredit bukan hanya sekedar masalah administratif, tetapi memiliki dampak yang luas terhadap korban. Dari segi finansial, korban dapat mengalami kesulitan ekonomi akibat pencatatan buruk dalam sistem perbankan. Dari segi psikologis, korban mengalami stres, kecemasan dan frustrasi akibat ketidakpastian penyelesaian kasus. Sementara itu, dari segi sosial, korban bisa kehilangan kepercayaan terhadap sistem keuangan dan mengalami dampak negatif dalam lingkungannya. Oleh karena itu, perlindungan data pribadi harus menjadi perhatian serius bagi lembaga keuangan untuk mencegah kasus serupa terjadi di masa depan.

Kasus kebocoran data pribadi yang terjadi terhadap korban menunjukkan vulnerabilitas data pribadi nasabah dalam sistem perbankan, terutama ketika sistem keamanan informasi dan pengawasan oleh internal bank tidak cukup memadai. Dalam era digital yang semakin canggih, nasabah perlu lebih proaktif dalam melindungi data pribadinya agar tidak disalahgunakan oleh pihak yang tidak bertanggung jawab. Sebagai pengguna layanan keuangan, nasabah dapat melakukan beberapa langkah pencegahan yang bisa dilakukan untuk menghindari kasus serupa seperti:

a) Mengamankan Informasi Pribadi Secara Digital dan Fisik
Dengan cara tidak membagikan informasi pribadi seperti nomor KTP (Kartu Tanda Penduduk), NPWP (Nomor Pokok Wajib Pajak), nomor rekening, atau informasi keuangan lainnya melalui media sosial atau platform yang tidak aman. Jangan pernah membagikan kode OTP (One Time Password), PIN (*Personal Identification Number*), atau kata sandi kepada siapapun, termasuk kepada pihak yang mengaku sebagai pegawai bank (Junaedi, 2017). Simpan dokumen-dokumen penting seperti KTP (Kartu Tanda Penduduk), Kartu Keluarga, buku tabungan, kartu kredit di tempat yang aman, seperti brankas dan jangan pernah mengakses layanan perbankan online atau melakukan transaksi keuangan mengunnakan Wifi publik karena sangat rentan terhadap peretasan (*hacking*).

b) Meningkatkan Keamanan Akun Digital dan Perbankan Online
Gunakan kata sandi (*password*) yang kuat dan unik, dengan kombinasi huruf besar, huruf kecil, angka dan simbol khusus. Jangan pernah menggunakan satu kata sandi yang sama untuk akun perbankan dan akun media sosial lainnya, rutin mengganti kata sandi setiap 3-6 bulan untuk memgurangi resiko peretasan (*hacking*). Mengaktifkan notifikasi transaksi secara *real-time* untuk semua transaksi perbankan, sehingga nasabah dapat segera mengetahui jika ada transaksi mencurigakan dan jika menerima notifikasi transaksi yang tidak diketahui, segera hubungi call center resmi bank dan blokir kartu kredit atau rekening yang terindikasi disalahgunakan.

c) Rutin Memeriksa Data Keuangan
Melakukan pengecekan BI Checking atau SLIK OJK (Sistem Layanan Informasi Keuangan OJK) secara berkala untuk memastikan tidak ada pinjaman atau kartu kredit fiktif yang terdaftar atas nama nasabah, pengecekan SLIK OJK dapat dilakukan secara gratis melalui situs resmi OJK atau di kantor OJK terdekat (Sunarto, Natal, Adnan, & Noor, 2023). Rutin memeriksa mutasi rekening dan laporan transaksi kartu kredit untuk

mendeteksi transaksi yang mencurigakan, jika menemukan adanya transaksi yang janggal dan mencurigakan segera laporkan kepada pihak bank agar kartu kredit atau rekening nasabah dapat segera di blokir dan dilakukan investigasi lebih lanjut.

d) Meningkatkan Edukasi dan Kesadaran Akan Pentingnya Keamanan Data Pribadi
Meningkatkan kesadaran tentang *phising* dan penipuan digital dengan cara selalu waspada terhadap *phising* (penipuan digital) melalui email, SMS (*Short Message Service*), atau telepon yang mengaku sebagai pihak bank maupun petugas pajak dengan meminta data pribadi. Jangan mengklik link mencurigakan yang mengaku berasal dari bank atau lembaga keuangan lainnya dan pelajari tips-tips aman dalam bertransaksi secara digital yang sering diberikan oleh OJK dan Kominfo.

