

PERLINDUNGAN DATA PRIBADI SEBAGAI INSTRUMEN HUKUM DALAM MENANGGULANGI KEJAHATAN PERBANKAN

Noris Sugiarto¹, Indra Yuliawan², Arista Candra Irawati³

^{1,2,3} Program Studi Ilmu Hukum, Universitas Ngudi Waluyo

norissugiarto@gmail.com, aristacandrairawati@unw.ac.id

ABSTRACT

Digital transformation in the banking sector has enhanced the efficiency of financial services while simultaneously increasing the risk of data-driven banking crimes. Customers' personal data have become both the object and the primary means of various criminal activities, such as identity theft, phishing, and misuse of financial information. This condition necessitates robust personal data protection as an integral part of the banking legal system. This article aims to analyze the concept of personal data protection in the context of banking crimes, examine the legal framework governing personal data protection in the Indonesian banking sector, and explain the urgency of personal data protection as a legal instrument for preventing banking crimes. The research employs a normative legal method with statutory and conceptual approaches. The findings indicate that Law Number 27 of 2022 on Personal Data Protection strengthens the principle of bank secrecy and functions as both a preventive and repressive legal instrument in addressing data-based banking crimes. Personal data protection plays a crucial role not only in safeguarding customers' rights but also in maintaining public trust and the stability of the national banking system.

Keywords: Personal Data Protection; Banking Crimes; Personal Data Protection Law.

ABSTRAK

Transformasi digital di sektor perbankan telah mendorong peningkatan efisiensi layanan keuangan, namun sekaligus meningkatkan risiko kejahatan perbankan berbasis data pribadi. Data pribadi nasabah menjadi objek sekaligus sarana utama dalam berbagai modus kejahatan, seperti pencurian identitas, *phishing*, dan penyalahgunaan informasi keuangan. Kondisi ini menuntut adanya perlindungan data pribadi yang kuat sebagai bagian dari sistem hukum perbankan. Artikel ini bertujuan untuk menganalisis konsep perlindungan data pribadi dalam konteks kejahatan perbankan, mengkaji pengaturan hukum perlindungan data pribadi di sektor perbankan Indonesia, serta menjelaskan urgensi perlindungan data pribadi sebagai instrumen hukum dalam pencegahan kejahatan perbankan. Metode penelitian yang digunakan adalah penelitian hukum normatif dengan pendekatan perundang-undangan dan konseptual. Hasil penelitian menunjukkan bahwa Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi memperkuat prinsip rahasia bank dan berfungsi sebagai instrumen hukum preventif dan represif dalam menanggulangi kejahatan perbankan berbasis data. Perlindungan data pribadi tidak hanya berperan dalam melindungi hak nasabah,

tetapi juga dalam menjaga kepercayaan publik dan stabilitas sistem perbankan nasional.

Kata kunci: Perlindungan Data Pribadi; Kejahatan Perbankan; UU Perlindungan Data Pribadi

A. Pendahuluan

Perkembangan teknologi informasi telah mendorong transformasi signifikan dalam sektor perbankan melalui digitalisasi layanan keuangan. Digitalisasi tersebut memungkinkan transaksi dilakukan secara cepat, efisien, dan tanpa batasan ruang serta waktu. Layanan *mobile banking*, *internet banking*, dan sistem pembayaran elektronik kini menjadi tulang punggung aktivitas keuangan masyarakat modern. Namun, di balik kemudahan tersebut terdapat risiko serius berupa meningkatnya pengolahan data pribadi nasabah dalam skala besar. Data pribadi yang diproses secara masif ini memiliki nilai ekonomi tinggi dan menjadi target utama kejahatan perbankan berbasis teknologi. Oleh karena itu, perlindungan data pribadi menjadi isu hukum yang krusial dalam menjaga keamanan dan kepercayaan publik terhadap sistem perbankan (Solove, 2021, hlm. 109–112).

Digitalisasi perbankan menempatkan bank sebagai pengendali data (*data controller*) yang bertanggung jawab atas pengelolaan data pribadi nasabah. Data tersebut mencakup identitas, informasi finansial, serta riwayat transaksi yang bersifat rahasia. Dalam praktiknya, semakin banyak data yang diproses, semakin besar pula potensi penyalahgunaan data tersebut. Kejahatan perbankan modern seperti *phishing*, pencurian identitas, dan *social engineering* kerap bermula dari kebocoran data pribadi (Gunawan, C., & Irawati, A. C. (2025). Kondisi ini menunjukkan adanya hubungan erat antara lemahnya perlindungan data dan meningkatnya kejahatan perbankan. Oleh sebab itu, perlindungan data pribadi tidak dapat dipisahkan dari upaya pencegahan tindak pidana perbankan (Kuner, 2017, hlm. 95–97).

