(2025), 3 (3): 595-606 Kultura 2985-5624
Jurnal Ilmu Hukum, Sosial, dan Humaniora

KEAMANAN DATA PRIBADI DI BANK: ANALISIS KEBOCORAN DATA PADA SISTEM PERBANKAN INDONESIA

Albert Hadi Putra [1], Sidi Ahyar Wiraguna [2]
Fakultas Ilmu Hukum Universitas Esa Unggul, Indonesia

Correspondence		
Email: alberthadiputra@gmail.com	No. Telp:	
Submitted 1 Agustus 2025	Accepted 4 Agustus 2025	Published 5 Agustus 2025

ABSTRAK

Sektor perbankan berperan krusial sebagai pengendali data pribadi nasabah di era digital, namun dihadapkan pada meningkatnya risiko kebocoran data seiring digitalisasi layanan. Insiden kebocoran data pada Bank Indonesia dan Bank Syariah Indonesia menyoroti urgensi penguatan keamanan data. Penelitian ini bertujuan menganalisis sistem keamanan yang diterapkan perbankan di Indonesia dalam konteks Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP), serta mengkaji mekanisme pertanggungjawaban hukum apabila terjadi kebocoran data nasabah. Rumusan masalah difokuskan pada bagaimana sistem keamanan perbankan diimplementasikan sesuai Undang-Undang Pelindungan Data Pribadi dan bagaimana mekanisme pertanggungjawaban hukumnya. Landasan teori utama adalah Undang-Undang Pelindungan Data Pribadi dan konsep perlindungan data pribadi. Metode analisis yang digunakan adalah yuridis normatif dengan mengkaji regulasi dan kasus yang relevan. Pembahasan akan mengevaluasi efektivitas sistem keamanan perbankan saat ini dan kerangka pertanggungjawaban hukum berdasarkan Undang-Undang Pelindungan Data Pribadi. Kesimpulan dari analisis ini menekankan pentingnya implementasi Undang-Undang Pelindungan Data Pribadi yang komprehensif dan mekanisme pertanggungjawaban yang tegas di sektor perbankan. Disarankan adanya perbaikan berkelanjutan pada infrastruktur keamanan siber dan peningkatan kepatuhan terhadap regulasi perlindungan data untuk memulihkan serta menjaga kepercayaan masyarakat.
Kata Kunci: Data Pribadi, Kebocoran Data, Keamanan Data, Perbankan, Perlindungan Hukum.

ABSTRACK

The banking sector plays a crucial role as a controller of customers' personal data in the digital era, but is faced with an increasing risk of data leakage along with the digitization of services. The data leak incident at Bank Indonesia and Bank Syariah Indonesia highlights the urgency of strengthening data security. This research aims to analyze the security system implemented by banks in Indonesia in the context of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), as well as examine the legal accountability mechanism in the event of a customer data leak. The formulation of the problem is focused on how the banking security system is implemented in accordance with the Personal Data Protection Law and how the legal accountability mechanism is. The main theoretical foundation is the Personal Data Protection Law and the concept of personal data protection. The analysis method used is normative juridical by examining relevant regulations and cases. The discussion will evaluate the effectiveness of the current banking security system and the legal accountability framework under the Personal Data Protection Act. The conclusions of this analysis emphasize the importance of the implementation of a comprehensive Personal Data Protection Law and a firm accountability mechanism in the banking sector. It is recommended that there be continuous improvements to cybersecurity infrastructure and increased compliance with data protection regulations to restore and maintain public trust.
Keywords: *Personal Data, Data Leakage, Data Security, Banking, Legal Protection*.

Pendahuluan

Bank merupakan badan usaha pelayanan yang melayani pada setor keuangan untuk menghimpun dana dari masyarakat dalam bentuk simpanan dan menyalurkannya kepada masyarakat dalam meningkatkan taraf hidup rakyat banyak (Indonesia, 2014). Artinya, bank menjadi salah satu badan usaha yang diamanahkan dalam kehidupan masyarakat dalam sektor keuangan, khususnya dalam mengelola dan menyimpan keuangan yang dilakukan oleh setiap individu kepada badan usaha tersebut. Dengan adanya bank, masyarakat diberi kemudahan dalam melakukan transaksi dan akses terhadap layanan keuangan. Bank juga merupakan pengendali data yang menjamin kemanan data nasabahnya, sehingga sudah banyak nasabah yang mempercayai layanan pada badan usaha tersebut (Elda Septi Darmayanti, 2025).

Membahas keamanan data, keamanan data sudah menjadi isu yang sangat krusial di era digital saat ini. Kemanan data tersebut mencakup data pribadi yang harus diamankan. Data pribadi merupakan data tentang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya, baik secara langsung maupun tidak langsung, melalui sistem elektronik maupun non elektronik (Elvina Putri Maheswari, 2025). (Undang-Undang (UU) Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi, 2022). Sektor perbankan menjadi salah satu badan usaha yang memegang amanah besar dalam mengelola dan menyimpan data pribadi pada nasabah. Digitalisasi layanan perbankan, mulai dari *mobile banking* hingga transaksi daring, semakin meningkatkan risiko terjadinya kebocoran data. Pasal 28G ayat (1) Undang-Undang Dasar Republik Indonesia menyebutkan"Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang dibawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancamanketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi" (Undang-Undang Dasar Negara Republik Indonesia 1945, N.D). Amanat konstitusi tersebut kemudian dipertegas dengan adanya Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP), yang mengatur perlindungan data pribadi warga negara di Indonesia. Sektor perbankan, sebagai pengendali data pribadi memiliki kewajiban khusus melindungi data pribadi nasabahnya dari akses ilegal, pengungkapan, atau kebocoran. Insiden kebocoran data pada sistem perbankan tidak hanya berpotensi menimbulkan kerugian finansial bagi nasabah, tetapi merusak reputasi institusi perbankan secara keseluruhan (Khetrina Maria Angnesia, 2025).

