

**URGENSI PERLINDUNGAN DATA PRIBADI DALAM SEKTOR  
PERBANKAN DI ERA DIGITAL**

***THE URGENCY OF PERSONAL DATA PROTECTION IN THE BANKING  
SECTOR IN THE DIGITAL ERA***

**Muhammad Wildan Ichsandi dan Wilma Silalahi**

**Fakultas Hukum, Universitas Tarumanagara, DKI Jakarta, Indonesia**

Korespondensi Penulis : [muhammad.207242011@stu.untar.ac.id](mailto:muhammad.207242011@stu.untar.ac.id)

Citation Structure Recommendation :

Ichsandi, Muhammad Wildan dan Wilma Silalahi. *Urgensi Perlindungan Data Pribadi dalam Sektor Perbankan di Era Digital*. Rewang Rencang : Jurnal Hukum Lex Generalis. Vol.5. No.12 (2024).

**ABSTRAK**

Perkembangan teknologi digital telah menciptakan tantangan baru dalam hal perlindungan data pribadi, terutama di sektor perbankan yang bersifat sensitif dan berbasis kepercayaan. Masyarakat kini semakin bergantung pada layanan keuangan digital, menjadikan data pribadi sebagai aset yang rentan terhadap penyalahgunaan. Kepercayaan publik terhadap lembaga perbankan ditentukan oleh komitmennya dalam menjaga kerahasiaan dan keamanan data nasabah. Regulasi yang ada, meskipun terus berkembang, belum sepenuhnya mampu menanggulangi ancaman kejahatan siber yang semakin kompleks. Penelitian ini bertujuan untuk mengkaji urgensi perlindungan hukum terhadap data pribadi nasabah dalam sektor perbankan di era digital. Penelitian ini menggunakan metode yuridis normatif dengan pendekatan peraturan perundang-undangan dan studi kepustakaan. Hasil penelitian menunjukkan bahwa meskipun telah ada berbagai ketentuan seperti UU ITE, UU PDP, dan POJK, implementasi perlindungan masih menghadapi tantangan besar, terutama dalam aspek pengawasan, sanksi, dan sistem keamanan. Prinsip kepercayaan dan kerahasiaan menjadi landasan hubungan antara bank dan nasabah, namun sering kali belum diimbangi dengan perlindungan teknologi yang memadai. Diperlukan integrasi antara norma hukum nasional dengan prinsip-prinsip internasional seperti APEC Privacy Framework guna memperkuat sistem pengamanan data. Oleh karena itu, pemerintah dan otoritas perbankan harus memperkuat sistem keamanan digital, memperjelas sanksi terhadap pelanggaran, serta memastikan kepatuhan sektor perbankan terhadap prinsip perlindungan data untuk menjamin rasa aman nasabah dan menjaga stabilitas keuangan nasional.

**Kata Kunci: Data Pribadi, Perbankan, Perlindungan Hukum, Kepercayaan, Keamanan Digital**

**ABSTRACT**

*The advancement of digital technology has posed new challenges in personal data protection, especially in the banking sector where sensitivity and trust are crucial. With increasing reliance on digital financial services, personal data has become highly vulnerable to misuse. Public trust in banking institutions depends on their commitment to safeguarding the confidentiality and security of customer data. Existing regulations, though evolving, have not yet fully addressed the growing threat of cybercrime. This study aims to examine the urgency of legal protection for personal data in the banking sector in the digital era. The research uses a normative juridical method with statutory and literature approaches. Findings show that although various laws such as the Indonesian Electronic Information and Transactions Law, the Personal Data Protection Law, and Financial Services Authority regulations exist, their implementation still faces major obstacles, particularly in supervision, sanctions, and technological safeguards. The principles of trust and confidentiality form the basis of bank-customer relationships, yet are often not supported by adequate digital protection systems. Integration between national legal norms and international standards, such as the APEC Privacy Framework, is essential to enhance data security. Therefore, government and financial authorities must strengthen cybersecurity systems, clarify legal consequences for violations, and ensure full compliance with data protection principles to build customer trust and maintain financial system stability.*

**Keywords:** *Personal Data, Banking, Legal Protection, Trust, Digital Security.*

**A. PENDAHULUAN**

Perkembangan teknologi informasi dan komunikasi yang berkembang pesat telah menciptakan berbagai peluang dan tantangan. Salah satu bidang yang terpengaruh oleh kemajuan teknologi informasi adalah terjadinya interaksi yang aktif antara individu dan penyedia jasa. Informasi telah memperkenalkan suatu etika baru, di mana setiap pihak yang memiliki informasi memiliki naluri untuk mendistribusikannya kepada pihak lain. Pertukaran informasi saat ini telah mendunia, komunitas informasi dari berbagai belahan dunia, berkomunikasi secara intensif satu sama lain. Hubungan antara komunitas dilakukan melalui teknologi informasi secara virtual atau ruang siber. Cakupan dan sistem teknologi informasi mencakup pengumpulan (*collect*), penyimpanan (*store*), proses, produksi, dan pengiriman, dari dan ke industri atau masyarakat dengan cepat dan efektif.<sup>1</sup>

---

<sup>1</sup> Abdul Raman Saad, *Personal Data & Privacy Protection*, Kelana Jaya Malaysia Journal, Vol.42, No.1 (2005), p.1-42.

Saat ini, dunia telah memasuki revolusi industri 4.0 yang telah mengubah semua aspek kehidupan manusia. Revolusi Industri 4.0 ditandai dengan meningkatnya penggunaan teknologi informasi di berbagai bidang dan membawa perubahan dalam setiap lini kehidupan. Revolusi ini ditandai dengan automasi (*automation*) penggunaan komputer dan peralatan elektrik yang pada akhirnya menggulirkan era baru revolusi industri 3.0. Roda revolusi tersebut ternyata terus bergulir seiring dengan perkembangan sains dan teknologi hingga kemudian muncul sistem *cyber physical*. Sistem ini mengharuskan adanya interaksi antara manusia yang terintegrasi dengan komputer dan kemampuan fisiknya (*digitalization*). Digitalisasi inilah yang menjadi awal mula bergulirnya era revolusi industri 4.0.<sup>2</sup>

Seiring dengan kemajuan zaman di era globalisasi ini, setiap aktivitas masyarakat tidak dapat dipisahkan dari peran teknologi. Hal ini juga berlaku pada lembaga keuangan yang kini mulai beralih ke lembaga keuangan berbasis teknologi. Salah satu inovasi dalam sektor keuangan saat ini adalah adanya adaptasi *Financial Technology* atau yang sering kita sebut dengan *fintech*. *Fintech* diyakini mampu menjadi solusi untuk mempermudah, mempercepat waktu, memberikan kenyamanan, dan lain-lain bagi para pengguna layanan *fintech* di Indonesia. *Fintech* merupakan penerapan dan pemanfaatan teknologi untuk meningkatkan layanan jasa perbankan dan keuangan yang umumnya dilakukan oleh perusahaan rintisan (*startup*) dengan memanfaatkan teknologi perangkat lunak, internet, komunikasi, dan komputasi terkini.<sup>3</sup>

Bank sebagai elemen dari sistem keuangan dan sistem pembayaran di suatu negara, memiliki peran yang sangat krusial. Peran signifikan bank ini terkait erat dengan fungsinya sebagai lembaga perantara keuangan (*financial intermediary*), yaitu yang beroperasi dalam kegiatan usaha penghimpunan dana (*fund raising*) dari masyarakat & penyaluran dana (*fund lending*) kepada masyarakat. Kegiatan penghimpunan dana dilakukan berdasarkan perjanjian atau kontrak penyimpanan maupun perjanjian atau kontrak diantara bank dengan nasabah penyimpan.

---

<sup>2</sup> Erna Prihasari, *Pentingnya Perlindungan Data Pribadi dalam Transaksi Pinjaman Online (The Urgency of Personal Protection in Peer to Peer Lending)*, Majalah Hukum Nasional, Vol.49 No.2 (2019), p.1.

<sup>3</sup> Nofie Iman, *Financial Technology dan Lembaga Keuangan*, Gathering Mitra Linkage Bank Syariah Mandiri, Yogyakarta, 2016, p.6.

Adapun dari kontrak tersebut, muncul hubungan kontraktual antara pihak bank dan nasabah. Hubungan kontraktual antara bank dan nasabah penyimpanan dana didasarkan pada Prinsip Kepercayaan (*fiduciary principle*) dan Prinsip Kerahasiaan (*confidential principle*).<sup>4</sup>

Hubungan kontraktual antara bank dan nasabah yang berlandaskan pada prinsip kepercayaan (*fiduciary principle*) mengakibatkan bank tidak hanya fokus pada kepentingan dirinya sendiri, tetapi juga harus memperhatikan kepentingan nasabah yang menyimpan dana. Kewajiban bank untuk memperhatikan kepentingan nasabahnya juga didasari oleh prinsip kerahasiaan (*confidential principle*). Prinsip ini mengharuskan bank untuk menjaga kerahasiaan semua data dan informasi yang berkaitan dengan nasabah, baik yang menyangkut keadaan keuangannya maupun informasi pribadi. Hal ini bertujuan untuk membangun kepercayaan dari masyarakat (nasabah penyimpanan dana), sehingga diharapkan dengan adanya kepercayaan tersebut, semakin banyak masyarakat yang akan menggunakan jasa bank sebagai tempat penyimpanan uang mereka<sup>5</sup>.