Secara konseptual, perlindungan data pribadi merupakan

bagian integral dari hak atas privasi sebagai hak asasi manusia. Hak atas privasi menuntut adanya jaminan bahwa data pribadi seseorang tidak diproses atau digunakan tanpa dasar hukum yang sah (Irawati, A. C., Wijaya, H., & Pratama, A. (2025). Dalam sektor perbankan, hak ini memiliki dimensi yang lebih luas karena berkaitan langsung dengan perlindungan harta kekayaan nasabah. Oleh karena itu, pelanggaran terhadap data pribadi nasabah dapat berdampak pada kerugian material dan immaterial. Negara memiliki kewajiban untuk menjamin perlindungan hak tersebut melalui instrumen hukum yang efektif. Konsepsi ini menempatkan perlindungan data pribadi sebagai kewajiban negara dalam kerangka negara hukum (Warren & Brandeis, 1890, hlm. 195–198).

Di Indonesia, perlindungan data pribadi memperoleh dasar hukum yang kuat dengan diundangkannya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Undang-undang ini menegaskan bahwa data pribadi merupakan hak subjek data yang wajib dilindungi dalam setiap proses pengolahan data. UU PDP mengatur

prinsip pemrosesan data, hak subjek data, serta kewajiban pengendali data. Keberadaan undang-undang ini menandai pergeseran paradigma dari perlindungan sektoral menuju perlindungan data yang komprehensif. Dalam konteks perbankan, bank secara tegas dikualifikasikan sebagai pengendali data yang memiliki tanggung jawab hukum. Oleh karena itu, UU PDP menjadi instrumen utama dalam penguatan perlindungan data nasabah (UU 27/2022).

Sebelum berlakunya UU PDP, perlindungan data nasabah bank terutama bertumpu pada prinsip rahasia bank sebagaimana diatur dalam Undang-Undang Perbankan. Prinsip tersebut mewajibkan bank untuk merahasiakan data dan simpanan nasabah. Namun, prinsip rahasia bank memiliki keterbatasan karena lebih berfokus pada kerahasiaan informasi keuangan. Perkembangan teknologi telah memperluas jenis data yang diproses oleh bank, termasuk data digital dan biometrik. Kondisi ini menunjukkan bahwa prinsip rahasia bank tidak lagi memadai sebagai satu-satunya instrumen perlindungan data. Oleh karena itu, UU PDP hadir untuk

melengkapi dan memperkuat rezim hukum perbankan (Marzuki, 2017, hlm. 134–136).

Kejahatan perbankan berbasis data menunjukkan bahwa lemahnya perlindungan data pribadi dapat berimplikasi langsung pada meningkatnya tindak pidana. Data yang bocor atau disalahgunakan dapat digunakan untuk melakukan transaksi ilegal dan pemalsuan identitas. Dalam banyak kasus, nasabah baru menyadari penyalahgunaan data setelah mengalami kerugian finansial. Hal ini menunjukkan bahwa perlindungan data pribadi memiliki fungsi preventif yang sangat penting. Dengan perlindungan data yang kuat, peluang pelaku kejahatan untuk mengakses data nasabah dapat diminimalkan. Oleh karena itu, perlindungan data pribadi berfungsi sebagai instrumen pencegahan kejahatan perbankan (Siregar & Putra, 2023, hlm. 220–223). Selain fungsi preventif, perlindungan data pribadi juga memiliki fungsi represif melalui mekanisme penegakan hukum. UU PDP mengatur sanksi administratif, perdata, dan pidana bagi pihak yang melanggar ketentuan perlindungan data. Sanksi tersebut dimaksudkan

untuk memberikan efek jera dan meningkatkan kepatuhan pengendali data. Dalam sektor perbankan, sanksi ini dapat diterapkan apabila terjadi kebocoran data akibat kelalaian atau kesengajaan. Penegakan hukum yang konsisten menjadi kunci efektivitas perlindungan data pribadi. Tanpa penegakan hukum yang tegas, perlindungan data hanya akan bersifat normatif (Ali, 2015, hlm. 88–90).