Pada tahun 2022 Bank Indonesia selaku bank sentral mengalami kebocoran data. Berdasarkan berita yang beredar di sosial media, melalui akun Twitter @darktracer_int membagikan potongan layar yang lengkap dengan keterangan file didalamnya (CNN Indonesia, 2022). Kejadian tersebut dibenarkan oleh Badan Siber dan Sandi Negara, dan serangan terjadi bermula pada 17 Desember 2021. Kebocoran tersebut terjadi secara berkala sampai pada tahun 2022 dan jumlah kebocoran data Bank Indonesia terus bertambah dalam jangka waktu tersebut. Selain itu, Bank Syariah Indonesia (BSI) mengalami hal yang serupa pada tahun 2023. Serangan *ransomware* yang diduga dilakukan oleh kelompok LockBit dilaporkan telah mengakibatkan kebocoran data pribadi sekitar 15 juta nasabah. Insiden ini menyebabkan gangguan layanan, kesulitan akses aplikasi *mobile banking*, keluhan nasabah di media sosial, dan kekhawatiran akan potensi penyalahgunaan data untuk penipuan atau kejahatan siber lainnya. Kebocoran data tersebut menjadi kekhawatiran bagi nasabah yang dirugikan, penyalahgunaan informasi pribadi untuk penipuan finansial bisa saja terjadi. Kebocoran data sistem perbankan juga dapat menimbulkan dampak yang merugikan bagi institusi perbankan, selain menimbulkan kerugian finansial, kebocoran data tersebut dapat merusak reputasi institusi perbankan.

Menanggapi kasus kebocoran data yang terjadi pada Bank Indonesia dan Bank Syariah Indonesia, dibutuhkannya urgensi mengenai keamanan data pribadi di sektor perbankan, mengingat dengan disahkannya Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi pada tanggal 17 Oktober 2022 menandai babak baru dalam tata kelola pelindungan data pribadi di Indonesia. Urgensi ini diharapkan agar tidak terjadi hal yang serupa kedepannya, sehingga masyarakat tidak lagi khawatir untuk mempercayai layanan keuangan pada sektor perbankan. Beberapa penelitian terdahulu telah membahas tema serta permasalahan yang penulis angkat. Sebagai bentuk orisinalitas, beberapa riset diperlukan penulis dengan tema dan permasalahan serupa dengan pokok bahasan yang berbeda dalam penelitian. Terdapat analisis yuridis yang berfokus pada kasus tunggal, seperti studi yang ditulis oleh Aditama Candra Kusuma dan Ayu Diah Rahmani yang berjudul *Analisis Yuridis Kebocoran Data Pada Sistem Perbankan Di Indonesia (Studi Kasus Kebocoran Data Pada Bank Indonesia),* yang menyoroti keterbatasan regulasi saat itu dan urgensi pengesahan

Rancangan Undang-Undang Pelindungan Data Pribadi (Kusuma & Rahmani, n.d.). Selain itu, penelitian yang lebih baru yang membahas implementasi Undang-Undang Pelindungan Data Pribadi, seperti studi yang ditulis oleh Danil Erlangga Mahameru, Aisyah Nurhalizah, Ahmad Wildan, Mochamad Haikal Badjeber, dan Mohamad Haikal Rahmadia yang berjudul *Implementasi Uu Perlindungan Data Pribadi Terhadap Keamanan Informasi Identitas Di Indonesia*, studi ini menyoroti pengimplementasian Undang-Undang Pelindungan Data Pribadi tehadap keamanan informasi identitas (Mahameru et al., n.d.) . Salah satu analisis pada sektor lain diluar perbankan, misalnya terkait kebocoran data di *platform e-commerce*, seperti studi yang ditulis oleh Maldi Omar Muhammad dan Lucky Dafira Nugroho yang berjudul *Perlindungan Hukum Terhadap Pengguna Aplikasi E-Commerce yang Terdampak Kebocoran Data Pribadi*, studi ini menyoroti perlindungan hukum bagi pengguna *e-commerce* yang mengalami kebocoran data pribadi (Muhammad & Nugroho, 2021) .

Berdasarkan uraian diatas, penelitian ini bertujuan menganalisis lebih lanjut sistem keamanan yang diterapkan oleh perbankan di Indonesia dalam konteks regulasi perlindungan data pribadi yang berlaku, yaitu Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi dan peraturan terkait dari Bank Indonesia atau Otoritas Jasa Keuangan (OJK), serta mengkaji mekanisme pertangggungjawaban hukum yang diterapkan apabila terjadi kebocoran data nasabah. Pemahaman mendalam terhadap isu ini diharapkan dapat memberikan kontribusi bagi perbaikan sistem keamanan perbankan dan penguatan perlindungan data pribadi di Indonesia.

Metode Penelitian

Penelitian ini mengguganakan metode penelitian hukum normatif, yaitu metode penelitian dengan mengkaji penelitian hukum dengan cara meneliti pustaka yang ada (Sidi A, 2025). Penelitian ini menggunakan pendekatan perundang-undangan (*statute approach).* Pendekatan perundang-undangan dipilih untuk menganalisis dan mengkaji secara sistematis berbagai peraturan perundang-undangan yang relevan dengan perlindungan data pribadi dan keamanan sistem informasi perbankan di Indonesia, termasuk Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi dan peraturan terkait dari Bank Indonesia atau Otoritas Jasa Keuangan (OJK).

Sumber bahan hukum yang digunakan dalam penelitian ini adalah sumber bahan primer, sumber bahan sekunder, dan sumber bahan tersier. Sumber bahan primer adalah sumber bahan hukum yang utama, meliputi Undang-Undang dan segala dokumen resmi yang memuat ketentuan hukum. Sumber bahan sekunder adalah bahan hukum tambahan sebagai pendukung sumber bahan primer, meliputi jurnal ilmiah, artikel berita, dan buku hukum. Sumber bahan tersier merupakan sumber hukum sebagai petunjuk dari sumber bahan primer dan sekunder, meliputi kamus, ensiklopedia, dan sumber internet lainnya. Teknik pengumpulan data dilakukan melalui studi kepustakaan (*library research*), yaitu dengan mengumpulkan, mengidentifikasi, dan mengkaji berbagai dokumen dan literatur yang relevan.