Menjaga kerahasiaan atas informasi keuangan nasabah merupakan prinsip fundamental yang harus dijunjung tinggi dalam seluruh aktivitas operasional perbankan. Perlindungan terhadap data dan kondisi keuangan nasabah bukan sekadar kewajiban normatif yang diatur dalam berbagai peraturan perundang-undangan, tetapi juga menjadi landasan etis yang membentuk fondasi hubungan antara bank dan nasabah. Dalam konteks ini, jaminan atas kerahasiaan menciptakan ruang kenyamanan dan rasa aman bagi nasabah untuk mempercayakan urusan keuangannya kepada institusi perbankan. Rasa percaya tersebut secara alamiah membentuk suatu hubungan hukum yang bersifat fidusia (*fiduciary relationship*), di mana bank memegang peran sebagai pihak yang dipercaya untuk menjaga informasi keuangan nasabah secara bertanggung jawab dan profesional. Semakin tinggi tingkat kepercayaan nasabah terhadap komitmen bank dalam menjaga kerahasiaan, maka semakin kuat pula loyalitas dan ketergantungan nasabah terhadap layanan yang diberikan. Dalam jangka panjang,

---

<sup>4</sup> Marnia Rani, *Perlindungan Otoritas Jasa Keuangan Terhadap Kerahasiaan dan Keamanan Data Pribadi Nasabah Bank*, Jurnal Selat, Vol.2, No.1, (Oktober 2014), p. 168.

<sup>5</sup> Djoni S. Gazali dan Rachmadi Usman, *Hukum Perbankan*, Sinar Grafika, Jakarta, 2010, p.27-30.

hal ini akan berdampak positif terhadap reputasi, stabilitas, dan daya saing bank di tengah kompetisi industri jasa keuangan.<sup>6</sup> Pengaturan kerahasiaan data nasabah memang tidak diatur secara eksplisit dalam Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan Atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan (“UU Perbankan”). UU Perbankan hanya mengatur mengenai prinsip kerahasiaan bank secara umum saja, yakni dalam bentuk istilah ‘rahasia bank’, yang diartikan sebagai segala sesuatu yang berhubungan dengan keterangan mengenai nasabah penyimpan dan simpanannya. Berdasarkan Pasal 1 angka 28 yang berbunyi Rahasia Bank adalah segala sesuatu yang berhubungan dengan keterangan mengenai nasabah penyimpanan dan simpanannya.

Dari pasal itu menunjukkan bahwa informasi mengenai nasabah bank tidak hanya terbatas pada keadaan keuangan, tetapi juga mencakup semua bentuk informasi tentang nasabah penyimpan. Nomor telepon (seluler) juga harus dirahasiakan oleh bank yang menyimpan dana nasabah. Jika bank dapat menjaga kerahasiaan nasabah penyimpan, hal ini akan memberikan rasa nyaman dan aman bagi nasabah untuk menyimpan dana di bank. Ini juga akan berpengaruh positif terhadap kepercayaan masyarakat terhadap bank. Pada dasarnya, prinsip kerahasiaan yang diterapkan dalam kegiatan perbankan bertujuan untuk kepentingan bank itu sendiri. Semakin banyak masyarakat yang menyimpan dana di bank, semakin besar pula keuntungan yang akan diperoleh bank tersebut. Guna mengatasi masalah yang telah disebutkan, diperlukan intervensi dari pihak berwenang dalam sektor perlindungan konsumen di bidang jasa keuangan. Perlindungan konsumen pengguna jasa keuangan, sesuai dengan Undang-Undang Nomor 21 Tahun 2011, berada di bawah lembaga Otoritas Jasa Keuangan. Lembaga Otoritas Jasa Keuangan, sebagai lembaga yang memiliki kewenangan dalam regulasi, pengawasan, dan perlindungan di bidang jasa keuangan, seharusnya dapat segera merespons keresahan masyarakat agar dapat memberikan rasa aman bagi nasabah yang menyimpan dana di bank. Keberadaan Otoritas Jasa Keuangan sebagai lembaga pengawas di sektor jasa keuangan diharapkan dapat melindungi konsumen dari Pelaku Usaha Jasa Keuangan (PUJK) yang dianggap dapat merugikan kepentingan konsumen, dalam hal ini adalah nasabah bank.<sup>7</sup>

---

<sup>6</sup> Yunus Husein, *Rahasia Bank dan Penegakan Hukum*, Pustaka Juanda Tigalima, Jakarta, 2010, p. 48.

<sup>7</sup> *Ibid.*, p. 169.

Berdasarkan latar belakang permasalahan yang telah dijelaskan sebelumnya, pada kesempatan ini, penulis merasa perlu untuk menganalisis berbagai peraturan mengenai perlindungan terhadap kerahasiaan dan keamanan data nasabah perbankan. Rumusan permasalahan dalam penelitian ini berangkat dari urgensi akan perlindungan hukum yang memadai terhadap kerahasiaan serta keamanan data pribadi, khususnya dalam konteks regulasi yang berlaku di Indonesia. Dalam era digital yang ditandai dengan pesatnya perkembangan teknologi informasi dan komunikasi, data pribadi menjadi aset yang sangat rentan terhadap berbagai bentuk penyalahgunaan. Oleh karena itu, penting untuk menelaah secara kritis bagaimana bentuk upaya perlindungan hukum yang dapat menjamin adanya kepastian hukum, keadilan, dan perlindungan terhadap hak-hak konstitusional individu atas data pribadinya. Penelusuran terhadap regulasi yang mengatur mengenai perlindungan data pribadi tidak hanya mencakup substansi norma dalam undang-undang, tetapi juga menyangkut efektivitas pelaksanaannya oleh para penyelenggara sistem elektronik maupun institusi keuangan.

Lebih lanjut, penelitian ini juga hendak mengkaji secara khusus bagaimana langkah-langkah hukum yang diambil oleh sektor perbankan dalam menjaga dan melindungi kerahasiaan serta keamanan data pribadi para nasabahnya. Dalam hubungan hukum antara bank dan nasabah, kepercayaan merupakan fondasi utama. Oleh karena itu, setiap bentuk pelanggaran terhadap prinsip kerahasiaan data nasabah tidak hanya berimplikasi pada aspek hukum, tetapi juga berdampak pada hilangnya kepercayaan publik terhadap sistem perbankan nasional. Dalam konteks ini, penelitian akan menelaah mekanisme preventif dan represif yang telah dan seharusnya dilakukan oleh bank serta otoritas pengawasnya untuk memastikan bahwa data pribadi nasabah tidak disalahgunakan, diakses secara tidak sah, atau disebarluaskan tanpa persetujuan. Kajian ini akan memperhatikan pula sejauh mana harmonisasi antara peraturan nasional dengan standar internasional dapat diintegrasikan guna membentuk kerangka perlindungan data yang tangguh dan adaptif terhadap perkembangan zaman.

Penelitian ini menggunakan pendekatan yuridis normatif sebagai landasan metodologisnya. Pendekatan ini lazim digunakan dalam kajian hukum yang menitikberatkan pada telaah terhadap norma-norma hukum tertulis, baik yang tertuang dalam peraturan perundang-undangan maupun dalam bentuk asas, doktrin, dan prinsip hukum lainnya.<sup>8</sup> Fokus utama dari pendekatan ini adalah pada studi kepustakaan (*library research*), di mana sumber data yang dianalisis berasal dari bahan-bahan hukum yang bersifat sekunder maupun primer, seperti undang-undang, peraturan pelaksana, putusan pengadilan, serta karya ilmiah yang relevan dengan permasalahan yang dikaji. Tujuan dari penelitian ini adalah untuk menggali, mengidentifikasi, serta menganalisis berbagai teori, konsep yuridis, asas-asas umum hukum, hingga ketentuan hukum positif yang memiliki keterkaitan langsung dengan isu yang menjadi objek penelitian.<sup>9</sup>

Dalam kerangka tersebut, penelitian ini tidak hanya membatasi diri pada hukum yang tertulis semata, tetapi juga mencakup hukum yang hidup dalam praktik (*living law*) serta prinsip-prinsip yang berkembang dalam doktrin keilmuan.<sup>10</sup> Ruang lingkup analisis mencakup penerapan asas-asas hukum, baik yang bersifat umum maupun yang bersifat khusus dalam konteks perlindungan data pribadi, serta sejauh mana prinsip-prinsip tersebut diadopsi dan diimplementasikan dalam tatanan hukum positif nasional.<sup>11</sup> Dengan demikian, bahan hukum yang digunakan dalam penelitian ini meliputi bahan hukum primer, seperti undang-undang dan peraturan turunannya, serta bahan hukum sekunder berupa literatur hukum, jurnal ilmiah, pendapat para ahli hukum, dan sumber kepustakaan lainnya yang mendukung pemahaman terhadap isu hukum yang dibahas. Kombinasi antara pendekatan normatif dengan sumber data yang komprehensif diharapkan dapat memberikan pemahaman yang utuh dan mendalam terhadap permasalahan hukum yang menjadi fokus dalam penelitian ini.

