

Analisis Yuridis Perlindungan Nasabah Bank Dalam Tindak Pidana Pencurian Data Melalui UU ITE dan UU Perbankan

Nayla Putri Abdullah¹ Natasya Yadila² Sabina Putri Amelia³ Alisha Reva Widiastiw⁴ Garneta Rizka Camilla⁵

¹⁻⁵Fakultas Hukum Universitas Pembangunan Nasional “Veteran” Jakarta
Email : 2210611091@mahasiswa.upnvj.ac.id¹, 2210611093@mahasiswa.upnvj.ac.id²,
2210611103@mahasiswa.upnvj.ac.id³, 2210611107@mahasiswa.upnvj.ac.id⁴,
2210611110@mahasiswa.upnvj.ac.id⁵

Abstract

Penelitian ini membahas isu perlindungan data pribadi dalam sektor perbankan Indonesia, yang menjadi semakin penting seiring perkembangan teknologi digital dan meningkatnya ancaman kejahatan siber. Penelitian dilakukan dengan menggunakan metode analisis yuridis normatif, yang mencakup kajian literatur, regulasi, dan kebijakan, seperti UU ITE dan UU Perbankan. Hasil penelitian menunjukkan bahwa, Meski telah ada regulasi, seperti UU ITE, UU Perbankan, dan POJK, penerapannya dinilai belum cukup efektif. Salah satu regulasi yang relevan adalah Pasal 26 ayat (1) UU ITE, yang mengatur bahwa penggunaan data pribadi dalam media elektronik harus mendapat persetujuan pemilik data, dan pelanggaran terhadap ketentuan ini dapat mengakibatkan gugatan perdata. Selain itu, bank diwajibkan menjaga kerahasiaan informasi nasabah sesuai standar keamanan yang memadai, sebagaimana diatur dalam Pasal 47 ayat (2) UU No. 10 Tahun 1998 tentang Perbankan. Regulasi ini dilengkapi dengan sanksi tegas berupa denda hingga Rp1 miliar atau pidana penjara hingga 8 tahun untuk pelaku pelanggaran. Permasalahan utama meliputi rendahnya tingkat kepatuhan lembaga keuangan terhadap standar keamanan, kurangnya literasi digital masyarakat, serta tantangan teknis dalam pengawasan dan penegakan hukum.

Abstrak

This study discusses the issue of personal data protection in the Indonesian banking sector, which is becoming increasingly important as digital technology advances and cybercrime threats increase. The study was conducted using a normative legal analysis method, which includes a review of literature, regulations, and policies, such as the ITE Law and the Banking Law. The results of the study indicate that, although there are regulations, such as the ITE Law, the Banking Law, and POJK, their implementation is considered ineffective. One of the relevant regulations is Article 26 paragraph (1) of the ITE Law, which stipulates that the use of personal data in electronic media must obtain the consent of the data owner, and violations of this provision can result in civil lawsuits. In addition, banks are required to maintain the confidentiality of customer information in accordance with adequate security standards, as stipulated in Article 47 paragraph (2) of Law No. 10 of 1998 concerning Banking. This regulation is equipped with strict sanctions in the form of fines of up to IDR 1 billion or imprisonment of up to 8 years for perpetrators of violations. The main problems include the low level of compliance of financial institutions with security standards, the lack of digital literacy of the community, and technical challenges in supervision and law enforcement.



<https://doi.org/10.5281/zenodo.14382558>

This is an open-access article under the [CC-BY-SA License](#).



PENDAHULUAN

Kemajuan teknologi sangat membantu manusia dalam melakukan berbagai tugas. Kita mengalami kemajuan ini setiap hari, contohnya adalah telepon seluler yang sering digunakan untuk komunikasi jarak jauh. Hadirnya internet telah memfasilitasi kemajuan teknologi yang memungkinkan individu di Indonesia dan sekitarnya untuk merasakan dampaknya. Evolusi internet menjadi semakin canggih, menampilkan berbagai aplikasi yang sangat membantu dalam memungkinkan berbagai aktivitas bagi banyak individu. Pengaruh teknologi informasi, media, komunikasi, dan sistem elektronik sangat menguntungkan untuk mengubah perilaku di seluruh dunia. Sistem yang dimaksud adalah perangkat keras.

Kegagalan dan kesalahan dalam teknologi informasi dan sistem elektronik terkadang berasal dari langkah-langkah keamanan yang tidak memadai yang dirancang untuk melindungi data pribadi pelanggan yang telah mendaftar di platform daring. perangkat lunak komputer, jaringan telekomunikasi, dan sistem komunikasi elektronik.¹

Meskipun demikian, tampaknya kemajuan ini dibarengi dengan berbagai permasalahan hukum terkait kejahatan informasi dan transaksi elektronik dalam sektor perbankan, yang jika tidak ditangani secara memadai, niscaya akan berdampak buruk bagi bank, masyarakat, dan nasabah.