Hasil dan Pembahasan

A. Implementasi Sistem Keamanan Data Pribadi oleh Perbankan Indonesia dalam Perspektif Undang-Undang Pelindungan Data Pribadi

Implementasi sistem keamanan data pribadi di sektor perbankan merupakan sebuah keniscayaan, terlebih dengan amanat Undang-Undang Pelindungan Data Pribadi. Bank, dalam kapasitasnya sebagai pengendali data pribadi, memikul tanggung jawab besar untuk memastikan bahwa data nasabah diproses secara sah dan aman (Sri Mulyati, 2925). Berbicara mengenai sistem keamanan perbankan maka perlindungan bagi konsumen dari ancaman kejahatan *cyber* merupakan salah satu isu krusial yang perlu dipecahkan (Mega Kharisma Sari & Zulfiani, n.d.).

1. Kewajiban Umum Pengendali Data Pribadi (Bank) Berdasarkan Undang-Undang Data Pribadi

Data Pribadi merupakan elemen kunci bagi kebebasan harga diri individu (Rosadi, 2023). Data pribadi setiap individu tersebut, meliputi privasi bagi setiap individu yang wajib dilindungi. Dalam hal melindungi, pengendali data berkewajiban untuk melindungi data pribadi setiap individu. Pengendali data merupakan setiap orang, badan publik, dan organisasi internasional yang bertindak sendiri-sendiri atau bersama-sama dalam menentukan tujuan dan melakukan kendali pemrosesan data pribadi (Undang-Undang (UU) Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi, 2022). Pada sektor perbankan, Bank merupakan sebuah institusi pengendali data yang wajib melindungi data pribadi setiap nasabahnya. Dengan adanya Undang-Undang Pelindungan Data Pribadi, meletakkan serangkaian kewajiban fundamental bagi setiap pengendali data pribadi, termasuk institusi perbankan. Kewajiban ini dirancang untuk memastikan bahwa pemrosesan data pribadi dilakukan dengan menghormati hak-hak subjek data.

Pasca di undangkannya Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi, Undang-Undang tersebut menjadi ketentuan landasan utama bagi perlindungan data pribadi. Pasal 20 ayat (1) Undang-Undang Pelindungan Data Pribadi menyatakan "Pengendali Data Pribadi wajib memiliki dasar pemrosesan Data Pribadi". Artinya pengendali data memiliki kewajiban untuk melakukan pemrosesan data pribadi. Dalam hal memproses data pribadi seseorang, pengendali data wajib memiliki dasar pemrosesan sesuai dengan ketentuan Undang-Undang. Pengendali data wajib melakukan pemrosesan data pribadi berdasarkan prinsip-prinsip Pelindungan Data Pribadi (Muryani Verina Dwi, 2025). Ketentuan prinsip-prinsip tersebut tertuang pada pasal 16 ayat (2) Undang Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi.

Ketentuan yang telah disebutkan diatas berlaku bagi setiap pengendali data yang ingin melakukan pemrosesan data pribadi seseorang, tidak terkecuali pada sektor perbankan yang sering melakukan pemrosesan data pribadi para nasabahnya (Wyanda Kinanti Syauqi Ramadhani, 2025). Pemrosesan data pribadi dilakukan sesuai dengan prinsip Pelindungan Data Pribadi meliputi:

1) Pengumpulan data pribadi dilakukan secara terbatas dan spesifik, sah secara hukum, dan transparan: Bank harus jelas mengenai data apa saja yang dikumpulkan dari nasabah, untuk tujuan apa, dan bagaimana data tersebut akan diproses. Transparansi ini diwujudkan melalui kebijakan privasi yang mudah diakses dan dipahami nasabah.
2) Pemrosesan Data Pribadi dilakukan sesuai dengan tujuannya: Data yang dikumpulkan untuk pembukaan rekening, misalnya, tidak boleh digunakan untuk tujuan pemasaran tanpa persetujuan tambahan, kecuali diizinkan oleh peraturan perundang-undangan.
3) Pemrosesan Data Pribadi dilakukan dengan menjamin hak Subjek Data Pribadi: Bank harus memiliki mekanisme untuk mengakomodasi hak-hak nasabah, seperti hak untuk mengakses, memperbaiki, atau menghapus data mereka.
4) Pemrosesan Data Pribadi dilakukan secara akurat, lengkap, tidak menyesatkan, mutakhir, dan dapat dipertanggungjawabkan: Bank wajib memastikan data nasabah terjaga kualitasnya dan memiliki sistem untuk verifikasi serta pembaruan.
5) Pemrosesan Data Pribadi dilakukan dengan melindungi keamanan Data Pribadi dari pengaksesan yang tidak sah, pengungkapan yang tidak sah, pengubahan yang tidak sah, penyalahgunaan, perusakan, dan/atau penghilangan Data Pribadi: Ini adalah inti dari kewajiban keamanan, yang menuntut bank untuk mengimplementasikan langkah-langkah teknis dan organisasional yang memadai.
6) Pemrosesan Data Pribadi dilakukan dengan memberitahukan tujuan dan aktivitas Pemrosesan, serta kegagalan dalam Pelindungan Data Pribadi: Kewajiban notifikasi ini krusial, terutama jika terjadi insiden kebocoran data.

7) Data Pribadi dimusnahkan dan/atau dihapus setelah masa retensi berakhir atau berdasarkan permintaan Subjek Data Pribadi, kecuali ditentukan lain oleh peraturan perundang-undangan: Bank harus memiliki kebijakan retensi data yang jelas.
8) Pemrosesan Data Pribadi dilakukan dengan bertanggung jawab dan dapat menunjukkan kesesuaiannya dengan kewajiban Pemrosesan Data Pribadi: Prinsip akuntabilitas ini menuntut bank untuk dapat mendemonstrasikan kepatuhannya.

2. Kewajiban Khusus Perbankan dalam Menjamin Keamanan Data Nasabah

Selain kewajiban umum, Undang- Undang Pelindungan Data Pribadi juga mengatur kewajiban spesifik yang relevan dengan operasional perbankan. Kewajiban ini diberlakukan secara spesifik bagi setiap pengendali data yang ingin memproses data pribadi setiap individu. Membahas pemrosesan data pribadi pada sistem perbankan, tentunya menjadi hal krusial dalam memproses data setiap nasabahnya. Data diri setiap nasabahnya menjadi poin penting untuk dilindungi, karena didalamnya terdapat kerahasiaan pada setiap nasabah.