Perlindungan data pribadi juga berkaitan erat dengan kepercayaan publik terhadap sistem perbankan. Kepercayaan merupakan fondasi utama dalam aktivitas perbankan karena berkaitan dengan pengelolaan dana masyarakat. Kebocoran data dapat menurunkan kepercayaan tersebut dan berdampak pada stabilitas sistem keuangan. Oleh sebab itu, bank dituntut untuk menerapkan tata kelola data yang baik. Perlindungan data pribadi menjadi bagian dari *good corporate governance* perbankan. Dengan demikian, isu perlindungan data memiliki dimensi hukum dan ekonomi sekaligus (OECD, 2013, hlm. 19–21). Perspektif hukum normatif, perlindungan data pribadi dalam perbankan harus dipahami sebagai

kewajiban hukum yang melekat pada bank. Kewajiban ini mencakup aspek teknis, administratif, dan organisatoris. Bank wajib memastikan bahwa setiap pemrosesan data dilakukan secara sah dan aman. Pelanggaran terhadap kewajiban tersebut dapat menimbulkan tanggung jawab hukum. Dalam konteks kejahatan perbankan, tanggung jawab ini menjadi sangat penting. Oleh karena itu, analisis yuridis terhadap kewajiban bank menjadi relevan (Solove, 2021, hlm. 145–147).

Keberadaan UU PDP telah memberikan kerangka hukum yang jelas, implementasinya di sektor perbankan masih menghadapi berbagai tantangan. Tantangan tersebut meliputi kesiapan infrastruktur teknologi dan sumber daya manusia. Selain itu, masih terdapat kesenjangan antara norma hukum dan praktik di lapangan. Beberapa kasus kebocoran data menunjukkan adanya kelemahan sistem pengamanan internal bank. Kondisi ini mengindikasikan bahwa regulasi perlu didukung oleh pengawasan yang efektif. Oleh karena itu, kajian akademik diperlukan untuk menilai efektivitas

implementasi UU PDP (Kuner, 2017, hlm. 101–103).

Penelitian ini memandang perlindungan data pribadi sebagai instrumen hukum yang strategis dalam menanggulangi kejahatan perbankan. Instrumen hukum tidak hanya berfungsi sebagai aturan tertulis, tetapi juga sebagai sarana pengendalian sosial. Dengan norma yang jelas dan sanksi yang tegas, hukum dapat membatasi perilaku yang berpotensi menimbulkan kejahatan. UU PDP memiliki potensi besar dalam memperkuat pencegahan kejahatan perbankan. Namun, efektivitasnya perlu diuji melalui kajian akademik. Hal ini menjadi dasar penting penelitian ini (Ali, 2015, hlm. 101–103). Perlindungan data pribadi memiliki posisi sentral dalam sistem hukum perbankan modern. Perlindungan data tidak lagi dapat dipandang sebagai isu teknis semata. Kejahatan perbankan berbasis data menunjukkan adanya hubungan langsung antara lemahnya perlindungan data dan meningkatnya tindak pidana. Oleh karena itu, pendekatan hukum menjadi sangat penting dalam menanggulangi masalah ini. Penelitian ini berupaya

mengkaji isu tersebut secara sistematis. Fokus kajian diarahkan pada peran hukum perlindungan data dalam sektor perbankan (Marzuki, 2017, hlm. 158–160).

Berdasarkan latar belakang tersebut, rumusan masalah dalam penelitian ini dirumuskan sebagai berikut: (1) Bagaimana konsep perlindungan data pribadi dalam hukum perbankan?; (2) Bagaimana pengaturan hukum perlindungan data pribadi dalam menanggulangi kejahatan perbankan? dan (3) Bagaimana urgensi perlindungan data pribadi sebagai instrumen hukum dalam pencegahan kejahatan perbankan.

Fokus studi penelitian mengenai perlindungan data pribadi sebagai instrumen hukum dalam menanggulangi kejahatan perbankan memiliki urgensi yang tinggi. Perkembangan teknologi menuntut respons hukum yang adaptif dan progresif. Perlindungan data pribadi menjadi kunci dalam menjaga keamanan dan kepercayaan publik terhadap sistem perbankan. Tanpa perlindungan data yang memadai, kejahatan perbankan akan terus berkembang. Oleh karena itu, kajian ini relevan secara akademik dan

praktis. Penelitian ini diharapkan mampu memberikan pemahaman komprehensif mengenai peran hukum perlindungan data pribadi.