---

<sup>8</sup> Soerjono Soekanto dan Sri Mamudji, *Penelitian Hukum Normatif (Suatu Tinjauan Singkat)*, Raja Grafindo Persada, Jakarta, 2003, p.13.

<sup>9</sup> Gracia Gracia, dkk, *Implementasi Konsep Euthanasia: Supremasi Hak Asasi Manusia dan Progresivitas Hukum di Indonesia*, Ikatan Penulis Mahasiswa Hukum Indonesia Law Journal, Vol.2, No.1 (2022), p.1-24.

<sup>10</sup> Soerjono Soekanto, *Pengantar Penelitian Hukum*, UI Press, Jakarta, 1996, p.63.

<sup>11</sup> Soerjono Soekanto dan Sri Mamudji, *Loc.Cit.*, p.13.

## B. PEMBAHASAN

### 1. Perlindungan Hukum Terhadap Regulasi Kerahasiaan dan Keamanan Data Pribadi

Pengaturan mengenai perlindungan data pribadi di Indonesia pada mulanya telah memperoleh pengakuan normatif melalui UU ITE. Salah satu ketentuan yang menjadi tonggak awal dalam menjamin hak atas privasi data pribadi tertuang dalam Pasal 26 ayat (1) UU ITE, yang secara tegas menyatakan bahwa, kecuali ditentukan lain oleh peraturan perundang-undangan, penggunaan setiap informasi melalui media elektronik yang berkaitan dengan data pribadi seseorang wajib dilakukan atas dasar persetujuan dari orang yang bersangkutan. Ketentuan ini menegaskan prinsip utama bahwa setiap individu memiliki kedaulatan penuh atas data pribadinya, yang tidak dapat diakses, dimanfaatkan, atau disebarluaskan tanpa adanya persetujuan eksplisit dari pemilik data. Dengan demikian, persetujuan menjadi syarat mutlak (*consent as a legal basis*) yang harus dipenuhi sebelum data pribadi dapat digunakan dalam aktivitas apa pun di ranah digital.<sup>12</sup>

Lebih jauh lagi, ketentuan dalam Pasal 26 tidak hanya memberikan perlindungan secara normatif, tetapi juga membuka ruang bagi pemilik data untuk menempuh upaya hukum apabila terjadi pelanggaran. Sebagaimana diatur dalam ayat (2) pasal tersebut, seseorang yang merasa bahwa data pribadinya telah digunakan tanpa izin berhak mengajukan gugatan perdata terhadap pihak yang melakukan pelanggaran. Selain itu, pemilik data juga dapat meminta penyelenggara sistem elektronik untuk menghapus data pribadi yang tidak relevan sebagai bagian dari pelaksanaan hak atas pengendalian data. Mekanisme ini mencerminkan adanya prinsip akuntabilitas dan transparansi yang menjadi bagian integral dalam pengelolaan data pribadi, sekaligus memberikan jaminan kepastian hukum kepada warga negara dalam menghadapi potensi penyalahgunaan informasi pribadi di era digital.<sup>13</sup>

---

<sup>12</sup> HR Ridwan, *Hukum Administrasi Negara*, Raja Grafindo Perkasa, Jakarta, 2011, p.45.

<sup>13</sup> Retno Kusniati, *Sejarah Perlindungan Hak-Hak Asasi Manusia dalam Kaitannya dengan Konsepsi Negara Hukum*, Jurnal Inovatif Hukum, Vol.4, No.5, (2019), p.80.

Regulasi di Indonesia juga mengatur perusahaan yang membangun bisnisnya dengan melibatkan publik untuk mendaftarkan informasi pribadi yang sensitif kepada perusahaan tersebut. Oleh karena itu, perusahaan harus memahami aturan, prinsip, dan praktik perlindungan data pribadi. Selain itu, pemerintah juga mengatur hubungan kontraktual antara bank dan nasabah yang merupakan pengguna jasa bank. Dalam hal ini, nasabah memberikan informasi dan data pribadi yang sangat sensitif, terutama dalam konteks perbankan dan keuangan, sehingga harus siap menerapkan prinsip kerahasiaan.<sup>14</sup> Aspek yang cukup khusus mengenai perlindungan data pribadi terdapat dalam regulasi telekomunikasi dan informatika. Pada awalnya, perlindungan hak atas privasi diatur dalam UU No. 36 tahun 1999 tentang Telekomunikasi, yang menetapkan bahwa kerahasiaan informasi dan komunikasi pribadi seseorang adalah bagian dari pengaturan mengenai perlindungan hak atas privasi, yang melarang tindakan penyadapan.<sup>15</sup>

Selanjutnya, pengaturan mengenai perlindungan data pribadi memiliki cakupan yang lebih luas dan diatur dalam Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Tertuang dalam Pasal 26 ayat (1) yang berbunyi, 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. Memahami frasa yang terdapat dalam pasal 26 UU ITE berarti bahwa setiap individu memiliki hak penuh atas data pribadi mereka. Oleh karena itu, jika ingin menggunakan data pribadi, harus ada persetujuan dari orang yang bersangkutan (pemilik data). Apabila terjadi pelanggaran, akan ada konsekuensi hukum yang berlaku. Pihak yang merasa datanya telah digunakan tanpa izin dapat mengajukan gugatan sesuai dengan ketentuan yang diatur dalam Pasal 26 ayat (2) UU ITE, dengan meminta penghapusan data pribadi yang tidak relevan kepada penyelenggara sistem elektronik sebagai bentuk hak pemilik data.<sup>16</sup>

---

<sup>14</sup> Marnia Rani, *Op.Cit.*, p.172.

<sup>15</sup> Wahyudi Djafar, *Hukum Perlindungan Data Pribadi di Indonesia: Lanskap, Urgensi dan Kebutuhan Pembaruan*, Makalah disampaikan sebagai materi dalam kuliah umum, Tantangan Hukum dalam Era Analisis Big Data, Yogyakarta: Program Pasca Sarjana FH UGM, 2019.

<sup>16</sup> Siti Yuniarti, *Perlindungan Hukum Data Pribadi di Indonesia, Business Economic, Communication, and Social Sciences Journal (BECOSS)*, Vol.1, No.1 (2019), p.152.

Perlindungan terhadap data pribadi sebagai bagian dari hak asasi manusia tidak hanya diatur dalam kerangka hukum sektoral, tetapi juga memperoleh pengakuan secara eksplisit dalam instrumen hukum nasional yang lebih luas, yakni Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia. Dalam Pasal 21 undang-undang tersebut ditegaskan bahwa setiap orang berhak atas keutuhan pribadi, baik secara rohani maupun jasmani, yang mencakup hak atas perlindungan terhadap privasi diri. Oleh karena itu, seseorang tidak dapat dijadikan objek penelitian tanpa persetujuannya. Ketentuan ini menegaskan bahwa perlindungan terhadap integritas pribadi juga mencakup larangan eksploitasi data pribadi tanpa dasar hukum yang sah, khususnya dalam konteks pengumpulan informasi yang berkaitan dengan kehidupan pribadi, opini, atau pernyataan yang menyentuh ranah privat, termasuk rekaman suara dan gambar.

Lebih lanjut, pengaturan perlindungan data pribadi juga diatur dalam sektor administrasi kependudukan sebagaimana tercantum dalam Pasal 79 ayat (1) Undang-Undang Republik Indonesia Nomor 24 Tahun 2013 yang merupakan perubahan atas Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan. Pasal tersebut mengamanatkan bahwa seluruh data perseorangan dan dokumen kependudukan wajib disimpan dan dilindungi kerahasiaannya oleh negara. Dalam konteks ini, data pribadi dimaknai sebagai seluruh informasi yang berkaitan dengan identitas individu, yang harus dijaga keakuratannya, kerahasiaannya, serta hanya dapat diakses dan digunakan sesuai ketentuan hukum yang berlaku.

Kewajiban untuk menjaga kerahasiaan data ini menjadi tanggung jawab penyelenggara administrasi kependudukan, termasuk petugas dan instansi pelaksana yang mengelola sistem informasi penduduk. Ketentuan teknis lebih lanjut mengenai pelaksanaan perlindungan data pribadi dalam lingkup administrasi kependudukan diatur dalam Peraturan Presiden Nomor 67 Tahun 2011 tentang Kartu Tanda Penduduk Berbasis Nomor Induk Kependudukan Secara Nasional.