Hal pertama yang harus diperhatikan dalam pemrosesan data pribadi yang dilakukan oleh institusi Bank adalah melakukan persetujuan dengan para nasabah. Persetujuan menjadi langkah awal untuk melakukan pemrosesan data pribadi, serta pemilik data (nasabah) juga berhak menolak apabila tidak mau datanya diproses oleh Bank. Bank wajib mendapatkan persetujuan yang sah, spesifik, dan eksplisit dari nasabah untuk setiap tujuan pemrosesan data pribadi mereka. Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi telah mengatur proses persetujuan pemrosesan data pribadi. Proses tersebut meliputi penyampaian informasi pemrosesan data, bentuk persetujuan, serta bukti persetujuan yang wajib ditunjukkan pengendali data pribadi yang telah diberikan oleh Subjek data pribadi.

Pengendali data bertanggung jawab atas pemrosesan data pribadi, dan mewajibkan pengendali data pribadi untuk "melindungi dan memastikan keamanan Data Pribadi yang diprosesnya" dengan menetapkan langkah-langkah teknis operasional untuk mencegah gangguan pemrosesan data. Dalam melakukan pemrosesan data pribadi, pengendali data wajib menjaga kerahasiaan data pribadi, melakukan pengawasan terhadap setiap pihak yang melakukan pemrosesan data pribadi, serta pengendali data wajib melindungi data pribadi dari pemrosesan yang tidak sah. Ini artinya, Bank sebagai pengendali data harus:

- Melakukan penilaian risiko (Data Protection Impact Assessment/DPIA) terutama untuk pemrosesan data yang berisiko tinggi.
- Menerapkan teknologi keamanan yang sesuai, seperti enkripsi data saat transit dan *at rest*, sistem deteksi intrusi, *multi-factor authentication* (MFA).
- Mengembangkan dan menguji rencana kesinambungan bisnis dan pemulihan bencana (*Business Continuity Plan/Disaster Recovery Plan*) yang mencakup aspek keamanan data.
- Melakukan pengujian penetrasi (*penetration testing*) secara berkala untuk mengidentifikasi kerentanan.

Kewajiban dalam Undang-Undang Pelindungan Data Pribadi ini melengkapi dan memperkuat ketentuan yang sudah ada. UU No. 10 Tahun 1998 tentang Perubahan atas UU No. 7 Tahun 1992 tentang Perbankan (UU Perbankan), khususnya Pasal 40, mengatur mengenai Rahasia Bank. Rahasia bank adalah segala sesuatu yang berhubungan dengan keterangan mengenai nasabah penyimpan dan simpanannya. Meskipun UU PDP mengatur data pribadi secara lebih luas (tidak hanya data keuangan), prinsip kerahasiaan dalam UU Perbankan sejalan dengan prinsip integritas dan kerahasiaan dalam UU PDP. Selain itu juga, Otoritas Jasa Keuangan juga telah mengeluarkan berbagai peraturan terkait, seperti:

- Peraturan OJK No. 1/POJK.07/2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan, yang mewajibkan pelaku usaha jasa keuangan untuk menjaga keamanan informasi dan/atau data pribadi konsumen.
- Surat Edaran OJK No. 14/SEOJK.07/2014 tentang Kerahasiaan dan Keamanan Data dan/atau Informasi Pribadi Konsumen.
- Peraturan OJK mengenai Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum (misalnya, POJK No. 38/POJK.03/2016 yang kemudian diperbarui). Peraturan ini mengharuskan bank menerapkan manajemen risiko TI yang efektif, termasuk aspek keamanan siber.

Kebocoran data pribadi warga negara Indonesia merupakan tantangan serius dari segi ekonomi (Setiawan et al., 2022). Berdasarkan kasus kebocoran data di BI (akhir 2021, terungkap 2022) akibat serangan *ransomware* pada salah satu server non-kritikal, dan serangan *ransomware* LockBit terhadap BSI (Mei 2023) yang diduga membocorkan data 15 juta nasabah serta mengganggu layanan, menjadi cermin nyata. Kedua kasus kebocoran data tersebut menjadi bukti nyata, bahwa Bank dengan segala keamanannya tetap saja bisa mengalami kebocoran data. Berdasarkan pemberitaan, Bank Indonesia telah terjadi penyerangan pada server di kantor cabang Bengkulu dan menargetkan data yang tidak tergolong kritikal. Bank Indonesia mengklaim data nasabah dan sistem pembayaran inti tetap aman. Namun, insiden ini menunjukkan bahwa bahkan infrastruktur pendukung pun bisa menjadi titik masuk jika tidak diamankan dengan baik. Undang-Undang Pelindungan Data Pribadi, melalui Pasal 35 dan 36, menuntut perlindungan menyeluruh terhadap seluruh sistem yang memproses data pribadi. Selanjutnya Bank Syariah Indonesia mengalami serangan yang berdampak lebih luas, mengganggu layanan ATM dan *mobile banking* selama berhari-hari, serta dugaan eksfiltrasi data nasabah dalam jumlah besar. Hal ini menimbulkan pertanyaan mengenai implementasi enkripsi data sensitif (Pasal 37 Undang-Undang Pelindungan Data Pribadi), segmentasi jaringan, deteksi intrusi, dan respons insiden. Kewajiban pemberitahuan kegagalan pelindungan data pribadi kepada subjek data dan Otoritas Jasa Keuangan/Komisi Pelindungan Data Pribadi (Pasal 46 Undang-Undang Pelindungan Data Pribadi) menjadi sangat relevan di sini. Penundaan atau ketidakjelasan informasi dari BSI di awal insiden sempat menimbulkan keresahan publik.

Banyak bank mungkin telah memiliki kebijakan keamanan data dan prosedur operasional standar, namun implementasiannya yang kurang optimal. Terlebih Ancaman siber terus berevolusi (misalnya, *ransomware* yang semakin canggih, serangan *zero-day*). Bank perlu pendekatan keamanan yang adaptif (*adaptive security architecture*), tidak hanya mengandalkan pertahanan perimeter tradisional. Kesadaran dan pelatihan sumber daya manusia perbankan perlu diperhatikan mengenai pentingnya keamanan data dan praktik terbaik (*cyber hygiene*) adalah krusial. Faktor kelalaian manusia seringkali menjadi pintu masuk serangan. Bank juga seringkali menggunakan layanan vendor pihak ketiga untuk berbagai sistem TI. Undang-Undang Pelindungan Data Pribadi (Pasal 20 ayat (2) huruf e Jo. Pasal 51) juga menuntut pengendali data memastikan drosesor data (vendor) memberikan jaminan tingkat keamanan yang memadai. Kontrak dengan pihak ketiga harus mencakup klausul perlindungan data yang kuat.