Rumusan masalah ini disusun untuk memberikan fokus analisis yang sistematis. Setiap rumusan masalah saling berkaitan dan membentuk satu kesatuan kajian, diharapkan mampu menjawab persoalan hukum secara komprehensif. Tujuan penelitian ini untuk menganalisis konsep perlindungan data pribadi dalam konteks hukum perbankan Indonesia. Selain itu, untuk mengkaji pengaturan hukum perlindungan data pribadi dalam menanggulangi kejahatan perbankan. Tujuan lainnya adalah menjelaskan urgensi perlindungan data pribadi sebagai instrumen hukum. Tujuan tersebut dirancang untuk memberikan kontribusi teoritis dan praktis. Kontribusi teoritis berupa pengembangan kajian hukum perlindungan data. Sementara itu, kontribusi praktis diharapkan berguna bagi regulator dan industri perbankan.

B. Metode Penelitian

Metode penelitian yang digunakan dalam penelitian ini adalah

metode yuridis normative dengan pendekatan yang digunakan yaitu metode pendekatan yuridis empiris. Metode penelitian yuridis normatif adalah penelitian hukum kepustakaan yang dilakukan dengan cara meneliti bahan-bahan kepustakaan. Penelitian ini dilakukan guna untuk mendapatkan bahan-bahan berupa teori-teori, konsep-konsep, serta peraturan hukum yang berhubungan dengan pokok bahasan. Ruang lingkup penelitian ini akan dilakukan penelitian dengan cara menafsirkan peraturan perundang-undangan dengan menganalisis Perlindungan Data Pribadi sebagai Instrumen Hukum dalam Menanggulangi Kejahatan Perbankan.

Spesifikasi dalam penelitian ini yaitu deskriptif analitis. Suatu penelitian yang berusaha menggambarkan masalah hukum, sistem hukum, peraturan perundang-undangan dan mengkajinya atau menganalisisnya sesuai dengan kenyataan. Peristiwa hukum yang berlaku pada saat tertentu tersebut sangat bergantung pada situasi dan dinamika masyarakat yang berkembang.

C. Hasil Penelitian dan Pembahasan

Konsep Data Pribadi dan Kejahatan Perbankan

Data pribadi dalam kajian hukum dipahami sebagai informasi yang merepresentasikan identitas individu dan memungkinkan seseorang dikenali secara langsung maupun tidak langsung. Informasi tersebut mencakup data identitas, data keuangan, hingga data perilaku digital. Dalam konteks masyarakat modern, data pribadi memiliki nilai strategis karena dapat dikapitalisasi secara ekonomi. Oleh sebab itu, data pribadi tidak lagi bersifat netral, melainkan memiliki dimensi kekuasaan dan kontrol. Dalam sektor perbankan, data pribadi menjadi fondasi utama layanan keuangan digital. Posisi strategis ini menjadikan data pribadi sebagai objek yang rentan terhadap penyalahgunaan (Nissenbaum, 2010, hlm. 2–5).

Dalam sistem perbankan, data pribadi nasabah mencakup informasi identitas, rekening, transaksi, dan profil risiko keuangan. Data tersebut diproses secara terus-menerus dalam sistem elektronik yang saling terhubung. Kompleksitas sistem ini meningkatkan efisiensi, namun

sekaligus membuka celah kerentanan keamanan. Semakin luas distribusi data, semakin tinggi pula risiko kebocoran dan akses ilegal. Kondisi ini menjadikan data pribadi sebagai target utama kejahatan perbankan modern. Oleh karena itu, perlindungan data harus dipahami sebagai kebutuhan struktural dalam perbankan (Acquisti, Taylor, & Wagman, 2016, hlm. 445–447).

Kejahatan perbankan kontemporer menunjukkan pergeseran dari kejahatan fisik ke kejahatan berbasis informasi. Pelaku kejahatan memanfaatkan data pribadi untuk mengakses rekening dan melakukan transaksi ilegal. Dalam konteks ini, data pribadi berfungsi sebagai sarana utama (*means*) terjadinya tindak pidana. Kejahatan semacam ini sering kali sulit dideteksi karena tidak melibatkan kekerasan fisik. Akibatnya, korban sering terlambat menyadari kerugian yang dialami. Fenomena ini menegaskan bahwa data pribadi telah menjadi instrumen kriminal (Brenner, 2013, hlm. 87–90).