Meskipun peraturan tersebut menjadi dasar dalam mengembangkan sistem identitas nasional berbasis data tunggal, namun dalam praktiknya masih terdapat kekosongan norma terkait mekanisme perlindungan terhadap data biometrik, seperti sidik jari dan retina mata, khususnya dalam konteks pasca perekaman maupun permintaan akses terhadap data oleh pihak ketiga. Hal ini menimbulkan kekhawatiran akan potensi penyalahgunaan data sensitif penduduk apabila tidak disertai dengan kerangka hukum yang kuat dan mekanisme pengawasan yang memadai. Oleh karena itu, terdapat kebutuhan mendesak untuk memperkuat kebijakan perlindungan data pribadi melalui harmonisasi antar peraturan dan pembentukan sistem perlindungan yang terintegrasi dalam skala nasional.<sup>17</sup>

Selain itu, diterbitkannya Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik. Disebutkan dalam Pasal 6 yang berbunyi, penyelenggara Sistem Elektronik yang melakukan proses sebagaimana dimaksud dalam Pasal 3 wajib menyediakan formulir persetujuan dalam Bahasa Indonesia untuk meminta Persetujuan dari Pemilik Data Pribadi yang dimaksud. Tujuan dari hal ini adalah untuk melindungi hak setiap pengguna sistem elektronik dengan cara yang nyaman, sehingga tidak ada pihak yang dirugikan. Seperti yang telah dijelaskan dalam Pasal 26 ayat (1-5), yang berbunyi, Pemilik Data Pribadi berhak: (a) atas kerahasiaan Data Pribadinya; (b) mengajukan pengaduan dalam rangka penyelesaian sengketa Data Pribadi atas kegagalan perlindungan kerahasiaan Data Pribadinya oleh Penyelenggara Sistem Elektronik kepada Menteri; (c) mendapatkan akses atau kesempatan untuk mengubah atau memperbarui Data Pribadinya tanpa mengganggu sistem pengelolaan Data Pribadi, kecuali ditentukan lain oleh ketentuan peraturan perundang-undangan; (d) mendapatkan akses atau kesempatan untuk memperoleh historis Data Pribadinya yang pernah diserahkan kepada Penyelenggara Sistem Elektronik sepanjang masih sesuai dengan ketentuan peraturan perundang-undangan; dan (e) meminta pemusnahan Data Perseorangan Tertentu miliknya dalam Sistem Elektronik yang dikelola oleh Penyelenggara Sistem Elektronik, kecuali ditentukan lain oleh ketentuan peraturan perundang-undangan.

---

<sup>17</sup> Wahyudi Djafar, *Op.Cit.*.

Perlindungan data pribadi yang diatur dalam Permenkominfo No. 20 tahun 2016 menyatakan bahwa jika Pemilik Sistem Elektronik melakukan pelanggaran, mereka hanya akan dikenakan sanksi administratif. Disebutkan dalam Pasal 36 ayat (1): Setiap Orang yang memperoleh, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarluaskan Data Pribadi tanpa hak atau tidak sesuai dengan ketentuan dalam Peraturan Menteri ini atau peraturan perundang-undangan lainnya dikenai sanksi administratif sesuai dengan ketentuan peraturan perundang-undangan berupa: a. peringatan lisan; b. peringatan tertulis; c. penghentian sementara kegiatan; dan/atau d. pengumuman di situs dalam jaringan (*website online*).

Dalam sektor perbankan dan keuangan, UU No.10 Tahun 1998 juga mengatur mengenai data pribadi. Di antaranya, mengatur terkait kerahasiaan bank,<sup>18</sup> yaitu bank diwajibkan untuk menjaga kerahasiaan semua informasi dan data yang berkaitan dengan nasabah, baik kondisi keuangan maupun informasi yang bersifat pribadi.<sup>19</sup> Sedangkan dalam aspek keuangan, OJK menerbitkan POJK Nomor 13/Pojk.02/2018 tentang Inovasi Keuangan Digital Di Sektor Jasa Keuangan. Dalam Pasal 30 ayat (1), penyelenggara wajib menjaga kerahasiaan, keutuhan, dan ketersediaan data pribadi, data transaksi, dan data keuangan yang dikelolanya sejak data diperoleh hingga data tersebut dimusnahkan.

Dengan adanya peraturan-peraturan tersebut, pengolahan data dan informasi harus dikelola dengan baik, jelas, dan terarah secara otomatis. Jika tidak dikelola dengan tepat, akibatnya bisa sangat fatal dan berbahaya, karena dapat berujung pada penyalahgunaan dan serangan kejahatan siber. Oleh karena itu, diperlukan analisis manajemen risiko untuk menghadapi serangan *cyber crime*. *Cyber crime* memiliki potensi untuk mengakibatkan hilangnya sistem informasi dan kendali atas data pribadi, dan hal ini sulit untuk diatasi. Kejahatan pencurian data yang dilakukan oleh *hacker* yang tidak bertanggung jawab tentu menimbulkan kerugian bagi para korban. Begitu pula dengan korban dari tindakan *phishing* yang membuat data pribadi mereka dapat diperjualbelikan dengan bebas, dengan risiko yang harus ditanggung oleh korban sangat besar. Oleh karena itu, penindakan terhadap kejahatan siber harus dikenakan hukuman yang berat.<sup>20</sup>

---

<sup>18</sup> Yunus Husein, *Op.Cit.*, p.11-13.

<sup>19</sup> Djoni S. Gazali dan Rachmadi Usman, *Op.Cit.*, p.30.

<sup>20</sup> Ineu Rahmawati, *Analisis Manajemen Risiko Ancaman Kejahatan Siber (Cyber Crime) dalam Peningkatan Cyber Defense*, Jurnal Pertahanan & Bela Negara, Vol.7, No.2 (2017), p.53.

Prinsip Perlindungan Data Pribadi dalam melaksanakan semua kegiatan yang berkaitan dengan pemrosesan, pengelolaan, penggunaan, dan penyebarluasan data pribadi, penting untuk memperhatikan prinsip-prinsip yang telah diatur dalam *APEC Privacy Framework*. Data pribadi harus dikumpulkan, disimpan, diproses, atau digunakan secara adil (“*fairly*”) dan sah (“*lawfully*”). Untuk menentukan apakah data pribadi tersebut diperoleh secara “*fair*”, biasanya dilihat dari metode yang digunakan untuk mengumpulkan, menyimpan, memproses, atau menggunakan data tersebut. Maksud pengumpulan data pribadi adalah untuk memperoleh data hanya untuk satu atau lebih tujuan tertentu yang sah. Data pribadi tidak boleh dikumpulkan kecuali untuk tujuan-tujuan yang sah yang secara langsung terkait dengan fungsi atau kegiatan pengelola data yang menggunakan data pribadi tersebut; pengumpulan data tersebut diperlukan untuk, atau secara langsung berkaitan dengan tujuan tersebut; dan data pribadi tersebut harus layak, relevan, serta tidak berlebihan dalam kaitannya dengan tujuan tersebut.<sup>21</sup>

Penggunaan Data Pribadi dikelola untuk tujuan tertentu tidak boleh, tanpa persetujuan dari subjek data, digunakan untuk tujuan lain selain dari tujuan di mana data pribadi tersebut dikumpulkan; atau untuk tujuan yang secara langsung berkaitan dengan tujuan tersebut. Data pribadi tidak boleh diperlakukan atau digunakan dengan cara yang bertentangan dengan tujuan penggunaannya. Data pribadi tidak boleh diungkapkan tanpa persetujuan dari subjek data, kecuali pengungkapan data pribadi tersebut dilakukan sesuai dengan tujuan awal atau secara langsung berkaitan dengan tujuan perolehannya. Keakurasian Data Pribadi yaitu langkah praktis perlu diambil untuk memastikan bahwa data pribadi akurat, lengkap, relevan, tidak menyesatkan, serta terkini, dengan mempertimbangkan tujuan atau yang terkait langsung dengan tujuan perolehan dan penggunaan data tersebut.<sup>22</sup>

---

<sup>21</sup> Abu Bakar Munir, dkk, *Data Protection Law in Asia*, International Data Privacy Law Journal, Vol.8, No.4 (November 2018), p.338-340.

<sup>22</sup> Sinta Dewi Rosadi, *Prinsip-Prinsip Perlindungan Data Pribadi Nasabah Kartu Kredit Menurut Ketentuan Nasional dan Implementasinya*, Jurnal Sosiohumaniora, Vol.19, No.3, (November 2017), p.206-212.

Jangka waktu menyimpan Data Pribadi yaitu yang disimpan untuk suatu tujuan tertentu tidak boleh disimpan lebih lama dari waktu yang diperlukan untuk tujuan penggunaannya. Prinsip ini mengharuskan pengelola data untuk meninjau data tersebut secara berkala dan menghapusnya jika sudah tidak diperlukan lagi, kecuali jika diperlukan untuk kepentingan umum. Akses kepada dan Koreksi atas Data Pribadi. Subjek data memiliki hak untuk mengakses data pribadinya yang dikelola oleh pengelola data, termasuk untuk melakukan koreksi terkait data pribadinya. Keamanan Data Pribadi. Semua langkah yang diperlukan harus diambil oleh pengelola data untuk mencegah akses, pemrosesan, perubahan, pengungkapan, serta perusakan data pribadi secara ilegal, termasuk terhadap kejadian yang dapat merugikan data pribadi. Langkah-langkah yang diambil oleh pengelola data harus mempertimbangkan: sifat dan ancaman terhadap data pribadi; lokasi di mana data tersebut disimpan; sistem keamanan yang digunakan; serta tindakan yang dilakukan untuk menjamin kehandalan, integritas, dan kompetensi orang yang memiliki data.<sup>23</sup>

Pengaturan Data Pribadi di Indonesia. Pada tahun 2005, Bank Indonesia menerbitkan Peraturan Bank Indonesia Nomor 7/6/PBI/2005 mengenai Transparansi Informasi Produk Bank dan Penggunaan Data Pribadi Nasabah. Melalui ketentuan ini, Bank Indonesia diwajibkan untuk menetapkan kebijakan yang mencakup prosedur perlindungan data pribadi nasabah kartu kredit di Indonesia. Ketentuan ini mengharuskan Bank untuk melindungi penggunaan data pribadi nasabah untuk tujuan komersial dengan cara yang transparan dan memerlukan persetujuan tertulis dari nasabah. Aturan prosedural yang harus disusun oleh Bank terkait perlindungan data pribadi nasabah adalah sebagai berikut: Jika Bank berencana untuk mendistribusikan atau menyebarluaskan data pribadi nasabah kepada pihak lain di luar badan hukum Bank untuk tujuan komersial, maka Bank harus mendapatkan persetujuan tertulis dari nasabah.