3. Penelitian Relevan terkait Implementasi Sistem Keamanan

Penelitian-penelitian sebelumnya memberikan konteks penting**,** beberapa diantaranya:

1) Studi oleh Aditama Candra Kusuma dan Ayu Diah Rahmani mengenai kasus kebocoran data di Bank Indonesia menyoroti keterbatasan regulasi *sebelum* UU PDP disahkan dan menggarisbawahi urgensi adanya payung hukum yang komprehensif. Dengan disahkannya UU PDP, fokus kini beralih ke bagaimana UU ini diimplementasikan dan ditegakkan.

2) Penelitian oleh Danil Erlangga Mahameru dkk. tentang implementasi UU PDP terhadap keamanan informasi identitas secara umum menunjukkan tantangan awal dalam adopsi dan penyesuaian berbagai sektor terhadap rezim baru ini. Temuan mereka mengenai pentingnya pemahaman yang seragam dan kapasitas teknis untuk implementasi juga relevan bagi sektor perbankan.
3) Meskipun belum banyak penelitian spesifik yang mengkaji implementasi UU PDP *pasca-insiden BSI* di sektor perbankan, pelajaran dari sektor lain, seperti e-commerce (misalnya, studi Maldi Omar Muhammad dan Lucky Dafira Nugroho), menunjukkan bahwa isu kebocoran data dan perlindungan hukum adalah masalah lintas sektoral yang memerlukan perhatian serupa pada aspek teknis, tata kelola, dan penegakan hukum.

Analisis terhadap penelitian relevan ini menguatkan dugaan bahwa meskipun Undang-Undang Pelindungan Data Pelindungan telah menyediakan kerangka hukum yang lebih solid, perjalanan menuju implementasi sistem keamanan data yang sepenuhnya patuh dan efektif di sektor perbankan masih panjang dan menghadapi berbagai tantangan praktis.

B. Mekanisme Pertanggungjawaban Hukum Perbankan Akibat Kebocoran Data Nasabah

1. Bentuk-Bentuk Pertanggungjawaban Hukum berdasarkan Undang-Undang Pelindungan Data Pribadi

Pertanggungjawaban bank atas keamanan dana nasabah merupakan poin penting yang harus diperhatikan untuk menjaga stabilitas kelancaran bisnis perbankan (Transparansi Hukum et al., 2022). Untuk itu, Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi mengatur mekanisme pertanggung jawaban jika terjadi kegagalan dalam melindungi data pribadi, termasuk kebocoran data. Undang-Undang tersebut diharapkan dijadikan perlindungan hukum bagi nasabah perbankan sebagai bentuk pertanggungjawaban Bank terhadap nasabahnya.

Undang-Undang Pelindungan Data Pribadi memperkenalkan beberapa lapis pertanggung jawaban hukum bagi pengendali data pribadi yang melanggar ketentuan. Pelanggar ketentuan tersebut dapat diberikan beberapa sanksi, meliputi sanksi administratif, ganti rugi, dan sanksi pidana. Pasal 57 ayat (1) dan (2) Undang-Undang Pelindungan Data Pribadi merinci berbagai sanksi administratif yang dapat dikenakan oleh lembaga pengawas (nantinya Komisi Pelindungan Data Pribadi, untuk sementara dilaksanakan oleh Menteri Komunikasi dan Informatika) atas pelanggaran UU PDP. Sanksi tersebut meliputi: peringatan tertulis; penghentian sementara kegiatan Pemrosesan Data Pribadi; dan/atau denda administratif. Denda administratif, sebagaimana diatur dalam Pasal 57 ayat (3), dapat dikenakan paling tinggi 2% (dua persen) dari pendapatan tahunan atau penerimaan tahunan variabel terhadap variabel pelanggaran. Untuk bank yang lalai hingga menyebabkan kebocoran data nasabah, terutama jika terbukti adanya pelanggaran terhadap kewajiban keamanan (Pasal 35-39) atau prinsip-prinsip pemrosesan (Pasal 16), sanksi administratif ini sangat mungkin diterapkan. Besaran denda yang signifikan diharapkan dapat menjadi efek jera.

Pasal 12 Undang-Undang Pelindungan Data Pribadi mengatur hak subjek data untuk menggugat dan menerima ganti rugi atas pelanggaran pemrosesan data pribadi tentang dirinya sesuai dengan ketentuan peraturan perundang-undangan. Lebih lanjut, Pasal 46 ayat (1) Undang-Undang Pelindungan Data Pribadi mengatur bahwa dalam hal terjadi kegagalan pelindungan data pribadi, Pengendali Data Pribadi wajib menyampaikan pemberitahuan tertulis paling lambat 3 x 24 jam kepada Subjek Data Pribadi dan Lembaga. Pasal 46 ayat (2) menyebutkan pemberitahuan tersebut paling sedikit memuat: (a) Data Pribadi yang terungkap; (b) kapan dan bagaimana Data Pribadi terungkap; dan (c) upaya penanganan dan pemulihan atas terungkapnya Data Pribadi oleh Pengendali

Data Pribadi. Kegagalan notifikasi ini saja sudah merupakan pelanggaran. Nasabah yang merasa dirugikan akibat kebocoran data pribadinya (misalnya, kerugian finansial akibat penipuan, kerugian imateriel akibat pencemaran nama baik) berhak mengajukan gugatan ganti rugi. Mekanisme ini bisa melalui gugatan perdata biasa atau, jika melibatkan banyak korban, melalui mekanisme *class action* sebagaimana diatur dalam hukum acara perdata.