e) Segera Melaporkan Jika Kebocoran Data Terjadi
Laporkan ke bank dan OJK jika mengalami kebocoran data pribadi atau penyalahgunaan kartu kredit, segera hubungi call center resmi bank untuk meminta pemblokiran rekening atau kartu kredit. Nasabah juga dapat melaporkan kasus ini kepada OJK melalui Aplikasi Portal Perlindungan Konsumen (AAPK) untuk mendapatkan perlindungan hukum dan investigasi lebih lanjut. Jika tidak adanya penyelesaian yang memuaskan dari pihak bank, nasabah dapat mengajukan sengketa melalui LAPS Sektor Jasa Keuangan (LAPS SJK) sebagai mediator untuk menyelesaikan sengketa perbankan tanpa harus melalui pengadilan. Berdasarkan Pasal 65 UU PDP, pengendali data yang dalam hal ini adalah bank wajib memberitahukan kebocoran data dalam waktu 3x24 jam. Jika bank tidak melakukannya, nasabah dapat melaporkan kasus ini ke Kementrian Kominfo untuk tindakan lebih lanjut.
Kasus kebocoran data yang terjadi pada korban menunjukkan pentingnya kewaspadaan nasabah dalam melindungi data pribadinya. Selain meningkatkan keamanan informasi oleh pengendali data (bank), nasabah juga harus proaktif dalam menjaga keamanan data pribadinya, baik secara digital maupun fisik. Dan dengan menerapkan langkah-langkah pencegahan yang komprehensif, nasabah dapat meminimalisir resiko kebocoran data pribadi dan melindungi diri dari penyalahgunaan identitas atau kejahatan siber di masa depan.

KESIMPULAN

Berdasarkan Pasal 65 Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), bank sebagai pengendali data memiliki kewajiban untuk menjaga keamanan data pribadi nasabah dan bertanggung jawab apabila terjadi kebocoran data. Namun, kasus kebocoran data yang dialami oleh korban menunjukkan adanya kegagalan dalam implementasi UU PDP. UU PDP telah memberikan kepastian hukum mengenai perlindungan data pribadi, penerapannya di sektor perbankan masih lemah. Oleh karena itu, diperlukan reformasi kebijakan, pengawasan yang lebih ketat, serta peningkatan kesadaran hukum untuk memastikan bahwa hak-hak subjek data benar-benar terlindungi dan kebocoran data dapat dicegah di masa mendatang.

Nasabah yang mengalami kebocoran data memiliki hak dan dapat melakukan upaya hukum dengan cara mengajukan pengaduan ke Otoritas Jasa Keuangan (OJK) jika pihak bank tidak memberikan solusi yang memadai. Selain itu, nasabah juga dapat menempuh jalur perdata untuk meminta ganti rugi atas kerugian finansial maupun kerugian non-finansial yang dialami. Dalam kasus yang lebih serius, laporan kepada Kementerian Komunikasi dan Informatika (Kominfo) serta kepolisian dapat menjadi langkah untuk menindaklanjuti kelalaian bank secara hukum.

Kebocoran data pribadi mengakibatkan dampak negatif terhadap korban dari segi finansial, psikologis dan sosial. Dari segi finansial, korban mengalami kerugian berupa status kolektibilitas (Coll 5) dalam BI Checking akibat penggunaan data secara ilegal, kesulitan mendapatkan pinjaman dimasa depan, serta potensi kewajiban membayar utang yang tidak

sah. Dari segi psikologis, korban mengalami stres, kecemasan berlebihan dan trauma akibat tekanan dari bank dan ketidakpastian penyelesaian masalah dan dari segi sosial, kasus ini berdampak pada hilangnya kepercayaan terhadap bank, munculnya stigma negatif dalam lingkungan sosial, serta gangguan dalam kehidupan profesional korban.

REFERENSI

Ardini, A. (2022). Legal Construction For The Obligors Of The Bank Of Indonesia Liquidity Assistance Funds (Blbi) In Returning State Assets That Guarantee Legal Certainty And Justice. *Journal of World Science*, *1*(8), 592–603.

Edbert, F., & Putra, M. R. S. (2023). Pertanggungjawaban Hukum Terhadap Kebocoran Data Pribadi pada Perusahaan Pengelola Jasa Keuangan Berbasis IT. *Unes Law Review*, *6*(2), 5966–5977.

Hisbulloh, M. H. (2021). Urgensi rancangan undang-undang (RUU) perlindungan data pribadi. *Jurnal Hukum*, *37*(2), 119–133.

Irmawati, E. (2023). *Perlindungan Hukum atas Kebocoran Data Pribadi Nasabah Bank Pengguna Mobile Banking dalam Perspektif Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi*. Universitas Kristen Indonesia.