Bank juga harus memberikan penjelasan secara tertulis dan/atau lisan kepada nasabah mengenai tujuan dan konsekuensi dari pemberian persetujuan terhadap permintaan tertulis atau penyebarluasan data pribadi nasabah.

---

<sup>23</sup> *Ibid.*, p.209.

Permintaan persetujuan tertulis tidak boleh mencakup klausul yang dapat digunakan secara sepihak oleh Bank untuk menyatakan bahwa nasabah telah memberikan persetujuan jika tidak memberikan tanda, tulisan, dan/atau tanda tangan pada lembaran permintaan persetujuan tertulis yang diajukan oleh Bank. Data pribadi nasabah yang memerlukan persetujuan tertulis untuk dapat diberikan atau disebarluaskan kepada pihak lain di luar badan hukum Bank untuk tujuan komersial adalah: a. Alamat; b. Tanggal lahir dan/atau umur; c. Nomor telepon; d. Nama ibu kandung; dan e. Keterangan lain yang merupakan identitas pribadi dan biasanya diberikan oleh Nasabah kepada Bank dalam pemanfaatan Produk Bank.

## **2. Langkah-Langkah Hukum untuk Melindungi Kerahasiaan dan Keamanan Data Pribadi Nasabah Perbankan**

Perbankan berfungsi sebagai lembaga perantara keuangan (*financial intermediation*) dalam sistem pembayaran, yang memiliki peranan sangat krusial dalam mendorong pertumbuhan perekonomian nasional. Oleh karena itu, keberadaan perbankan diharapkan dapat mendukung pelaksanaan pembangunan. Hal ini sesuai dengan yang dinyatakan dalam Pasal 4 Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan yang telah diubah dengan Undang-Undang Nomor 10 Tahun 1998, yang menyatakan bahwa tujuan Perbankan Indonesia adalah untuk mendukung pelaksanaan pembangunan nasional demi meningkatkan pemerataan, pertumbuhan ekonomi, dan stabilitas nasional menuju peningkatan kesejahteraan masyarakat luas. Lembaga keuangan bank (*bank financial institution*) adalah badan usaha yang menjalankan kegiatan di sektor keuangan dengan mengumpulkan dana dari masyarakat dalam bentuk simpanan dan menyalurkannya kepada masyarakat dalam bentuk pinjaman<sup>24</sup>.

Pelaksanaan kegiatan usaha perbankan yang meliputi kegiatan penghimpunan dana dan penyaluran dana perlu dilandasi dengan asas-asas hukum di bidang perbankan. Salah satu asas penting dalam kegiatan usaha perbankan adalah Asas Kepercayaan (*Fiduciary Principle*). *Fiduciary Principle* adalah asas yang menyatakan bahwa usaha bank dilandasi oleh hubungan kepercayaan antara bank dan nasabahnya.

---

<sup>24</sup> Abdulkadir Muhammad dan Rilda Murniati, *Segi Hukum Lembaga Keuangan dan Pembiayaan (Edisi Revisi)*, Citra Aditya Bakti, Bandung, 2004, p.17.

Bank beroperasi dengan dana dari masyarakat yang disimpan padanya atas dasar kepercayaan, sehingga setiap bank wajib menjaga kepercayaan masyarakat padanya. Hubungan antara bank dan nasabah penyimpan dana adalah hubungan pinjam-meminjam uang antara *debitor* (bank) dan *kreditor* (nasabah penyimpan dana) yang dilandasi oleh asas kepercayaan, yang dengan asas kepercayaan itu, akan timbul beban kewajiban-kewajiban kepercayaan (*fiduciary obligation*) kepada bank terhadap nasabahnya.<sup>25</sup>

Asas yang harus ada dalam kegiatan usaha perbankan adalah Kerahasiaan (*confidential Principle*), yaitu asas yang mengharuskan atau mewajibkan bank untuk merahasiakan segala hal yang berkaitan dengan keuangan dan lainnya dari nasabah bank yang menurut praktik umum di dunia perbankan harus dirahasiakan. Asas kerahasiaan dalam kegiatan usaha perbankan berkaitan dengan rahasia bank serta rahasia jabatan dari setiap pegawai dan pihak yang terafiliasi dengan bank. Secara umum, asas kerahasiaan sangat terkait dengan kepercayaan, yaitu untuk menjaga kepercayaan nasabah penyimpan kepada bank.<sup>26</sup>

Prinsip atau teori yang mendasari rahasia bank yang ada hingga saat ini adalah bersifat mutlak, bank memiliki kewajiban untuk menjaga rahasia nasabah yang diketahui oleh bank akibat kegiatan usahanya dalam segala keadaan, baik biasa maupun luar biasa dan bersifat nisbi atau relatif, bank diperbolehkan untuk membuka rahasia nasabahnya jika untuk kepentingan mendesak, seperti kepentingan negara. Berdasarkan teori rahasia bank yang bersifat mutlak, bahwa sudah sepatutnya bank yang telah memiliki hubungan kontraktual dengan nasabah, berkewajiban menjaga kerahasiaan segala informasi mengenai nasabahnya, agar bank tidak kehilangan kepercayaan dari masyarakat pengguna jasa bank (nasabah penyimpan dana). Upaya perlindungan terhadap kerahasiaan dan keamanan data pribadi nasabah bank juga menjadi tugas dan fungsi pemegang kebijakan di bidang jasa keuangan. Perlindungan terhadap konsumen pengguna jasa keuangan dalam hal ini adalah nasabah bank, sebelumnya menjadi kewenangan Bank Indonesia sebagai lembaga negara yang memiliki fungsi pengawasan dalam kegiatan usaha perbankan.<sup>27</sup>

---

<sup>25</sup> Rachmadi Usman, *Aspek-Aspek Hukum Perbankan di Indonesia*, Gramedia Pustaka Utama, Jakarta, 2001), p. 26-30.

<sup>26</sup> Muhammad Djumhana, *Asas-Asas Hukum Perbankan Indonesia*, Citra Aditya Bakti, Bandung, 2008, p. 202.

<sup>27</sup> *Ibid.*, p. 172.

Secara teoritis, terdapat 2 aliran (*school of thought*) dalam hal pengawasan lembaga keuangan. Pertama aliran yang mengatakan bahwa pengawasan industri keuangan sebaiknya dilakukan oleh beberapa institusi. Kedua aliran yang berpendapat pengawasan industri keuangan lebih tepat jika dilakukan beberapa lembaga. Di Inggris misalnya industri keuangannya diawasi oleh *Financial Supervisory Authority* (FSA), sedangkan di Amerika, industri keuangan diawasi oleh beberapa institusi. SEC misalnya mengawasi perusahaan sekuritas sedangkan industri perbankan diawasi oleh bank sentral (*the Fed*), FDIC dan OCC<sup>28</sup>.

Secara empiris, penelitian yang dilakukan oleh *Central Banking Publication* (1999) menunjukkan bahwa dari 123 negara yang diteliti, tiga perempatnya memberikan kewenangan pengawasan industri perbankan kepada bank sentral. Hal ini lebih terlihat di negara-negara yang sedang berkembang. Khusus untuk negara berkembang, alasannya adalah terkait masalah sumber daya (*resources*). Bank sentral dianggap cukup memadai dalam hal sumber daya (SDM dan dana). Dari sudut pandang politik, pencabutan kewenangan pengawasan dari bank sentral sejalan dengan munculnya kecenderungan untuk memberikan independensi kepada bank sentral. Ada kekhawatiran bahwa dengan adanya independensi bank sentral, jika bank sentral juga memiliki kewenangan untuk mengawasi bank, maka bank sentral akan memiliki kekuasaan yang sangat besar. Sebagai contoh, *Bank of England* pada tahun 1997 memperoleh independensinya dan dua minggu kemudian kewenangan pengawasan bank diambil alih dari bank sentral tersebut<sup>29</sup>.

Peran strategis lembaga perbankan dalam ekonomi masyarakat di Indonesia saat ini sangat berpengaruh. Bank sebagai lembaga yang berfungsi sebagai intermediasi, maka pihak perbankan harus memiliki tanggung jawab yang penting dalam menghimpun dana dari berbagai sumber dan menyediakannya kembali kepada masyarakat dalam bentuk kredit atau bentuk lainnya. Fungsi intermediasi ini menghidupkan perputaran uang di dalam perekonomian dengan mengalirkan dana dari pihak-pihak yang memiliki kelebihan dana ke pihak-pihak yang membutuhkan dana. Dana yang dikumpulkan oleh bank merupakan dana yang dipercayakan masyarakat yang harus dikelola dengan hati-hati dan transparan.

---

<sup>28</sup> Zulkarnain Sitompul, *Menyambut Kehadiran Otoritas Jasa Keuangan (OJK)*, Jurnal Pilars, Vol.7, No.2 (Januari 2004), p.1-4.

<sup>29</sup> *Ibid.*, p.2.

Keberadaan regulasi yang baik diperlukan untuk melindungi dana tersebut agar tidak menimbulkan kerugian bagi pihak-pihak yang terlibat, termasuk melindungi pihak bank itu sendiri. Kerugian yang terjadi dapat berdampak secara signifikan pada perekonomian negara secara keseluruhan. Maka, tindakan pencegahan dan pengelolaan yang bijaksana terhadap dana masyarakat menjadi sangat penting bagi bank dalam menjalankan perannya sebagai lembaga intermediasi.<sup>30</sup>

Dana yang dihimpun oleh lembaga perbankan dalam bentuk simpanan didasarkan pada kepercayaan yang diberikan oleh nasabah kepada lembaga tersebut, sehingga keamanan dan kerahasiaan dana serta data nasabah yang disimpan di bank dapat terjamin. Dalam konteks perbankan, prinsip kehati-hatian memerlukan perhatian yang khusus. Prinsip ini menegaskan bahwa bank harus mengambil langkah-langkah pencegahan untuk melindungi dana masyarakat sebagai konsumen atau nasabah yang menyimpan dana di bank, termasuk dalam menjaga data nasabah itu sendiri. Penerapan prinsip kehati-hatian dalam aktivitas perbankan merupakan upaya yang dilakukan oleh lembaga perbankan untuk mengurangi risiko yang muncul dalam kegiatan tersebut, termasuk upaya untuk mencegah terjadinya kebocoran data nasabah.<sup>31</sup>

Kerahasiaan bank merupakan salah satu elemen penting dalam interaksi antara lembaga perbankan dan nasabah. Hal ini mencakup kepercayaan yang diberikan oleh nasabah kepada bank bahwa informasi mengenai data pribadi mereka akan tetap aman dan terlindungi. Sebagai institusi keuangan yang dipercaya, bank harus bertanggung jawab untuk menjaga kerahasiaan semua informasi yang berkaitan dengan nasabah. Kepercayaan ini menjadi dasar hubungan antara nasabah dan bank, sehingga nasabah merasa tenang dalam menggunakan layanan perbankan untuk menyimpan dan mengelola dana serta data pribadi mereka. Dengan jaminan kerahasiaan data nasabah, diharapkan bank tidak akan menyalahgunakan informasi mengenai data pribadi nasabah.<sup>32</sup>

---

<sup>30</sup> Johannes Ibrahim, *Pertanggungjawaban Pidana Bank dalam Pelanggaran Kegiatan Operasional Didasarkan pada Undang-Undang Nomor 10 Tahun 1998*, Jurnal Dialogia Iuridica, Vol.7, No.2 (April 2016), p.44.

<sup>31</sup> Rachmadi Usman, *Op.Cit.*, p.21.

<sup>32</sup> Alfred Yetno, *Tanggung Jawab Bank Dalam Menjaga Keamanan dan Kerahasiaan Data Nasabah Perbankan Di Indonesia*, Morality: Jurnal Ilmu Hukum, Vol.10, No.1, (Juni 2024), p. 67-76.

Apabila pihak perbankan tidak melaksanakan tugas dan tanggung jawabnya secara profesional, hal ini dapat menimbulkan dampak signifikan yang merugikan nasabah. Untuk melindungi hal ini, pemerintah mengambil langkah-langkah preventif dan represif guna menjaga kepentingan masyarakat serta memastikan stabilitas sistem keuangan tetap terjaga dengan baik. Pengaturan mengenai sistem perbankan umumnya diatur dengan ketat melalui berbagai undang-undang dan peraturan yang bertujuan untuk mengawasi serta mengatur aktivitas perbankan. Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan menjadi dasar hukum utama yang mengatur kegiatan perbankan di Indonesia. Dalam peraturan tersebut terdapat berbagai ketentuan mengenai tanggung jawab bank, kepatuhan terhadap peraturan, dan prinsip kehati-hatian yang wajib diterapkan oleh pihak perbankan. Tujuannya adalah untuk memastikan bahwa pihak perbankan menjalankan operasionalnya dengan aman, transparan, dan bertanggung jawab terhadap kepentingan nasabah serta sistem keuangan secara keseluruhan di Indonesia.<sup>33</sup>

Keamanan data nasabah perbankan kini menjadi fokus utama dalam industri perbankan di Indonesia. Hal ini disebabkan oleh fakta bahwa data nasabah sering kali berisi informasi pribadi dan sensitif yang dapat disalahgunakan untuk tindakan kriminal seperti pencurian identitas atau penipuan. Oleh karena itu, perlindungan terhadap data dan dana nasabah yang melakukan transaksi perbankan sangat penting untuk membangun kepercayaan nasabah dalam melakukan berbagai jenis transaksi perbankan. Perlindungan data nasabah perbankan adalah aspek yang sangat krusial dan menjadi perhatian utama dalam industri perbankan di Indonesia. Tanggung jawab bank adalah untuk menjaga kerahasiaan semua informasi yang berkaitan dengan data nasabah, termasuk informasi keuangan dan data pribadi nasabah.

Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan Atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan. Disebutkan dalam Pasal 40 ayat (1) yang berbunyi, bank wajib merahasiakan keterangan mengenai Nasabah penyimpan dan simpanannya, kecuali dalam hal sebagaimana dimaksud dalam Pasal 41, Pasal 41A, Pasal 42, Pasal 44, dan Pasal 44A. Sedangkan OJK telah menerbitkan Surat Edaran Nomor 14/SEOJK.07/2014 mengenai Kerahasiaan dan

---

<sup>33</sup> *Ibid.*, p. 71-72.

Keamanan Data serta/atau Informasi Pribadi Konsumen. Surat edaran ini mengatur para PUJK, di mana pihak perbankan diwajibkan untuk melindungi data dan informasi pribadi konsumen. Mereka dilarang memberikan data dan informasi pribadi konsumen kepada pihak ketiga dengan cara apa pun. Meskipun peraturan perundang-undangan ini telah menetapkan ketentuan yang jelas mengenai perlindungan data nasabah, kenyataannya masih terdapat kasus penyalahgunaan data pribadi nasabah oleh oknum yang tidak bertanggung jawab. Oleh karena itu, bank perlu meningkatkan sistem keamanan dan pengawasan terhadap data nasabah agar penyalahgunaan data pribadi tidak terjadi. Perlindungan data nasabah di sektor perbankan bukan hanya sekadar kepatuhan terhadap peraturan, tetapi juga mencerminkan tanggung jawab etis untuk menjaga privasi dan keamanan nasabah. Perlindungan data nasabah sangat penting dalam membangun rasa kepercayaan nasabah dalam setiap aktivitas transaksi perbankan.<sup>34</sup>

Ketika kasus hukum terkait kejahatan siber yang dapat mempengaruhi sektor perbankan muncul, maka Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik menjadi peraturan yang relevan dan digunakan dalam situasi tersebut. Aturan dalam undang-undang ini mengatur aspek keamanan data serta transaksi elektronik, termasuk perlindungan terhadap pencurian data dan serangan siber lainnya. Oleh karena itu, pihak perbankan juga diwajibkan untuk mematuhi peraturan ini dan menerapkan langkah-langkah keamanan siber yang efektif guna melindungi informasi dan data nasabah. Pemerintah Indonesia telah mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Pengaturan mengenai perlindungan data pribadi menjadi sangat penting untuk memberikan dasar hukum dalam memastikan keamanan data pribadi. Tujuan dari perlindungan data pribadi juga mencakup jaminan hak-hak individu dalam menjaga privasi mereka, meningkatkan kesadaran masyarakat, serta memastikan pengakuan dan penghormatan terhadap pentingnya perlindungan data pribadi. Secara keseluruhan, implementasi kedua peraturan perundang-undangan ini krusial untuk menjaga stabilitas dalam kegiatan perbankan dan mencegah terjadinya kejahatan,

---

<sup>34</sup> Qatrunnada Ernanti, dkk, *Perlindungan Hukum Bagi Konsumen Perbankan dalam Penggunaan Data Pribadi Nasabah (Studi pada PT BRI Kantor Wilayah Semarang)*, Diponegoro Law Journal, Vol.5, No.3 (2016), p.1-5.

khususnya di dunia siber. Selain itu, pengawasan yang ketat dan penegakan hukum yang tegas juga diperlukan untuk menjamin kepercayaan masyarakat terhadap lembaga perbankan<sup>35</sup>.

Oleh karena itu, dalam konteks ini, Undang-Undang Nomor 10 Tahun 1998 mengenai Perbankan harus memberikan jaminan hukum yang berkaitan dengan perlindungan data nasabah untuk memastikan keamanan data nasabah yang dikelola oleh pihak perbankan. Selain itu, perlindungan data nasabah bertujuan untuk menjamin hak nasabah atas perlindungan data mereka serta memastikan pengakuan dan penghormatan terhadap pentingnya perlindungan data nasabah oleh pihak perbankan. Dalam Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan terdapat ketentuan yang mengatur perlindungan dana masyarakat yang disimpan di bank. Oleh karena itu, pihak perbankan diwajibkan untuk mendirikan lembaga penjamin simpanan yang bertugas menjamin dana masyarakat yang disimpan di bank. Namun, meskipun demikian, peraturan undang-undang tersebut tidak secara spesifik mengatur perlindungan data nasabah seperti halnya perlindungan terhadap dana nasabah<sup>36</sup>.

Di dalam Undang-Undang Nomor 19 Tahun 2016 mengenai Informasi dan Transaksi Elektronik, terdapat peningkatan keamanan dan kenyamanan bagi nasabah saat melakukan aktivitas perbankan melalui sistem elektronik yang disediakan oleh pihak perbankan. Ada beberapa alasan, antara lain, bahwa peraturan tersebut menegaskan bahwa pihak perbankan berperan sebagai penyelenggara sistem elektronik yang menawarkan layanan perbankan melalui Internet (e-banking), sehingga mereka bertanggung jawab secara hukum atas kerugian yang dialami nasabah akibat penggunaan layanan yang mereka sediakan. Namun, jika kerugian tersebut disebabkan oleh force majeure atau kesalahan serta kelalaian dari pihak nasabah, maka bank tidak akan bertanggung jawab. Pihak perbankan diwajibkan untuk menyelenggarakan sistem elektronik yang aman dan bertanggung jawab atas operasional sistem elektronik yang mereka kelola.<sup>37</sup>

---

<sup>35</sup> Sinta Dewi Rosadi, *Pembahasan UU Data Pribadi (UU RI NO.27 Tahun 2022)*, Sinar Grafika, Jakarta, 2023, p.51.

<sup>36</sup> Tiar Lina Situngkir; dkk, *Bank dan Lembaga Keuangan Non Bank*, Pusaka Rumah Citra, Jawa Tengah, 2020, p.102.

<sup>37</sup> Sumiaty Adelina Hutabarat, dkk., *CYBER-LAW: Quo Vadis Regulasi UU ITE dalam Revolusi Industri 4.0 Menuju. Era Society 5.0*, Sopenidia Publising Indonesia, Jambi, 2023, p.101.

Dari hal tersebut, dapat disimpulkan bahwa telah ada upaya yang dilakukan untuk melindungi nasabah dalam layanan perbankan, termasuk perlindungan data yang dikumpulkan, dimanfaatkan, atau digunakan untuk keperluan transaksi oleh nasabah. Selain itu, perlindungan terhadap data pribadi nasabah yang menggunakan layanan internet banking diperketat dengan persyaratan tertentu, seperti kewajiban untuk melakukan pemindaian wajah dan tanda tangan. Namun, meskipun upaya perlindungan telah dilakukan, ancaman kejahatan siber atau cyber crime masih tetap ada. Pihak perbankan akan bertanggung jawab atas kerugian yang dialami oleh nasabah pengguna internet banking jika terjadi kesalahan teknis atau kebocoran data nasabah akibat kelalaian dari pihak perbankan. Pihak perbankan juga akan memberikan perlindungan hukum kepada nasabah yang mengalami kerugian sesuai dengan ketentuan UU Perbankan.

Dalam hal ini, penting bagi pihak perbankan untuk memberikan perlindungan hukum kepada nasabah yang menggunakan produk-produk mereka. Perlindungan hukum ini sangat penting karena akan memperkuat kepercayaan masyarakat terhadap produk dan layanan perbankan sebagai konsumen. Perlindungan dan pemberdayaan terhadap nasabah sebagai konsumen merupakan tanggung jawab utama perbankan di Indonesia. Dengan menempatkan perlindungan nasabah sebagai konsumen, perbankan menunjukkan komitmen pemerintah dan lembaga perbankan dalam upaya memberikan posisi nasabah sebagai konsumen yang sejajar dengan pihak perbankan. Prinsip inilah yang perlu ada dalam UU Perbankan berkaitan dengan perlindungan data nasabah, sehingga kasus hukum yang merugikan nasabah akibat force majeure atau kesalahan dan kelalaian nasabah tidak sepenuhnya dibebankan kepada nasabah itu sendiri. Oleh karena itu, pihak perbankan harus memiliki sistem elektronik yang aman serta bertanggung jawab terhadap operasional sistem elektronik yang mengedepankan perlindungan data bagi nasabah dan memiliki prioritas utama dalam melindungi data nasabah.

### **C. PENUTUP**

Sebagai negara hukum yang menjunjung tinggi prinsip demokrasi dan hak asasi manusia, Indonesia secara konstitusional memberikan jaminan terhadap hak atas privasi dan perlindungan data pribadi sebagai bagian integral dari penghormatan terhadap martabat manusia. Perlindungan ini tidak hanya bersifat deklaratif, melainkan juga memerlukan penerapan konkret oleh setiap entitas, termasuk pelaku usaha, penyelenggara sistem elektronik, dan lembaga keuangan, dalam menjalankan kewajiban yuridis dan etis sebagaimana diamanatkan dalam peraturan perundang-undangan yang berlaku.

Dasar normatif pertama yang mengakui hak atas data pribadi sebagai bagian dari hak privasi tercermin dalam Pasal 26 UU ITE. Pasal ini secara eksplisit mensyaratkan bahwa penggunaan informasi yang menyangkut data pribadi seseorang harus memperoleh persetujuan dari subjek data. Pelanggaran terhadap ketentuan ini tidak hanya menimbulkan tanggung jawab perdata, tetapi juga membuka ruang bagi tindakan hukum lainnya. Prinsip serupa dikuatkan dalam Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia, khususnya Pasal 21, yang melarang penggunaan data pribadi, termasuk data biometrik seperti gambar dan suara, tanpa persetujuan eksplisit dari individu yang bersangkutan.

Pengaturan lebih lanjut terkait data kependudukan tercantum dalam Undang-Undang Nomor 24 Tahun 2013 yang mengubah Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan. Dalam peraturan ini ditegaskan bahwa data perseorangan dan dokumen kependudukan wajib dijaga kerahasiaannya oleh negara. Akan tetapi, Peraturan Presiden Nomor 67 Tahun 2011 yang mengatur penerapan KTP elektronik secara nasional belum sepenuhnya memberikan jaminan atas keamanan dan kerahasiaan data biometrik penduduk, sehingga menimbulkan kekhawatiran akan potensi penyalahgunaan di era digital yang sangat terbuka.

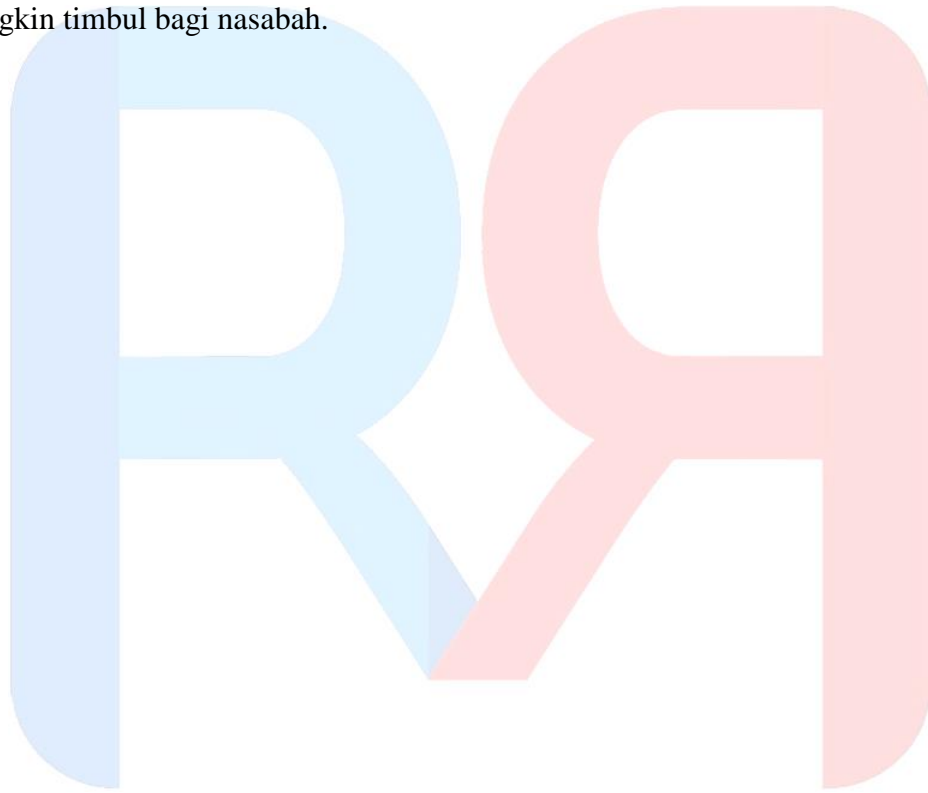
Di sektor teknologi informasi, Permenkominfo No. 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik telah mengatur prinsip perlindungan data pribadi seperti keabsahan pengumpulan, transparansi, pembatasan penggunaan, dan hak subjek data untuk melakukan akses dan koreksi.