Dalam sistem implementasinya, teknologi informasi dan komunikasi berfungsi sebagai pedang bermata dua. Teknologi informasi menawarkan berbagai keuntungan untuk meningkatkan kebahagiaan dan peradaban manusia, serta memajukan layanan publik dan internal dalam industri jasa. Sebaliknya, teknologi informasi dimanfaatkan oleh oknum yang tidak bertanggung jawab untuk melakukan tindakan ilegal yang melanggar kepentingan hukum individu, masyarakat, dan negara.²

Kejahatan tidak hanya mencakup tindakan ilegal tetapi juga melanggar hak sosial, ekonomi, dan beberapa hak lainnya. Pelanggaran hukum juga terkait dengan penyalahgunaan dan penyalahgunaan inovasi teknologi canggih. Munculnya pelanggaran yang terkait dengan teknologi modern umumnya disebut kejahatan dunia maya.

Pencurian data elektronik, yang umumnya disebut phishing, melibatkan perolehan informasi pribadi secara ilegal, termasuk ID Pengguna, PIN, nomor rekening bank, dan nomor kartu kredit. Informasi ini kemudian akan dimanfaatkan oleh penipu untuk menyusup ke akun, melakukan penipuan kartu kredit, atau memanipulasi pengguna agar mentransfer dana ke akun tertentu dengan dalih penghargaan.

Hukum berfungsi untuk melindungi kepentingan manusia. Untuk melindungi kepentingan manusia, hukum harus ditegakkan. Perlindungan hukum mengacu pada perlindungan yang diberikan oleh hukum atau peraturan perundang-undangan untuk menegakkan kepentingan manusia, sehingga memfasilitasi perkembangan kehidupan manusia yang normal dan damai.

Kitab Undang-Undang Hukum Pidana memuat ketentuan umum mengenai hukum siber. Dalam peraturan perundang-undangan di Indonesia berlaku asas *Lex Specialis derogat legi Generalis* yang berarti peraturan perundang-undangan yang bersifat khusus menggantikan peraturan perundang-undangan yang bersifat umum. Secara khusus, Indonesia telah memiliki peraturan perundang-undangan yang mengatur hukum siber di bidang perbankan, yaitu Undang-Undang Informasi dan Transaksi Elektronik Nomor 11 Tahun 2008 yang diubah dengan Undang-Undang Nomor 19 Tahun 2016, Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan Atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan, serta Undang-Undang (UU) Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (PDP). Adanya perlindungan hukum bagi nasabah memberikan rasa aman kepada nasabah terkait dengan eksploitasi data pribadinya.³ Selain itu ada juga, Peraturan Otoritas Jasa Keuangan, dan berbagai aturan lain yang dibutuhkan untuk mencegah cybercrime.

Oleh karena itu peneliti tertarik untuk meneliti sejauh mana UU ITE dan UU Perbankan dapat melindungi nasabah selain itu juga bagaimana peran ojk dalam melindungi nasabah dengan judul penelitian “Analisis Yuridis Perlindungan Nasabah Bank Dalam Tindak Pidana Pencurian Data Melalui UU ITE Dan UU Perbankan”

METODE

Dalam penelitian ini penulis menggunakan metode penelitian hukum normatif. Oleh karena itu sifat penelitian ini adalah kepustakaan (library research), artinya sebuah studi dengan mengkaji buku-buku atau kitab-kitab terkait dengan artikel ini yang berasal dari perpustakaan (bahan pustaka) yang berkaitan dengan tema yang diangkat. Dalam metode normatif ini, pendekatan hukum yang

¹ Kusuma, A. C., & Rahmani, A. D. (2022). Analisis Yuridis Kebocoran Data Pada Sistem Perbankan Di Indonesia (Studi Kasus Kebocoran Data Pada Bank Indonesia). *SUPREMASI: Jurnal Hukum*, 5(1), 46-63.

² Adam Chazawi. Tindak Pidana Informasi Dan Transaksi Elektronik. Malang: Media Nusa Crative, 2015.

³ Triputri, D. H., Mofea, S., Yulviani, D., & Pratama, R. (2023). Analisis Yuridis Terhadap Penerapan Sanksi Pidana Bagi Pelaku Penipuan Dalam Transaksi Elektronik Berdasarkan Asas *Lex Specialis Derogat Legi Generali* Ditinjau Dari Kuhp Dan UU ITE. *Lex Veritatis*, 2(01), 42-51.

digunakan adalah pendekatan perundang-undangan atau yang biasa dikenal sebagai statute approach. Sumber data yang digunakan adalah sumber data sekunder yang terdiri dari sumber bahan hukum primer berupa peraturan perundang-undangan terkait kebocoran data, bahan hukum sekunder berupa buku-buku dan jurnal terkait temapenelitian

HASIL DAN PEMBAHASAN

Hukum Di Indonesia Yang Mengatur Terkait Perlindungan Data Pribadi Nasabah Bank Dalam Kasus Pencurian Data Pribadi Berdasarkan UU ITE Dan UU PERBANKAN