Irsyad, F. R., Siregar, F. A., Marbun, J., & Hasyim, H. (2024). Menghadapi Era Baru: Strategi Perbankan Dalam Menghadapi Perubahan Pasar Dan Teknologi Di Indonesia. *Transformasi: Journal Of Economics And Business Management*, *3*(2), 29–46.

Iswandari, B. A. (2021). Jaminan Atas Pemenuhan Hak Keamanan Data Pribadi Dalam Penyelenggaraan E-Government Guna Mewujudkan Good Governance. *Jurnal Hukum Ius Quia Iustum*, *28*(1), 115–138.

Junaedi, D. I. (2017). Antisipasi Dampak Social Engineering Pada Bisnis Perbankan. *Infoman's: Jurnal Ilmu-Ilmu Informatika Dan Manajemen*, *11*(1), 1–10.

Keliat, V. U. (2024). Peran Regulasi Terkini Dalam Mengatasi Tantangan Hukum Perbankan Di Era Digital. *Jurnal Darma Agung*, *32*(1), 323–331.

Keliat, V. U., Siregar, A. P., Zulkifli, S., & Purba, I. (2023). Analisis Upaya Dan Peran Perlindungan Hukum Terhadap Kasus Peretasan Data Bank Syariah Indonesia. *Ilmu Hukum Prima (IHP)*, *6*(2), 182–190.

Leonard, T., Sitompul, N., Tanjaya, W., & Esther, J. (2023). PERLINDUNGAN HUKUM TERHADAP PIHAK KREDITUR AKIBAT RISIKO KREDIT DALAM TRANSAKSI FINTECHT BERBASIS P2P LENDING. *UNES Law Review*, *5*(4), 3089–3096.

Manurung, E. A. P., & Thalib, E. F. (2022). Tinjauan yuridis perlindungan data pribadi berdasarkan UU nomor 27 tahun 2022. *Jurnal Hukum Saraswati*, *4*(2), 139–148.

Manurung, F., Tarigan, A. D. W., Brahmana, H., & Alendra, A. (2023). KEDUDUKAN BANK INDONESIA CHECKING SEBAGAI ALAT BUKTI DALAM PERKARA KEPAILITAN DI PENGADILAN. *JURNAL RECTUM: Tinjauan Yuridis Penanganan Tindak Pidana*, *5*(1), 289–305.

Mochtar, M. B. (2023). Kepastian Hukum Atas Kebocoran Data Pribadi Pengguna Aplikasi Online. *YUSTISIA MERDEKA: Jurnal Ilmiah Hukum*, *9*(2), 1–12.

OJK, P. (2020). dalam Mengawasi Maraknya Pelayanan Financial Technology (Fintech) di Indonesia. *Jurnal Magister Hukum Udayana (Udayana Master Law Journal)*, *9*(3), 559–574.

Pakpahan, E. F., Chandra, K., & Tanjaya, A. (2020). Urgensi Pengaturan Financial Technology di Indonesia. *Jurnal Darma Agung*, *28*(3), 444–456.

Pakpahan, E. F., Chandra, L. R., & Dewa, A. A. (2020). Perlindungan Hukum Terhadap Data Pribadi Dalam Industri Financial Technology. *Veritas et Justitia*, *6*(2), 298–323.

Pakpahan, M. E., Zulkifli, S., & Sunarto, A. (2022). Perlindungan hukum pemberian kredit secara digitalisasi kepada debitur masa perkembangan financial technology (Fintech). *JURNAL RECTUM: Tinjauan Yuridis Penanganan Tindak Pidana*, *5*(1), 120–137.

Raineven, S. V. C. (2023). *PERLINDUNGAN HUKUM BAGI KONSUMEN YANG MENGALAMI KEBOCORAN DATA BERDASARKAN UNDANG-UNDANG NOMOR 27 TAHUN 2022 TENTANG PELINDUNGAN DATA PRIBADI DI INDONESIA*.

Sugiarto, A. J., Lie, G., & Putra, M. R. S. (2024). Perlindungan Kepada Nasabah Bank Terhadap Kebocoran Data (Studi Kasus Kebocoran Data pada Bank Indonesia). *Journal of Accounting Law Communication and Technology*, *2*(1), 107–114.

Sunarto, A., Natal, I. P., Adnan, M. A., & Noor, T. (2023). Perlindungan Konsumen Dalam Industri "Peer To Peer Lending" di Indonesia. *Jurnal Darma Agung*, *31*(4), 876–887.