Selain sanksi administratif dan ganti rugi, Undang-Undang Pelindungan Data Pribadi juga memuat ketentuan pidana bagi pelanggaran yang lebih serius dan disengaja. Pasal 65 dan 66 mengatur pidana bagi setiap orang yang dengan sengaja dan melawan hukum memperoleh atau mengumpulkan data pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum atau yang dapat mengakibatkan kerugian subjek data. Pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah). Pasal 67 dan 68 mengatur pidana bagi setiap orang yang dengan sengaja dan melawan hukum mengungkapkan atau menggunakan Data Pribadi yang bukan miliknya. Pidana penjara paling lama 4 (empat) tahun dan/atau pidana denda paling banyak Rp4.000.000.000,00 (empat miliar rupiah) untuk pengungkapan, dan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah) untuk penggunaan. Jika pelanggaran ini dilakukan oleh korporasi (bank), maka pidana dapat dijatuhkan kepada pengurus, pemegang kendali, pemberi perintah, atau pemilik manfaat korporasi (Pasal 70 ayat (1) Undang-Undang Pelindungan Data Pribadi). Selain pidana denda (maksimum pidana denda ditambah dua pertiga), korporasi dapat dijatuhi pidana tambahan berupa perampasan keuntungan, pembekuan sebagian atau seluruh usaha, hingga pembubaran korporasi (Pasal 70 ayat (2) Undang-Undang Pelindung Data Pribadi). Dalam konteks kebocoran data di bank, sanksi pidana ini bisa relevan jika terbukti ada unsur kesengajaan dari oknum internal bank dalam membocorkan atau menyalahgunakan data nasabah, atau jika kelalaian bank dalam menjaga keamanan data dianggap sedemikian rupa sehingga memenuhi unsur "melawan hukum" secara pidana korporasi.

2. Pertanggungjawaban Hukum dalam Konteks Regulasi Sektoral Perbankan

Mekanisme pertanggungjawaban dalam Undang-Undang Pelindungan Data Pribadi ini akan berjalan beriringan atau bahkan melengkapi mekanisme yang sudah ada dalam regulasi sektoral perbankan. Regulasi sektoral perbankan saat ini diatur dalam Undang-Undang Nomor 10 Tahun 1998 Tentang Perubahan Atas Undang-Undang Nomor 7 Tahun 1992 Tentang Perbankan, Undang-Undang tersebut memuat pelanggaran terhadap kewajiban menjaga rahasia bank (Pasal 40 Undang-Undang Perbankan) juga memiliki konsekuensi pidana (UNDANG-UNDANG REPUBLIK INDONESIA NOMOR 10 TAHUN 1998 TENTANG PERUBAHAN ATAS UNDANG-UNDANG NOMOR 7 TAHUN 1992, n.d.). Pasal 47 ayat (1) dan (2) Undang-Undang Perbankan mengatur sanksi pidana bagi anggota dewan komisaris, direksi, pegawai bank, atau pihak terafiliasi yang dengan sengaja memberikan keterangan yang wajib dirahasiakan. Selain itu, Otoritas Jasa Keuangan sebagai pengawas sektor jasa keuangan memiliki kewenangan untuk mengenakan sanksi administratif kepada bank yang melanggar ketentuan, termasuk yang berkaitan dengan perlindungan konsumen dan manajemen risiko TI. Sanksi ini bisa berupa teguran tertulis, denda, pembatasan kegiatan usaha, hingga pencabutan izin usaha. Peraturan Otoritas Jasa Keuangan Perlindungan Konsumen (No. 1/POJK.07/2013) misalnya, juga menekankan tanggung jawab Pelaku Usaha Jasa Keuangan (PUJK) untuk menjaga keamanan data konsumen (PERATURAN OTORITAS JASA KEUANGAN REPUBLIK INDONESIA NOMOR: 1/PJOK.07/2013 TENTANG PERLINDUNGAN KONSUMEN SEKTOR JASA KEUANGAN, n.d.).

Dalam praktik, bisa terjadi *concurrent liability* atau pertanggungjawaban yang tumpang tindih. Prinsip *lex specialis derogat legi generali* (aturan khusus mengesampingkan aturan umum) mungkin berlaku dalam beberapa aspek, namun Undang-Undang Pelindungan Data Pribadi sebagai undang-undang payung perlindungan data pribadi juga memiliki bobot signifikan. Kemungkinan besar, penegakan akan bersifat komplementer, di mana Otoritas Jasa Keuangan fokus pada aspek kepatuhan prudensial dan perlindungan konsumen di sektor keuangan, sementara Komisi Pelindungan Data Pribadi (atau Kemenkominfo untuk sementara) fokus pada aspek kepatuhan umum terhadap Undang-Undang Pelindungan Data Pribadi. Koordinasi antar lembaga menjadi sangat penting.

Membahas kasus Bank Indonesia dan Bank Syariah Indonesia. Meskipun Bank Indonesia mengklaim data kritikal aman, investigasi tetap perlu untuk menentukan apakah ada kelalaian dalam pengamanan server yang diretas. Jika ada, sanksi administratif dari Undang-Undang Pelindungan Data Pribadi bisa relevan, meskipun status Bank Indonesia sebagai bank sentral mungkin memiliki implikasi tersendiri dalam penegakan. Berbanding terbalik dengan kasus Bank Syariah Indonesia yang lebih kompleks karena dampak luas dan dugaan kebocoran data nasabah dalam jumlah besar. Potensi pertanggungjawaban Bank Syariah Indonesia dapat meliputi, sanksi administratif dari Otoritas Jasa Keuangan dan Komisi Pelindungan Data Pribadi (Kemenkominfo) karena gagal melindungi data nasabah dan potensi pelanggaran kewajiban notifikasi, gugatan ganti rugi dari nasabah yang merasa dirugikan, baik secara perorangan maupun *class action*, potensi penyelidikan pidana jika ditemukan unsur kesengajaan atau kelalaian berat yang memenuhi unsur pidana korporasi dalam UU PDP. Penyelesaian kasus BSI sejauh ini (berdasarkan informasi publik) lebih banyak berfokus pada pemulihan layanan dan investigasi internal/eksternal. Namun, tuntutan pertanggungjawaban hukum dari nasabah dan regulator masih menjadi bayang-bayang yang signifikan.

Meskipun kerangka hukumnya ada, penegakan pertanggungjawaban hukum akibat kebocoran data tidaklah mudah. Bagi nasabah, membuktikan kerugian langsung akibat kebocoran data dan adanya kausalitas dengan kelalaian bank bisa menjadi tantangan. Bank mungkin berdalih bahwa serangan siber adalah *force majeure* atau tindakan pihak ketiga yang canggih. Mengidentifikasi pelaku serangan siber seringkali sulit, mempersulit proses pidana terhadap peretas. Namun, fokus Undang-Undang Pelindungan Data Pribadi adalah pada tanggung jawab pengendali data untuk mencegah dan merespons, terlepas dari identitas peretas. Tingkat kesadaran nasabah akan hak-hak mereka berdasarkan Undang-Undang Pelindungan Data Pribadi dan kemauan untuk menempuh jalur hukum juga mempengaruhi efektivitas penegakan.

Berdasarkan uraian diatas, penulis berpendapat Undang-Undang Pelindungan Data Pribadi menyediakan arsenal hukum yang lebih kuat dibandingkan sebelumnya untuk menuntut pertanggungjawaban bank. Namun, efektivitasnya akan sangat bergantung pada implementasi teknis di lembaga pengawas dan penegak hukum, serta preseden kasus yang terbentuk. Perlunya pedoman atau peraturan pelaksana Undang-Undang Pelindungan Data Pribadi yang lebih detail mengenai tata cara investigasi, pengenaan sanksi administratif (khususnya perhitungan denda), dan mekanisme ganti rugi untuk kasus kebocoran data massal.

Analisis terhadap implementasi sistem keamanan dan mekanisme pertanggungjawaban hukum di sektor perbankan ini didasari oleh beberapa kerangka teori. Teori perlindungan hukum menjadi sorotan yang menjelaskan bahwa hukum diciptakan untuk memberikan perlindungan terhadap berbagai kepentingan individu dan masyarakat. Menurut Soerjono Soekanto, perlindungan hukum adalah segala upaya

pemenuhan hak dan pemberian bantuan untuk memberikan rasa aman kepada saksi dan atau korban yang dapat diwujudkan dalam bentuk restitusi, kompensasi, pelayanan medis, dan bantuan hukum (Soekanto, 2014). Dalam konteks ini, Undang-Undang Pelindungan Data Pribadi dan regulasi terkait bertujuan memberikan perlindungan hukum terhadap hak privasi dan keamanan data pribadi nasabah bank dari penyalahgunaan atau kelalaian. Perlindungan ini bersifat preventif (kewajiban bank untuk membangun sistem keamanan) dan represif (sanksi dan ganti rugi jika terjadi pelanggaran).

Teori tanggung jawab hukum membahas dasar-dasar mengapa suatu pihak harus bertanggung jawab atas kerugian yang timbul akibat perbuatannya atau kelalaiannya. Menurut Hans Kelsen, Tanggung jawab hukum menyatakan bahwa seseorang bertanggung jawab atas hukum atas perbuaatan tertentu atau bahwa dia memikul tanggung jawab hukum, artinya dia bertanggung jawab atas suatu sanksi bila perbuatannya bertentangan dengan peraturan yang berlaku (Kelsen, 2014). Dalam kasus kebocoran data, pertanggungjawaban bank dapat didasarkan pada kesalahan/kelalaian. Bank bertanggung jawab jika terbukti lalai dalam menerapkan standar keamanan yang wajar. Dalam konteks tertentu, bisa mengarah pada *strict liability* (tanggung jawab mutlak) di mana bank sebagai pengendali data dianggap bertanggung jawab atas keamanan data yang diprosesnya, terlepas dari pembuktian kesalahan spesifik, terutama jika gagal memenuhi kewajiban dasar Undang-Undang Pelindungan Data Pribadi. Undang-Undang Pelindungan Data Pribadicenderung memperkuat posisi nasabah dalam hal ini.

Undang-Undang Pelindungan Data Pribadi mengadopsi terminologi Konsep Pengendali Data (Data Controller) dan Prosesor Data (Data Processor) dari kerangka hukum perlindungan data global (seperti Global Data Protection Regulation). Bank, dalam sebagian besar aktivitasnya dengan nasabah, bertindak sebagai Pengendali Data. Ini berarti bank yang menentukan tujuan dan sarana pemrosesan data pribadi nasabah, sehingga memikul tanggung jawab utama atas kepatuhan terhadap Undang-Undang Pelindungan Data Pribadi. Jika bank menggunakan vendor untuk memproses data (misalnya, penyedia layanan *cloud*), vendor tersebut bertindak sebagai Prosesor Data, dan bank tetap bertanggung jawab untuk memastikan vendor tersebut juga patuh. Pemahaman peran ini krusial dalam menentukan alokasi tanggung jawab.

Analisis berdasarkan teori-teori ini menunjukkan bahwa Undang-Undang Pelindungan Data Pribadi secara signifikan mengubah lanskap hukum perlindungan data di Indonesia, termasuk bagi sektor perbankan. Implementasi yang efektif dan penegakan yang konsisten akan menjadi kunci untuk mewujudkan tujuan Undang-Undang Pelindungan Data Pribadi dalam melindungi data pribadi warga negara dan membangun kepercayaan dalam ekosistem digital. Kasus-kasus yang menimpa Bank Indonesia dan Bank Syariah Indonesia menjadi pengingat penting akan tantangan yang masih harus dihadapi.

Kesimpulan dan Saran

Berdasarkan analisis terhadap keamanan data pribadi di sektor perbankan Indonesia, dapat ditarik kesimpulan bahwa sektor perbankan memegang tanggung jawab besar sebagai pengendali data pribadi nasabah di tengah era digitalisasi yang meningkatkan risiko kebocoran data. Kasus kebocoran data yang menimpa Bank Indonesia dan Bank Syariah Indonesia menjadi pengingat penting akan urgensi penguatan sistem keamanan data. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) telah hadir sebagai landasan hukum fundamental, namun implementasi yang komprehensif dan mekanisme pertanggungjawaban yang tegas di sektor perbankan masih menjadi pekerjaan rumah yang

harus diselesaikan. Meskipun kerangka hukum telah ada, efektivitasnya sangat bergantung pada implementasi teknis yang solid di lembaga perbankan dan penegakan hukum yang konsisten, serta kesadaran dari semua pihak akan pentingnya pelindungan data pribadi.