Di Indonesia, pelanggaran terhadap hak privasi melalui penyalahgunaan data pribadi masih marak, khususnya di sektor perbankan. Praktik pertukaran data nasabah secara bebas antar pusat kartu kredit, pengungkapan informasi transaksi kepada pihak yang tidak berwenang, serta perdagangan data nasabah baik di antara lembaga perbankan maupun melalui pihak ketiga yang tidak bertanggung jawab, merupakan contoh nyata dari pelanggaran tersebut.⁴

Pentingnya perlindungan hukum terhadap data pribadi semakin mendapat perhatian seiring dengan peningkatan jumlah pengguna telepon seluler dan internet. Berbagai kasus yang mencuat, terutama yang berkaitan dengan kebocoran data pribadi yang berujung pada penipuan atau tindak kriminal seperti pornografi, semakin memperkuat urgensi penyusunan regulasi hukum untuk melindungi data pribadi. Perlindungan data pribadi berhubungan erat dengan konsep privasi, yang pada dasarnya merupakan upaya menjaga martabat dan integritas individu secara pribadi.⁵ Konsep privasi, yang sering diasosiasikan dengan negara-negara maju, merujuk pada hak fundamental individu untuk menjaga kehidupan pribadi dari campur tangan yang tidak sah.⁶

Permasalahan penyalahgunaan data pribadi telah menjadi fenomena global, termasuk di Indonesia. Kasus-kasus yang telah tercatat merupakan representasi dari ribuan kasus pelanggaran privasi yang terjadi. Permasalahan pencurian data pribadi menuntut adanya perlindungan hukum yang lebih komprehensif. Regulasi yang berlaku saat ini, meskipun telah ada, dinilai belum cukup memadai untuk melindungi hak privasi individu. Saat ini undang-undang yang digunakan untuk melindungi data pribadi yaitu Undang-Undang pada Pasal 7914 ayat (1) Undang-Undang Nomor 24 Tahun 2013 Tentang Perubahan atas Undang-Undang Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan (UU Administrasi Kependudukan), Pasal 5815 Peraturan Pemerintah Nomor 37 Tahun 2007 tentang Pelaksanaan Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan (PP Administrasi Kependudukan), dan Pasal 26 ayat (1)16 Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.⁷

Undang Undang Republik Indonesia No. 19 Tahun 2016 tentang Perubahan atas Undang-Undang Republik Indonesia Nomor 11 Tahun 2011 tentang Informasi dan Transaksi Elektronik (Selanjutnya disebut “UU ITE”), meliputi perlindungan dari penggunaan tanpa izin, perlindungan oleh penyelenggara sistem elektronik, dan perlindungan dari akses ilegal. sebagai UU generik memuat norma perlindungan data pribadi pada Pasal 26, UU ITE mengatur berbagai hal terkait perlindungan data pribadi, termasuk larangan penggunaan data tanpa izin dan kewajiban penyelenggara sistem elektronik untuk melindungi data pengguna. UU ini juga menetapkan bahwa penggunaan data pribadi harus didasarkan pada prinsip persetujuan pemilik data atau aturan hukum yang berlaku. Pada dasarnya ketentuan ini memuat dua dasar legitimasi pemrosesan data pribadi yaitu (a) consent/persetujuan; dan (b) norma hukum positif. Kedua prinsip ini adalah dasar lawful data processing.

Pasal 26 Undang-Undang ITE mengatur bahwa penggunaan data pribadi dalam media elektronik harus mendapatkan persetujuan dari pemilik data. Pelanggaran terhadap ketentuan ini dapat mengakibatkan gugatan perdata. Selain itu, UU ini juga mewajibkan penyedia layanan internet untuk menghapus data pribadi pengguna atas permintaan yang bersangkutan.

⁴ Siti Yuniarti, “PERLINDUNGAN HUKUM DATA PRIBADI DI INDONESIA,” JURNAL BECOSS Vol.1, No. (2019): 148.

⁵ Wahyudi Djafar dan Asep Komarudin, *Perlindungan Hak Atas Privasi Di Internet-Beberapa Penjelasan Kunci*(jakarta: Elsam, 2014), 2.

⁶ Rosalinda Elsin Latumahina, “Aspek Hukum Perlindungan Data Pribadi Di Dunia Maya,” Jurnal GEMA AKTUALITA 3, no. 2 (2014): hal 17.

⁷ Rumlus, M. H., & Hartadi, H. (2020). Kebijakan penanggulangan pencurian data pribadi dalam media elektronik. *Jurnal Ham*, 11(2), 285-299.

Setiap orang yang melanggar ketentuan ini dapat digugat atas kerugian yang ditimbulkan. Ketentuan Pasal 26 UU ITE adalah sebagai berikut:

1. Kecuali ditentukan lain oleh peraturan perundang-undangan, penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan.
2. Setiap orang yang melanggar haknya sebagaimana yang dimaksud pada ayat 1 dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan undang-undang ini.
3. Setiap penyelenggara sistem elektronik wajib menghapus informasi elektronik dan/atau dokumen elektronik yang tidak relevan yang berada di bawah kendalinya atas permintaan orang yang bersangkutan berdasarkan penetapan pengadilan.
4. Setiap penyelenggara sistem elektronik wajib menyediakan mekanisme penghapusan informasi elektronik dan/atau dokumen elektronik yang tidak relevan sesuai dengan ketentuan peraturan perundang-undangan.
5. Ketentuan mengenai tata cara penghapusan informasi elektronik dan/atau dokumen elektronik sebagaimana dimaksud pada ayat (3) dan ayat (4) diatur dalam peraturan pemerintah.