Penyalahgunaan data pribadi dalam perbankan menimbulkan dampak multidimensional. Selain kerugian finansial, korban juga

mengalami kerugian psikologis dan hilangnya rasa aman. Kejahatan berbasis data sering kali bersifat lintas batas, sehingga menyulitkan penegakan hukum (Irawati, A. C., & da Silva, E. B. (2025). Hal ini menunjukkan bahwa kejahatan perbankan berbasis data memiliki karakter kompleks. Oleh karena itu, pendekatan hukum konvensional sering kali tidak memadai. Perlindungan data pribadi harus diposisikan sebagai bagian dari kebijakan kriminal modern (Wall, 2007, hlm. 56–58).

Dengan demikian, konsep data pribadi dalam perbankan tidak dapat dilepaskan dari dinamika kejahatan berbasis teknologi. Data pribadi telah berubah menjadi komoditas sekaligus alat kejahatan. Perlindungan data tidak hanya bersifat administratif, tetapi juga berkaitan langsung dengan pencegahan tindak pidana. Pendekatan hukum yang komprehensif menjadi kebutuhan mendesak. Hal ini menegaskan bahwa perlindungan data pribadi memiliki dimensi pidana, perdata, dan administrasi sekaligus Pengaturan Hukum Perlindungan Data Pribadi di Sektor Perbankan

Pengaturan perlindungan data dalam sektor perbankan secara historis berangkat dari kewajiban menjaga kerahasiaan informasi nasabah. Kerahasiaan ini merupakan bagian dari kepercayaan antara bank dan nasabah. Namun, regulasi awal perbankan lebih menekankan aspek kerahasiaan daripada pengelolaan data secara menyeluruh. Perkembangan teknologi mengubah pola pengolahan data menjadi lebih kompleks. Akibatnya, kerangka hukum lama menjadi kurang memadai. Hal ini menuntut pembaruan regulasi (Basel Committee on Banking Supervision, 2018, hlm. 3–5).

Rezim perlindungan data modern menempatkan bank sebagai pengendali data yang bertanggung jawab penuh atas pemrosesan data pribadi. Tanggung jawab ini mencakup pengamanan, akurasi, dan penggunaan data sesuai tujuan. Regulasi perlindungan data menuntut akuntabilitas yang lebih tinggi dari institusi perbankan. Bank tidak lagi hanya wajib merahasiakan data, tetapi juga wajib mengelolanya secara aman. Pendekatan ini mencerminkan pergeseran paradigma hukum. Perlindungan data

menjadi kewajiban aktif (European Union, 2016).

Di Indonesia, penguatan pengaturan tersebut diwujudkan melalui Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Undang-undang ini mengadopsi prinsip-prinsip global perlindungan data. Hak subjek data dan kewajiban pengendali data diatur secara eksplisit. Dalam sektor perbankan, ketentuan ini memperluas tanggung jawab bank. Bank wajib memastikan keamanan seluruh siklus pemrosesan data. Dengan demikian, UU PDP memperkuat sistem hukum perbankan (UU 27/ 2022).

UU PDP juga mengatur mekanisme sanksi administratif, perdata, dan pidana. Pengaturan sanksi ini mencerminkan pendekatan *deterrence* dalam hukum. Sanksi pidana digunakan sebagai upaya terakhir untuk mencegah pelanggaran serius. Dalam konteks perbankan, sanksi ini relevan karena kebocoran data dapat berdampak luas. Regulasi sanksi juga meningkatkan kepatuhan institusional. Oleh karena itu, pengaturan hukum perlindungan data memiliki fungsi represif yang jelas (BIS, 2021, hlm. 12–14).

Secara keseluruhan, pengaturan hukum perlindungan data di sektor perbankan mencerminkan respons hukum terhadap perkembangan teknologi. Hukum tidak lagi bersifat statis, melainkan adaptif. Perlindungan data menjadi bagian dari tata kelola perbankan yang baik. Hal ini menunjukkan integrasi antara hukum perbankan dan hukum perlindungan data. Dengan demikian, sistem hukum perbankan bergerak menuju model perlindungan yang komprehensif. Perlindungan Data Pribadi sebagai Instrumen Pencegahan Kejahatan Perbankan.