Namun demikian, sanksi atas pelanggaran terhadap regulasi ini masih bersifat administratif dan belum memberikan efek jera yang memadai, terutama dalam menghadapi eskalasi kejahatan siber yang semakin kompleks. Sebaliknya, sektor perbankan dan keuangan menunjukkan pendekatan yang lebih progresif.

UU Perbankan menegaskan kewajiban lembaga keuangan untuk menjaga kerahasiaan data nasabah sebagai bentuk kewajiban fidusia. Pendekatan ini diperkuat oleh POJK No. 13/POJK.02/2018 yang mewajibkan penyelenggara jasa keuangan untuk menjamin kerahasiaan, integritas, dan ketersediaan data pribadi, data transaksi, dan data keuangan sejak saat pengumpulan hingga pemusnahan. Ketentuan ini bertujuan untuk meminimalkan risiko serangan siber, seperti pencurian identitas dan phishing, yang berpotensi merugikan konsumen secara ekonomi dan sosial. Untuk itu, pendekatan *risk-based* dalam manajemen data menjadi sangat penting. Hal ini mencakup pelaksanaan audit keamanan data secara berkala, penguatan sistem proteksi siber, serta penetapan prosedur mitigasi yang efektif. Kejahatan terhadap data pribadi harus dipandang sebagai bentuk pelanggaran serius terhadap hak asasi manusia dan sebagai ancaman terhadap stabilitas sistem keuangan digital, sehingga memerlukan penegakan hukum yang tegas dan pemberlakuan sanksi yang proporsional.

Dalam konteks internasional, APEC Privacy Framework menawarkan prinsip-prinsip dasar yang dapat dijadikan acuan etis dan normatif dalam perlindungan data pribadi. Prinsip-prinsip tersebut meliputi pemberian informasi kepada subjek data (*notice*), persetujuan (*consent*), pembatasan pengumpulan (*collection limitation*), penggunaan sesuai tujuan (*use limitation*), keamanan (*security*), akurasi data (*data quality*), serta akuntabilitas (*accountability*). Data pribadi harus dikumpulkan secara sah, digunakan untuk tujuan yang telah ditentukan, dan tidak boleh disebarluaskan tanpa persetujuan, kecuali diatur secara tegas oleh hukum atau dibenarkan oleh alasan yang sah secara hukum. Hak-hak subjek data meliputi hak untuk mengetahui data yang dikumpulkan, mengakses data tersebut, serta melakukan koreksi apabila terjadi kesalahan atau ketidaksesuaian.

Di sisi lain, pengelola data wajib menjaga akurasi, integritas, dan keamanan data serta memastikan bahwa data tersebut tidak disimpan melebihi jangka waktu yang diperlukan, kecuali ditentukan lain oleh ketentuan hukum. Dalam konteks sektor perbankan, praktik terbaik mewajibkan persetujuan tertulis dari nasabah atas setiap penggunaan data pribadi untuk keperluan komersial. Persetujuan tersebut harus diperoleh secara sadar dan bebas, serta tidak boleh tersembunyi dalam klausul baku yang berpotensi menyesatkan. Selain itu, bank memiliki kewajiban untuk memberikan penjelasan yang transparan, baik secara lisan maupun tertulis, mengenai tujuan penggunaan data dan konsekuensi yang mungkin timbul bagi nasabah.



## DAFTAR PUSTAKA

### Buku

- Djumhana, Muhammad. 2008. *Asas-Asas Hukum Perbankan Indonesia*. (Bandung: Citra Aditya Bakti).
- Gazali, Djoni S dan Rachmadi Usman. 2010. *Hukum Perbankan*. (Jakarta: Sinar Grafika, Jakarta).
- Husein, Yunus. 2010. *Rahasia Bank dan Penegakan Hukum*. (Jakarta: Pustaka Juanda Tigalima).
- Hutabarat, Sumiaty Adelina, dkk.. 2023. *CYBER-LAW: Quo Vadis Regulasi UU ITE dalam Revolusi Industri 4.0 Menuju Era Society 5.0*. (Jambi: Sopendia Publising Indonesia).
- Iman, Nofie. 2016. *Financial Technology dan Lembaga Keuangan*. (Yogyakarta: Gathering Mitra Linkage Bank Syariah Mandiri)
- Muhammad, Abdulkadir dan Rilda Murniati. 2004. *Segi Hukum Lembaga Keuangan dan Pembiayaan (Edisi Revisi)*. (Bandung: Citra Aditya Bakti).
- Situngkir; Tiar Lina, dkk. 2020. *Bank dan Lembaga Keuangan Non Bank*. (Jawa Tengah: Pusaka Rumah Citra).
- Soekanto, Soerjono. 1996. *Pengantar Penelitian Hukum*. (Jakarta: UI Press).
- Soekanto, Soerjono. dan Sri Mamudji. 2003. *Penelitian Hukum Normatif (Suatu Tinjauan Singkat)*. (Jakarta: Raja Grafindo Persada).
- Rosadi, Sinta Dewi. 2023. *Pembahasan UU Data Pribadi (UU RI NO. 27 Tahun 2022)*. (Jakarta: Sinar Grafika).
- Ridwan, HR. 2011. *Hukum Administrasi Negara*. (Jakarta: RajaGrafindo Perkasa).
- Usman, Rachmadi. 2001. *Aspek-Aspek Hukum Perbankan di Indonesia*. (Jakarta: Gramedia Pustaka Utama).

### Publikasi Ilmiah

- Ernanti, Qatrunnada, dkk.. *Perlindungan Hukum bagi Konsumen Perbankan Dalam Penggunaan Data Pribadi Nasabah (Studi pada PT BRI Kantor Wilayah Semarang)*. Diponegoro Law Journal. Vol.5. No.3 (2016).
- Gracia, Gracia, dkk.. *Implementasi Konsep Euthanasia: Supremasi Hak Asasi Manusia dan Progresivitas Hukum di Indonesia*. Ikatan Penulis Mahasiswa Hukum Indonesia Law Journal. Vol.2. No.1 (2022).
- Kusniati, Retno. *Sejarah Perlindungan Hak-Hak Asasi Manusia dalam Kaitannya dengan Konsepsi Negara Hukum*. Jurnal Inovatif Hukum. Vol.4. No.5 (2019).
- Ibrahim, Johannes. *Pertanggungjawaban Pidana Bank dalam Pelanggaran Kegiatan Operasional Didasarkan pada Undang-Undang Nomor 10 Tahun 1998*. Jurnal Dialogia Iuridica. Vol.7. No.2 (April 2016).
- Munir, Abu Bakar, dkk.. *Data Protection Law in Asia*. International Data Privacy Law Journal. Vol.8. No.4 (November 2018).
- Priliasari, Erna. *Pentingnya Perlindungan Data Pribadi dalam Transaksi Pinjaman Online (The Urgency of Personal Protection in Peer to Peer Lending)*. Majalah Hukum Nasional. Vol.49. No.2 (2019).

- Rani, Marnia. *Perlindungan Otoritas Jasa Keuangan terhadap Kerahasiaan dan Keamanan Data Pribadi Nasabah Bank*. Jurnal Selat. Vol.2. No.1. (Oktober 2014).
- Rahmawati, Ineu. *Analisis Manajemen Risiko Ancaman Kejahatan Siber (Cyber Crime) dalam Peningkatan Cyber Defense*. Jurnal Pertahanan & Bela Negara. Vol.7. No.2 (Oktober 2017).
- Rosadi, Sinta Dewi. *Prinsip-Prinsip Perlindungan Data Pribadi Nasabah Kartu Kredit Menurut Ketentuan Nasional dan Implementasinya*. Jurnal Sosiohumaniora. Vol.19. No.3 (November 2017).
- Saad, Abdul Raman. *Personal Data & Privacy Protection*. Kelana Jaya Malaysia Journal. Vol.42. No.1 (2005).
- Sitompul, Zulkarnain. *Menyambut Kehadiran Otoritas Jasa Keuangan (OJK)*, Jurnal Pilars. Vol.7. No.2 (Januari 2004).
- Yetno, Alfred. *Tanggung Jawab Bank dalam Menjaga Keamanan dan Kerahasiaan Data Nasabah Perbankan di Indonesia*. Morality: Jurnal Ilmu Hukum. Vol.10. No.1 (Juni 2024).
- Yuniarti, Siti. *Perlindungan Hukum Data Pribadi di Indonesia*. Business Economic, Communication, and Social Sciences Journal (BECOSS). Vol.1. No.1 (2019).

#### **Karya Ilmiah**

- Djafar, Wahyudi. 2019. *Hukum Perlindungan Data Pribadi di Indonesia: Lanskap, Urgensi dan Kebutuhan Pembaruan*, Makalah disampaikan sebagai materi dalam kuliah umum, Tantangan Hukum dalam Era Analisis Big Data, (Yogyakarta: Program Pasca Sarjana Fakultas Hukum Universitas Gadjah Mada).