Pemerintah mengakui bahwa data pribadi memiliki nilai ekonomi yang tinggi. Oleh karena itu, Undang-Undang ITE melarang penggunaan data pribadi tanpa izin pemiliknya. Pelanggaran terhadap aturan ini dapat dianggap sebagai pencurian dan dapat dituntut secara hukum. Dalam penjelasannya Pasal 26 UU ITE juga menyatakan bahwa data pribadi merupakan salah satu bagian dari hak pribadi seseorang.⁸ Hal ini dinyatakan dalam pasal 26 UU ITE bahwa setiap orang dapat melakukan gugatan terhadap perolahan data pribadi tanpa persetujuannya.

Pasal 28G UUD 1945 memberikan kita hak untuk melindungi data pribadi. Untuk mewujudkan hak ini, kita perlu memiliki kebijakan yang kuat dan komprehensif dalam mencegah pencurian data. Dengan begitu, pemanfaatan data dapat dilakukan dengan aman dan bertanggung jawab, sangat dibutuhkan untuk menentukan langkah-langkah yang pasti dalam proses pengamanan. Selain itu Peraturan Perundang-undangan memiliki efek memaksa agar data dan informasi tersebut dapat dilindungi sebagaimana mestinya.⁹

Lebih lanjut juga dijelaskan di dalam Pasal 30 UU ITE, diatur bahwa siapa pun yang secara sengaja dan tanpa hak mengakses sistem elektronik, seperti sistem perbankan, dengan tujuan memperoleh informasi elektronik atau dokumen, termasuk data pribadi nasabah, dapat dijatuhi pidana penjara hingga 6–8 tahun dan/atau denda hingga Rp600 juta–Rp800 juta.¹⁰

Lebih lanjut, Pasal 34 UU ITE memperketat sanksi terhadap pelaku kejahatan yang memanfaatkan data hasil retasan, seperti memperjualbelikan atau mendistribusikan data pribadi nasabah. Mereka dapat dijatuhi pidana berdasarkan Pasal 45 dengan ancaman hukuman penjara maksimal 6 tahun dan/atau denda hingga Rp1 miliar.

Aturan ini menegaskan pentingnya perlindungan data pribadi dalam sektor perbankan, mengingat data nasabah sering menjadi target utama pelaku kejahatan untuk digunakan dalam aksi penipuan, pencurian identitas, atau tindak kriminal lainnya. Dengan regulasi ini, nasabah memiliki payung hukum yang jelas untuk melindungi hak privasi dan keamanan data mereka, sementara bank wajib memastikan sistem mereka sesuai dengan standar keamanan yang memadai.

Pasal 1 Angka 1 UU Nomor 10 Tahun 1998 mendefinisikan perbankan sebagai segala sesuatu yang berhubungan atau menyangkut tentang bank baik dilihat secara kelembagaan, kegiatan usaha serta cara dan proses dalam menjalankan kegiatan usahanya. Ketentuan hukum yang dapat digunakan untuk menetapkan dan memberikan perlindungan hukum dalam penyelenggaraan layanan internet banking dapat dicermati pada Pasal 29 ayat (4) UU Nomor 10 Tahun 1998 yang menyatakan bahwa bank berkewajiban untuk menyediakan dan menyampaikan informasi mengenai kemungkinan adanya risiko kerugian terkait dengan transaksi nasabah yang dilakukan oleh bank demi tercapainya

⁸ Human Rights Committee General Comment No. 17, On the Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, 1988, 17.

⁹ Suari, K. R. A., & Sarjana, I. M. (2023). Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia. *Jurnal Analisis Hukum*, 6(1), 132-142.

¹⁰ Aditama C.K dan Ayu Diah R. (2022). Analisis Yuridis Kebocoran Data Pada Sistem Perbankan Di Indonesia (Studi Kasus Kebocoran Data Pada Bank Indonesia). *SUPREMASI: Jurnal Hukum*, 5(1), 46-63.

kepentingan nasabahnya. Pada permasalahan perlindungan hukum terhadap kerugian nasabah akibat error system, penerapan peraturan ini wajib untuk dilakukan oleh bank secara pro aktif dalam memberikan informasi-informasi sehubungan dengan risiko kerugian atas pemanfaatan layanan bank oleh nasabah.¹¹

Sementara itu, menurut Pasal 47 ayat (2) Undang- undang No.10 Tahun 1998 Tentang Perbankan, yang berkewajiban memegang teguh rahasia bank adalah:

- a. Anggota Dewan Komisaris Bank
- b. Anggota Direksi Bank
- c. Pegawai Bank
- d. Pihak terafiliasi lainnya dari Bank

Ketentuan pelaksanaan dari rahasia bank dalam Undang-Undang Perbankan, untuk melindungi kerahasiaan dan keamanan data pribadi nasabah Lembaga Otoritas Jasa Keuangan menerbitkan Peraturan Otoritas Jasa Keuangan (POJK) Nomor 1/ POJK.07/2013 Tahun 2013 Tentang Perlindungan Konsumen Sektor Jasa Keuangan.¹² Peraturan POJK ini, dalam Pasal 31 ayat (1) dan (2) ditentukan bahwa pelaku usaha jasa keuangan dilarang dengan cara apapun memberikan data dan/atau informasi mengenai konsumennya kepada pihak ketiga. Larangan tersebut dikecualikan dalam hal:

- a. Konsumen memberikan persetujuan tertulis; dan/atau
- b. Diwajibkan oleh peraturan perundang-undangan.