Untuk menjawab tantangan tersebut dan meningkatkan kepercayaan masyarakat, beberapa langkah strategis perlu diimplementasikan. Pertama, perbankan wajib melakukan perbaikan berkelanjutan pada infrastruktur keamanan siber mereka, mengadopsi teknologi keamanan adaptif, dan memastikan manajemen risiko teknologi informasi yang efektif. Kedua, peningkatan kepatuhan terhadap seluruh ketentuan dalam UU PDP dan peraturan sektoral terkait harus menjadi prioritas, termasuk dalam hal transparansi pemrosesan data dan pemenuhan hak-hak subjek data. Ketiga, sangat penting untuk meningkatkan kesadaran dan kompetensi sumber daya manusia di sektor perbankan mengenai keamanan data dan praktik terbaik dalam menjaga kerahasiaan informasi nasabah. Terakhir, pemerintah diharapkan segera mengeluarkan peraturan pelaksana UU PDP yang lebih teknis dan detail, khususnya mengenai standar keamanan data, tata cara pelaporan insiden, perhitungan denda administratif, dan mekanisme ganti rugi yang efektif bagi nasabah yang terdampak kebocoran data.

Daftar Pustaka

Elda Septi Darmayanti, S. A. (2025). Tanggung jawab hukum pinjaman online terhadap penyebaran data nasabah secara ilegal. *ALADALAH: Jurnal Politik, Sosial, Hukum dan Humaniora*, 233-251.

Elvina Putri Maheswari, S. A. (2025). Urgensi persetujuan pemilik data dalam pengelolaan data pribadi oleh platform digital. *Jurnal Ilmu Komunikasi Dan Sosial Politik*, 908-914.

Indonesia, I. B. (2014). *MENGELOLA BANK KOMERSIAL*. Jakarta: PT Gramedia Pustaka Utama .

Kelsen, H. (2014). *Teori Umum Tentang Hukum dan Negara.* Bandung: Nusa Media.

Khetrina Maria Angnesia, S. A. (2025). Analisis Pertanggungjawaban Hukum Pemerintah dalam Menegakkan Pelindungan Data Pribadi di Era Digital. *Perspektif Administrasi Publik dan hukum*, 176-187.

Muryani Verina Dwi, W. S. (2025). EFEKTIVITAS UNDANG-UNDANG PERLINDUNGAN DATA PRIBADI DALAM MENJAWAB TANTANGAN KEAMANAN SIBER DI INDONESIA. *Causa: Jurnal Hukum dan Kewarganegaraan*, 81-90.

Rosadi, S. D. (2023). *Pembahasan UU Pelindungan Data Pribadi (UU RI No. 27 Tahun 2022).* Jakarta Timur: Sinar Grafika.

Sidi A, W. (2025). EKSPLORASI METODE PENELITIAN DENGAN PENDEKATAN NORMATIF DAN EMPIRIS DALAM PENELITIAN HUKUM DI INDONESIA. *Lex Jurnalica*, 66-72.

Soekanto, S. (2014). *Pengantar Penelitian Hukum.* Jakarta: Universitas Indonesia.

Sri Mulyati, S. A. (2925). PERLINDUNGAN DATA PRIBADI DI ERA DIGITAL. *Causa: Jurnal Hukum dan Kewarganegaraan*, 91-100.

Wyanda Kinanti Syauqi Ramadhani, S. A. (2025). Implementasi Pelindungan Data Pribadi dalam Sistem Informasi pada Perusahaan Jasa Keuangan. *Perspektif Administrasi Publik dan hukum*, 158-175.

CNN Indonesia. (2022, January 24). *Kebocoran Data Bank Indonesia Belum Selesai, Naik Jadi 74GB* .

PERATURAN OTORITAS JASA KEUANGAN REPUBLIK INDONESIA NOMOR: 1/PJOK.07/2013 TENTANG PERLINDUNGAN KONSUMEN SEKTOR JASA KEUANGAN. (n.d.).

Kusuma, A. C., & Rahmani, A. D. (n.d.). *Analisis Yuridis Kebocoran Data Pada Sistem Perbankan Di Indonesia (Studi Kasus Kebocoran Data Pada Bank Indonesia)*. www.bi.go.id.

Mahameru, D. E., Nurhalizah, A., Wildan, A., Haikal Badjeber, M., & Rahmadia, M. H. (n.d.). *IMPLEMENTASI UU PERLINDUNGAN DATA PRIBADI TERHADAP KEAMANAN INFORMASI IDENTITAS DI INDONESIA*. https://journal.upnvj.ac.id/index.php/esensihukum/index

Mega Kharisma Sari, C., & Zulfiani, A. (n.d.). *Law, Development & Justice Review Upaya Menghadapi Kejahatan Terhadap Sistem Keamanan Perbankan Indonesia di Era Cyberspace*.

Muhammad, M. O., & Nugroho, L. D. (2021). Perlindungan Hukum Terhadap Pengguna Aplikasi E-Commerce yang Terdampak Kebocoran Data Pribadi. *Pamator Journal*, *14*(2), 165–174. https://doi.org/10.21107/pamator.v14i2.12472

UNDANG-UNDANG REPUBLIK INDONESIA NOMOR 10 TAHUN 1998 TENTANG PERUBAHAN ATAS UNDANG-UNDANG NOMOR 7 TAHUN 1992. (n.d.).

Setiawan, H. B., Fatma, &, & Najicha, U. (2022). PERLINDUNGAN DATA PRIBADI WARGA NEGARA INDONESIA TERKAIT DENGAN KEBOCORAN DATA. *Jurnal Kewarganegaraan*, *6*(1).

Transparansi Hukum, J., Cahyo Setiono, G., Rahman, I., & Delaria Ananfa, E. (2022). *TANGGUNG JAWAB BANK SEBAGAI WUJUD PERLINDUNGAN HUKUM BAGI NASABAH KONTRAK PERBANKAN*. *5*(1).

UNDANG-UNDANG DASAR NEGARA REPUBLIK INDONESIA 1945. (n.d.).

Undang-Undang (UU) Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi, Pub. L. No. 27 (2022).