Perlindungan data pribadi berfungsi sebagai instrumen pencegahan kejahatan perbankan melalui penguatan keamanan sistem. Pencegahan dilakukan dengan mengurangi peluang terjadinya kejahatan. Sistem keamanan yang kuat mempersulit pelaku kejahatan mengakses data nasabah. Dengan demikian, perlindungan data memiliki fungsi preventif. Pendekatan ini sejalan dengan teori pencegahan kejahatan modern. Hukum digunakan untuk mengendalikan risiko (Clarke, 1997, hlm. 4–6).

Dalam perbankan, pencegahan dilakukan melalui standar keamanan dan kepatuhan regulasi. Kepatuhan ini menciptakan budaya kehati-hatian. Banyak kejahatan terjadi akibat kelalaian internal. Oleh karena itu, perlindungan data juga berfungsi sebagai mekanisme pengendalian organisasi. Pendekatan ini menekankan pentingnya tata kelola internal. Dengan demikian, pencegahan bersifat sistemik (BIS, 2021, hlm. 18–20).

Selain preventif, perlindungan data juga memiliki fungsi represif. Fungsi ini diwujudkan melalui penegakan hukum dan sanksi. Ancaman sanksi pidana menciptakan efek jera. Efek jera penting untuk mencegah pengulangan kejahatan. Dalam sektor perbankan, fungsi represif memperkuat kepatuhan. Oleh karena itu, perlindungan data berfungsi ganda (Ashworth, 2015, hlm. 56–58).

Pendekatan preventif dan represif harus berjalan seimbang. Pencegahan tanpa penegakan hukum akan lemah. Sebaliknya, penegakan hukum tanpa pencegahan akan bersifat reaktif. Perlindungan data pribadi memungkinkan keseimbangan tersebut. Dengan

demikian, perlindungan data menjadi instrumen kebijakan kriminal. Hal ini relevan dalam menghadapi kejahatan berbasis teknologi (Clarke, 1997, hlm. 21–23).

Melalui perlindungan data, sistem perbankan dapat meminimalkan risiko kejahatan. Risiko yang lebih rendah meningkatkan kepercayaan publik (Wijaya, H., & Irawati, A. C. (2025). Kepercayaan ini penting bagi stabilitas sistem keuangan. Oleh karena itu, perlindungan data memiliki nilai strategis. Instrumen hukum ini berkontribusi langsung pada pencegahan kejahatan perbankan (BIS, 2021, hlm. 25–27). **Urgensi Perlindungan Data Pribadi dalam Sistem Hukum Perbankan.**

Urgensi perlindungan data pribadi pertama-tama terlihat dari perlindungan hak nasabah. Hak atas data pribadi merupakan bagian dari hak atas privasi. Pelanggaran data dapat merugikan nasabah secara langsung. Oleh karena itu, perlindungan data merupakan bentuk perlindungan hukum konsumen (Irhamdessetya, H., Irawati, A. C., Wijaya, H., & Affandi, A. I. (2025). Negara berkewajiban menjamin hak tersebut. Hal ini menunjukkan urgensi

normatif (Nissenbaum, 2010, hlm. 101–103). Selain hak individu, perlindungan data juga berkaitan dengan kepentingan publik. Kejahatan perbankan berbasis data dapat merusak kepercayaan masyarakat. Kepercayaan merupakan fondasi sistem perbankan. Tanpa kepercayaan, stabilitas keuangan terganggu. Oleh karena itu, perlindungan data menjadi kebutuhan publik. Urgensinya bersifat sistemik (Basel Committee, 2018, hlm. 14–16).

Perlindungan data juga berkontribusi pada stabilitas ekonomi nasional. Risiko kejahatan perbankan dapat berdampak sistemik. Perlindungan data mengurangi risiko tersebut. Dengan demikian, perlindungan data memiliki dimensi makroekonomi. Negara berkepentingan menjaga stabilitas ini. Oleh karena itu, urgensi perlindungan data semakin kuat (BIS, 2021, hlm. 30–32). Perspektif hukum, perlindungan data mencerminkan perkembangan hukum responsif terhadap teknologi. Hukum dituntut untuk adaptif. Perlindungan data merupakan salah satu bentuk adaptasi tersebut. Tanpa perlindungan yang memadai, hukum

akan tertinggal. Oleh karena itu, urgensi pembaruan hukum tidak dapat diabaikan (*Wall, 2007, hlm. 201–203*).