Ketentuan Pasal 47 ayat (2) UU No.7 Tahun 1992 Tentang Perbankan, memuat ketentuan bahwa pembocoran adalah sengaja memberikan keterangan yang wajib dirahasiakan. Sedangkan pada ayat (2)-nya dimuat ketentuan mengenai pembocoran rahasia bank dikarenakan adanya paksaan. Si pemaksa dengan sengaja tanpa membawa perintah tertulis dari Menteri Keuangan atau izin Menteri Keuangan. Penerima bocoran rahasia bank tidaklah dapat dikategorikan sebagai pelaku penadahan, baik dilihat dari segi teori materiil maupun dari teori formal.

Peran Lembaga Pengawasan Seperti Otoritas Jasa Keuangan (OJK) Dalam Mencegah Dan Menanggulangi Tindak Pidana Pencurian Data Pribadi Nasabah Bank

Berdasarkan Undang-Undang Nomor 21 Tahun 2011 tentang Otoritas Jasa Keuangan, Otoritas Jasa Keuangan (OJK) merupakan organisasi independen yang mempunyai kewenangan mengawasi dan mengatur seluruh kegiatan sektor jasa keuangan Indonesia secara komprehensif. Hal ini mencakup pasar modal, perbankan, dan sektor jasa keuangan non-bank lainnya seperti asuransi, dana pensiun, lembaga pembiayaan, dan lembaga jasa keuangan lainnya.¹³ Di era digital, penyebaran data yang tidak disetujui tentu menimbulkan risiko yang signifikan dan dapat mengikis kepercayaan konsumen terhadap organisasi jasa keuangan. Bank sendiri diakui mempunyai kewajiban untuk menjaga informasi pribadi nasabahnya, termasuk transaksi keuangan dan identifikasi. Dalam hal ini, OJK tentu saja berperan sebagai pengawas dan regulator yang bertugas mencegah bank-bank yang lalai membocorkan dan menyalahgunakan data konsumen.¹⁴

Peran lembaga pengawasan seperti Otoritas Jasa Keuangan (OJK) dalam mencegah dan menanggulangi tindak pidana pencurian data pribadi nasabah bank sangat penting dalam menjaga integritas sistem perbankan dan kepercayaan publik terhadap lembaga keuangan di Indonesia. Dalam hal hukum perbankan, perlindungan terhadap data pribadi nasabah menjadi salah satu aspek yang sangat diperhatikan, mengingat banyaknya ancaman yang muncul seiring dengan pesatnya perkembangan teknologi digital dan penggunaan sistem perbankan elektronik. Sebagai lembaga yang berwenang mengawasi dan mengatur sektor jasa keuangan, OJK memiliki tanggung jawab besar dalam menciptakan dan memastikan lingkungan perbankan yang aman, transparan, dan dapat

¹¹ Alamudi, I. A. A. I. A. (2023). Analisis Perundang-undangan: Kajian Kritis Undang-Undang Perbankan Syariah. *Qonun Iqtishad EL Madani Journal*, 2(2), 30-38.

¹² Putra, R. D., Sinlae, E. S. P., Syafa, T. S., Syahda, I. F., & Siswajanthy, F. (2024). Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang Dalam Perbankan. *Al-Zayn: Jurnal Ilmu Sosial & Hukum*, 2(1), 70-80.

¹³ Muhammad Tazil Ramadhan and Diana Wiyanti, "Peran Otoritas Jasa Keuangan Dalam Mengawasi Kegiatan Lembaga Bank Berdasarkan Undang-Undang Otoritas Jasa Keuangan Nomor 21 Tahun 2011 Dan Undang-Undang Perbankan Nomor 10 Tahun 1998 Terkait," *Bandung Conference Series: Law Studies*4, No. 1 (2024): 766–74, <https://doi.org/10.29313/Bcsls.V4i1.12484>.

¹⁴ Ruth Devisa Br Sukatendel, "Peran Otoritas Jasa Keuangan Terhadap Tindak Pidana Penyebaran Data Pribadi Oleh Perusahaan Financial Technology," 2021.

dipercaya. Salah satu fokus utama OJK adalah memastikan bahwa lembaga perbankan mematuhi berbagai ketentuan yang terkait dengan perlindungan data pribadi nasabah sesuai dengan peraturan yang berlaku, termasuk Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan UU Perbankan.

Sebagaimana dalam Pasal 30 Undang-Undang Nomor 21 Tahun 2011 tentang Otoritas Jasa Keuangan yang menjadi landasan hukum tanggung jawab OJK dalam melindungi konsumen, menguraikan secara rinci bagaimana OJK mengawasi dan mengendalikan berbagai operasional organisasi jasa keuangan untuk menjamin keamanan konsumen. Terkait kebocoran data di era digital, OJK mempunyai kewenangan untuk mengajukan gugatan atas nama nasabah yang dirugikan dan menuntut ganti rugi kepada bank yang melanggar undang-undang perlindungan data pribadi di industri jasa keuangan. Salah satu akibat potensial dari pelanggaran ini adalah data tersebut dapat digunakan oleh pihak ketiga yang nantinya bertanggung jawab.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) juga turut memuat peraturan perundang-undangan tentang perlindungan konsumen selain Undang-Undang Nomor 21 Tahun 2011. UU PDP sendiri merupakan undang-undang yang menjamin hak masyarakat dalam menjaga informasi pribadinya. Peraturan perundang-undangan ini memuat sejumlah pasal yang dijadikan acuan perlindungan informasi pribadi seseorang. Karena memungkinkan seseorang untuk mengontrol informasi yang dimiliki oleh pihak ketiga, Pasal 7 UU PDP menjelaskan bahwa subyek kekuasaan pribadi berhak mengakses dan memperoleh salinan data pribadi tentang dirinya. Ini pun adalah hak yang krusial dalam hal perlindungan data pribadi dan privasi individu. Hak ini memberikan jaminan kepada masyarakat bahwa mereka akan mengetahui informasi apa yang telah dikumpulkan tentang mereka, bagaimana informasi tersebut akan digunakan, dan mengapa informasi tersebut akan diproses.

Selain Pasal 7, Pasal 12 UU PDP mengatur tugas pemerintah untuk memberikan pengamanan yang efisien terhadap informasi pribadi seseorang dan menjamin agar tidak disalahgunakan. Dengan kata lain, pemerintah perlu memastikan bahwa terdapat aturan, proses, dan sistem yang dapat mencegah penyalahgunaan dan kebocoran informasi pribadi oleh pihak ketiga, yang dapat merugikan masyarakat.¹⁵ Selain diatur dalam undang-undang, Peraturan Otoritas Jasa Keuangan Nomor 22 Tahun 2023 tentang Perlindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan juga mengatur tentang perlindungan konsumen di industri jasa keuangan. Hal ini terutama terlihat pada Pasal 3 ayat (2) huruf d yang menyatakan bahwa Pelaku Usaha Jasa Keuangan (PUJK) harus menerapkan prinsip perlindungan aset konsumen yang menitikberatkan pada perlindungan keamanan finansial konsumen dari berbagai risiko yang dapat membahayakan kekayaan atau asetnya.

Selain itu, pasal ini menjelaskan cara menjaga privasi dan data pelanggan, menekankan perlunya PUJK mengutamakan keamanan dan kerahasiaan data pribadi konsumen. Perlindungan ini tentu diperlukan, terutama mengingat kemajuan teknologi digital yang memudahkan pengumpulan dan pengelolaan data pribadi. Perlindungan data juga diatur dalam Pasal 19 yang menyatakan bahwa PUJK harus berpegang pada dasar-dasar pengolahan perlindungan data pribadi guna melindungi kerahasiaan informasi konsumen, termasuk identitas lengkap individu dan korporasi. Pelanggar hukum yang menyebarkan informasi konsumen atau data pribadi untuk tujuan selain yang diatur dalam peraturan perundang-undangan atau peraturan perundang-undangan lainnya dikenakan denda paling banyak Rp15.000.000.000.000,00 (lima belas miliar rupiah).

OJK berperan sebagai pengawas yang memonitor penerapan kebijakan dan prosedur yang dilakukan oleh bank terkait dengan perlindungan data pribadi nasabah. Pengawasan ini mencakup aspek teknis, seperti sistem keamanan digital yang digunakan oleh bank, serta prosedur internal yang dilakukan oleh bank dalam mengelola dan melindungi data pribadi nasabah dari potensi ancaman, termasuk pencurian data oleh pihak yang tidak bertanggung jawab. Selain itu, OJK juga memiliki kewenangan untuk memberikan sanksi terhadap lembaga perbankan yang tidak mematuhi peraturan perlindungan data pribadi. Sanksi tersebut dapat berupa teguran, denda, atau bahkan pencabutan izin

¹⁵ Kurniawan. Ananta, Fadli Sutarli. Shelly, "Peranan Pemerintah Melalui Undang-Undang Perlindungan Data Pribadi Dalam Menanggulangi Phising Di Indonesia," *Journal Of Social Science Research*3 (2023): 176–176, <https://doi.org/10.5040/9781635577068-0537>.

operasional bank jika terbukti melakukan kelalaian yang dapat merugikan nasabah atau masyarakat luas. Dengan demikian, OJK berfungsi sebagai lembaga yang memberi efek jera kepada bank yang tidak berupaya melindungi data pribadi nasabah dengan baik.

Dalam upaya mencegah tindak pidana pencurian data pribadi, OJK mengembangkan berbagai pedoman dan regulasi yang harus diikuti oleh lembaga perbankan. Salah satu peraturan yang sangat relevan adalah kewajiban bagi bank untuk menerapkan sistem keamanan yang memadai dalam transaksi elektronik dan pengelolaan data pribadi nasabah. OJK memastikan bahwa setiap bank melakukan evaluasi terhadap sistem keamanan mereka secara berkala untuk mengidentifikasi dan mengatasi potensi celah yang dapat dimanfaatkan oleh pelaku kejahatan siber. OJK juga berperan dalam memberikan pelatihan dan sosialisasi kepada lembaga perbankan mengenai pentingnya perlindungan data pribadi. Melalui berbagai program edukasi, OJK membantu bank memahami bagaimana cara mengelola dan melindungi data nasabah dengan baik, serta bagaimana menghindari tindakan yang dapat membuka celah bagi pencurian data. Sosialisasi ini juga mencakup upaya untuk meningkatkan kesadaran para pihak di bank mengenai dampak dari pencurian data pribadi.

Sebagai lembaga pengawas, OJK juga bekerja sama dengan berbagai instansi terkait, seperti Badan Siber dan Sandi Negara (BSSN) dan Kepolisian, untuk menciptakan sistem keamanan yang lebih terintegrasi. Kolaborasi ini bertujuan untuk memperkuat penanggulangan cyber crime di sektor perbankan, termasuk pencurian data pribadi nasabah. OJK dapat membantu dalam penyediaan data dan informasi yang diperlukan dalam investigasi dan penegakan hukum terkait kasus pencurian data. OJK juga menerapkan pendekatan berbasis risiko dalam pengawasan lembaga perbankan. Artinya, OJK lebih memfokuskan pengawasannya pada bank-bank yang memiliki risiko tinggi terkait dengan pencurian data pribadi, baik karena volume transaksi yang besar, banyaknya nasabah, ataupun penggunaan teknologi yang lebih kompleks. Dengan pendekatan ini, OJK dapat lebih cepat mendeteksi potensi ancaman yang ada dan mengambil langkah preventif yang lebih tepat sasaran.

Penting untuk dicatat bahwa OJK tidak hanya berperan dalam mencegah tindak pidana pencurian data pribadi, tetapi juga dalam menangani kasus-kasus yang sudah terjadi. Ketika pencurian data pribadi terjadi, OJK bekerja sama dengan pihak kepolisian dan lembaga hukum lainnya untuk memastikan bahwa proses hukum berjalan dengan transparan dan adil. OJK juga memastikan bahwa korban, dalam hal ini nasabah bank, mendapatkan hak-haknya, termasuk hak untuk memperoleh ganti rugi atas kerugian yang timbul akibat pencurian data. Selain itu, OJK juga memiliki mekanisme untuk memfasilitasi penyelesaian sengketa antara nasabah dan bank yang terkait dengan masalah pencurian data pribadi. Melalui Lembaga Alternatif Penyelesaian Sengketa (LAPS), OJK memberikan kesempatan bagi nasabah untuk menyelesaikan sengketa dengan bank secara damai tanpa melalui jalur pengadilan, yang sering kali memakan waktu dan biaya yang cukup tinggi.

Dalam mendukung keamanan data nasabah, OJK juga melakukan audit dan inspeksi secara rutin terhadap sistem keamanan dan prosedur pengelolaan data pribadi yang diterapkan oleh bank. Proses ini bertujuan untuk memastikan bahwa bank-bank tersebut selalu memenuhi standar yang telah ditetapkan dalam peraturan perundang-undangan terkait dengan perlindungan data pribadi. Selain dari sisi regulasi dan pengawasan, OJK juga turut mengembangkan sistem pelaporan dan pemantauan yang memungkinkan nasabah untuk melaporkan jika terjadi kecurigaan atau pelanggaran terkait pencurian data pribadi. Dengan adanya sistem ini, nasabah memiliki akses langsung untuk menyampaikan keluhan dan mendapatkan perlindungan yang cepat dan tepat dari bank dan OJK.

SIMPULAN

Kemajuan teknologi informasi dan komunikasi telah membawa manfaat besar bagi kehidupan manusia, khususnya dalam sektor perbankan. Namun, kemajuan ini juga memunculkan tantangan serius berupa tindak pidana pencurian data pribadi nasabah. Berbagai regulasi, seperti UU ITE, UU Perbankan, UU Perlindungan Data Pribadi, serta peraturan Otoritas Jasa Keuangan (OJK), telah dirancang untuk melindungi nasabah dari ancaman ini. Perlindungan hukum mencakup hak atas privasi data, kewajiban bank menjaga kerahasiaan nasabah, serta sanksi bagi pelanggar. OJK, sebagai lembaga pengawas sektor jasa keuangan, memainkan peran kunci dalam memastikan kepatuhan lembaga perbankan terhadap standar perlindungan data pribadi. Hal ini termasuk memastikan adanya

sistem keamanan yang memadai dan memberikan efek jera kepada pelanggar. Meski demikian, implementasi aturan masih menghadapi berbagai tantangan, seperti kurangnya kesadaran di kalangan masyarakat dan kelalaian lembaga perbankan.