Dengan demikian, urgensi perlindungan data pribadi dalam sistem hukum perbankan bersifat multidimensional. Perlindungan data menyangkut hak individu, kepentingan publik, dan stabilitas ekonomi. Tanpa perlindungan yang kuat, kejahatan perbankan akan terus berkembang. Oleh karena itu, perlindungan data harus menjadi prioritas kebijakan hukum. Hal ini menegaskan relevansi dan urgensi penelitian ini.

E. Kesimpulan

Data pribadi memiliki kedudukan strategis dalam sistem perbankan modern. Digitalisasi layanan perbankan telah menjadikan data pribadi nasabah sebagai fondasi utama operasional bank. Namun, kondisi tersebut sekaligus meningkatkan kerentanan terhadap kejahatan perbankan berbasis data. Kejahatan seperti pencurian identitas, *phishing*, dan penyalahgunaan data menunjukkan bahwa data pribadi telah menjadi sarana utama tindak pidana perbankan. perlindungan data

pribadi tidak dapat dipandang sebagai isu administratif semata. Perlindungan tersebut harus ditempatkan dalam kerangka hukum yang komprehensif. Konsep perlindungan data pribadi dalam hukum perbankan menunjukkan keterkaitan erat antara perlindungan hak nasabah dan pencegahan kejahatan. Data pribadi merupakan bagian dari hak atas privasi yang wajib dilindungi oleh negara. Dalam sektor perbankan, pelanggaran terhadap data pribadi berpotensi menimbulkan kerugian finansial dan psikologis bagi nasabah. Hal ini menunjukkan bahwa perlindungan data juga merupakan bentuk perlindungan konsumen jasa keuangan. Dengan demikian, perlindungan data pribadi memiliki dimensi hak asasi manusia dan kepentingan publik sekaligus.

Keberadaan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi memperkuat sistem hukum perbankan nasional. UU PDP melengkapi prinsip rahasia bank yang sebelumnya diatur dalam Undang-Undang Perbankan. Pengaturan mengenai hak subjek data, kewajiban pengendali data, serta sanksi

administratif, perdata, dan pidana memberikan dasar hukum yang lebih komprehensif. Dalam konteks perbankan, bank diposisikan sebagai pengendali data yang bertanggung jawab penuh atas keamanan data nasabah. Dengan demikian, UU PDP berfungsi sebagai instrumen hukum penting dalam menanggulangi kejahatan perbankan berbasis data. Perlindungan data pribadi juga terbukti memiliki fungsi preventif dan represif dalam penanggulangan kejahatan perbankan. Secara preventif, perlindungan data mendorong penguatan sistem keamanan informasi dan kepatuhan terhadap standar hukum. Secara represif, ancaman sanksi pidana dalam UU PDP menciptakan efek jera bagi pelaku pelanggaran data. Kombinasi kedua fungsi tersebut menjadikan perlindungan data pribadi sebagai instrumen kebijakan kriminal yang relevan. Dengan demikian, perlindungan data tidak hanya melindungi individu, tetapi juga berkontribusi pada stabilitas sistem perbankan dan kepercayaan publik.

Berikut saran dari penelitian ini:

Bagi Pemerintah

Optimalisasi implementasi Undang-Undang Nomor 27 Tahun

2022 tentang Perlindungan Data Pribadi, khususnya di sektor perbankan. Penguatan tersebut dapat dilakukan melalui penyusunan peraturan pelaksana yang lebih teknis dan adaptif terhadap perkembangan teknologi digital perbankan. Selain itu, diperlukan kejelasan pembagian kewenangan antarotoritas yang berwenang dalam pengawasan perlindungan data pribadi. Koordinasi antara otoritas perbankan dan lembaga perlindungan data menjadi penting untuk mencegah tumpang tindih kewenangan. Dengan regulasi dan pengawasan yang kuat, perlindungan data pribadi dapat berfungsi optimal sebagai instrumen pencegahan kejahatan perbankan.

Bagi Pengawas Sektor Keuangan

Otoritas pengawas sektor keuangan, khususnya perbankan, disarankan meningkatkan fungsi pengawasan terhadap pengelolaan data pribadi nasabah. Pengawasan tidak hanya difokuskan pada kepatuhan formal, tetapi juga pada efektivitas sistem keamanan informasi yang diterapkan oleh bank. Otoritas perlu mendorong penerapan prinsip kehati-hatian dan manajemen

risiko data secara berkelanjutan. Penting untuk mendeteksi potensi pelanggaran sejak dini dan mencegah terjadinya kejahatan perbankan berbasis data.