SARAN

Otoritas Jasa Keuangan (OJK), dan lembaga perbankan terus meningkatkan regulasi dan implementasi perlindungan data pribadi melalui penguatan sistem keamanan digital, penyelenggaraan edukasi kepada masyarakat terkait risiko kejahatan siber, serta penerapan sanksi tegas terhadap pelanggaran yang dilakukan oleh pelaku usaha jasa keuangan. Bank juga perlu memastikan transparansi dalam pengelolaan data nasabah dan memperoleh persetujuan yang jelas dalam setiap proses pengumpulan atau pemanfaatan data pribadi. Dengan demikian, kepercayaan masyarakat terhadap sistem perbankan dapat terjaga, sekaligus menciptakan ekosistem keuangan yang aman, adil, dan terlindungi dari tindak pidana pencurian data.

REFERENSI

- Adam Chazawi (2015). *Tindak Pidana Informasi Dan Transaksi Elektronik*. Malang: Media Nusa Creative,
- Azmi, A. N. (2021). *Kewenangan Lembaga Otoritas Jasa Keuangan Dalam Rangka Meminimalisir Tindak Pidana Pencucian Uang Di Indonesia* (Doctoral Dissertation, Universitas Islam Sultan Agung Semarang).
- Djafar, W., & Komarudin, A. (2014). *Perlindungan Hak Atas Privasi Di Internet-Beberapa Penjelasan Kunci*. Elsam, Jakarta.
- Human Rights Committee General Comment No, On The Right To Respect Of Privacy, Family, Home And Correspondence, And Protection Of Honour And Reputation, 1988, 17.
- Isnugraheny, R. F., Megawati, Z. E., & Susilawati, S. (2024). Optimalisasi Prinsip Kerahasiaan Data Nasabah Dan Peranan Otoritas Jasa Keuangan Dalam Mencegah Kebocoran Informasi. *Media Hukum Indonesia (Mhi)*, 2(4).
- Kartiko, N. D., Soegiono, S. P., Siswanto, C. A., & Indradewi, A. A. (2024). Perlindungan Konsumen Sektor Keuangan: Peran Ojk Dalam Menghadapi Ancaman Phising Dan Skimming. *Iuris Studia: Jurnal Kajian Hukum*, 5(2), 347-363.
- Kusuma, A. C., & Rahmani, A. D. (2022). Analisis Yuridis Kebocoran Data Pada Sistem Perbankan Di Indonesia (Studi Kasus Kebocoran Data Pada Bank Indonesia). *Supremasi: Jurnal Hukum*, 5(1), 46-63.
- Ramadhan, M. T., & Wiyanti, D. (2024, February). Peran Otoritas Jasa Keuangan Dalam Mengawasi Kegiatan Lembaga Bank Berdasarkan Undang-Undang Otoritas Jasa Keuangan Nomor 21 Tahun 2011 Dan Undang-Undang Perbankan Nomor 10 Tahun 1998 Terkait. In *Bandung Conference Series: Law Studies* (Vol. 4, No. 1, Pp. 766-774).
- Richardus Eko Indrajit. (2020). "Fenomena Kebocoran Data; Mencari Sumber Penyebab Dan Akar Permasalahannya,." Folder.Idsirtii.Or.Id.
- Rumlus, M. H., & Hartadi, H. (2020). Kebijakan Penanggulangan Pencurian Data Pribadi Dalam Media Elektronik. *Jurnal Ham*, 11(2), 285-299.
- Siti Yuniarti, "Perlindungan Hukum Data Pribadi Di Indonesia,." *Jurnal Becoss* Vol.1, No. (2019): 148.
- Suari, K. R. A., & Sarjana, I. M. (2023). Menjaga Privasi Di Era Digital: Perlindungan Data Pribadi Di Indonesia. *Jurnal Analisis Hukum*, 6(1), 132-142.
- Sukatendel, R. D. Peran Otoritas Jasa Keuangan Terhadap Tindak Pidana Penyebaran Data Pribadi Oleh Perusahaan Financial Technology (Studi Penelitian Di Otoritas Jasa Keuangan Sumatera Utara).
- Sutarli, A. F., & Kurniawan, S. (2023). Peranan Pemerintah Melalui Undang-Undang Perlindungan Data Pribadi Dalam Menanggulangi Phising Di Indonesia. *Innovative: Journal Of Social Science Research*, 3(2), 4208-4221.



Triputri, D. H., Mofea, S., Yulviani, D., & Pratama, R. (2023). Analisis Yuridis Terhadap Penerapan Sanksi Pidana Bagi Pelaku Penipuan Dalam Transaksi Elektronik Berdasarkan Asas Lex Specialis Derogat Legi Generali Ditinjau Dari Kuhp Dan Uu Ite. *Lex Veritatis*, 2(01), 42-51.