Bagi Perbankan

Perlindungan data pribadi sebagai bagian integral dari tata kelola perusahaan yang baik (*good corporate governance*). Bank perlu meningkatkan investasi pada sistem keamanan teknologi informasi serta memperkuat kebijakan internal terkait pengelolaan data. Peningkatan kapasitas dan kesadaran sumber daya manusia mengenai perlindungan data. Membangun budaya kepatuhan dan tanggung jawab terhadap perlindungan data nasabah.

Bagi Penegak Hukum

Penegakan hukum terhadap pelanggaran data pribadi harus dilakukan secara konsisten untuk menciptakan efek jera. Aparat penegak hukum perlu mengembangkan pendekatan yang adaptif terhadap karakter kejahatan berbasis teknologi. Kerja sama lintas lembaga dan lintas negara juga menjadi penting mengingat kejahatan data sering bersifat transnasional. Dengan penegakan hukum yang

efektif, perlindungan data pribadi dapat berfungsi secara optimal sebagai instrumen represif.

Bagi Akademisi

Kajian empiris mengenai efektivitas penerapan perlindungan data pribadi di sektor perbankan. Difokuskan pada studi kasus kebocoran data atau penegakan hukum atas pelanggaran data pribadi. Pendekatan multidisipliner yang menggabungkan aspek hukum, teknologi, dan ekonomi akan memberikan gambaran yang lebih komprehensif.

DAFTAR PUSTAKA

- Acquisti, A., Taylor, C., & Wagman, L. (2016). The economics of privacy. *Journal of Economic Literature*, 54(2), 442–492. <https://doi.org/10.1257/jel.54.2.42>
- Ali, A. (2015). *Menguak teori hukum*. Kencana.
- Ashworth, A. (2015). *Sentencing and criminal justice* (6th ed.). Cambridge University Press.
- Bank for International Settlements. (2021). *Principles for operational resilience*. BIS.
- Basel Committee on Banking Supervision. (2018). *Cyber-*

- resilience: Range of practices. Bank for International Settlements.
- Brenner, S. W. (2013). *Cybercrime and the law: Challenges, issues, and outcomes*. Northeastern University Press.
- Clarke, R. V. (1997). *Situational crime prevention*. Harrow and Heston.
- European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation)*. Official Journal of the European Union.
- Gunawan, C., & Irawati, A. C. (2025). Penerapan Prinsip Proses Hukum yang Adil dalam Investigasi Tindak Pidana dalam Transaksi E-Commerce. *Iuris Studia: Jurnal Kajian Hukum*, 6(3), 935-942.
- Irhamdessetya, H., Irawati, A. C., Wijaya, H., & Affandi, A. I. (2025). Peran Advokat Dalam Menjamin Due Process of Law Pada Perkara Penipuan Ekonomi (Pasal 379a KUHP): Refleksi Atas Sinergi dan Integritas Catur Wangsa Penegak Hukum. *Semarang Law Review (SLR)*, 6(2), 441-456.
- Irawati, A. C., Wijaya, H., & Pratama, A. (2025). Comparing Data Protection and Due Process Implementation in Indonesia. *Jurnal Ilmiah Dunia Hukum*, 9(2), 18-36.
- Irawati, A. C., & da Silva, E. B. (2025). Beyond Formality in Indonesian Pretrial Law: KUHAP Reform, Human Rights, and Islamic Law. *Al-Ahkam*, 35(2), 261-286.
- Kuner, C. (2017). The European Union and the search for an international data protection framework. *Groningen Journal of International Law*, 5(2), 55-76.
- Marzuki, P. M. (2017). *Penelitian hukum* (Edisi revisi). Kencana.
- Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.
- OECD. (2013). *The OECD privacy framework*. OECD Publishing.
- Siregar, A. N., & Putra, M. A. P. (2023). Perlindungan hukum data pribadi nasabah dalam layanan perbankan digital. *Jurnal Hukum IUS QUIA IUSTUM*, 30(2), 215-232.

Solove, D. J. (2021). *Understanding privacy* (2nd ed.). Harvard University Press.

Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age*. Polity Press.

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, 4(5), 193–220.

Wijaya, H., & Irawati, A. C. (2025). Konsturksi Hukum Pidana Bagi Pelaku Penyalahgunaan Kartu Kredit. *JURNAL ILMIAH HUKUM DAN DINAMIKA MASYARAKAT*, 23(1), 55-68.

Peraturan Perundang-Undangan

Republik Indonesia. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan*