e-ISSN: 2830-1501

Jurnal Penelitian Ilmu-Ilmu Sosial
https://journals2.ums.ac.id/index.php/sosial
Volume 5, No. 1, 2024, Hal. 19-33
Research Article

Implementation of Data Protection Authority (DPA) in Indonesia: The Urgency of Legal Protection of Customer's Personal Data in E-Banking Service Transactions

Risqiana[1*], Jessenia Hayfa[2], Rizky Rani[3], Sheren Regina Wungkana[4]

[1] Fakultas Hukum, Universitas Jember, Jl. Kalimantan Nomor 37, Krajan Timur, Sumbersari, Jember, East Java, 68121, Indonesia
[2] Fakultas Hukum, Universitas Jember, Jl. Kalimantan Nomor 37, Krajan Timur, Sumbersari, Jember, East Java, 68121, Indonesia
[3] Fakultas Hukum, Universitas Jember, Jl. Kalimantan Nomor 37, Krajan Timur, Sumbersari, Jember, East Java, 68121, Indonesia
[4] Fakultas Hukum, Universitas Jember, Jl. Kalimantan Nomor 37, Krajan Timur, Sumbersari, Jember, East Java, 68121, Indonesia

*Corresponding author's email: risqiana609@gmail.com

Abstract

The development of science and technology has led to significant changes, shifting global supply chains into the digital and virtual realm. One of the technological advancements that offers new business opportunities, particularly in the banking sector, is e-banking, which transforms the way transactions are conducted, making them cashless. However, substantial progress in digital banking technology also brings high risks, encompassing both tangible and intangible losses, significantly if customer rights are weakened due to the bank's violations. Currently, the ITE Law and the Personal Data Protection Law in Indonesia are inadequate for safeguarding customers in the context of e-banking services. Therefore, this research aims to achieve customer security and protection from personal data leakage and fraud risks by implementing the Data Protection Authority (DPA). This approach also encourages banks to take responsibility for their actions and provides a strong legal basis for customers to seek compensation for potential losses. To address this issue, our research employs a normative juridical research method, which examines legal norms, principles, and doctrines related to protecting customers' data in digital-based banking transactions. The Data Protection Authority (DPA) is proposed as a crucial legal protection concept for safeguarding customer personal data, playing a vital role in preventing cybercrime and the misuse of personal information. With the establishment of a comprehensive DPA, law enforcement against violations in digital-based banking transactions will become more effective, preserving an individual's freedom of expression and supporting the mission of sustainable development.

Keywords: *data protection authority, personal data, e-banking*

Abstrak

Perkembangan ilmu pengetahuan dan teknologi telah menciptakan perubahan besar dengan beralihnya rantai suplai global ke ranah digital dan virtual. Salah satu perkembangan teknologi yang memberikan peluang bisnis baru, terutama untuk jasa perbankan, adalah e-banking yang mengubah cara bertransaksi menjadi tanpa tunai. Namun, kemajuan signifikan dalam teknologi perbankan digital juga membawa risiko tinggi, termasuk kerugian materiil dan immateriil, terutama jika hak nasabah menjadi lemah karena pelanggaran dari pihak bank. Saat ini, Undang-Undang ITE dan Undang-Undang Perlindungan Data Pribadi belum cukup memadai untuk melindungi nasabah dalam konteks layanan e-banking di Indonesia. Sehingga dalam hal ini, penelitian yang mendasarkan pada penerapan Data Protection Authority (DPA) bertujuan untuk mencapai keamanan dan perlindungan nasabah dari risiko kebocoran data pribadi dan penipuan. Selain itu, mendorong pihak bank untuk bertanggung jawab atas tindakan mereka, dengan dasar hukum yang kuat bagi nasabah untuk menuntut ganti rugi atas kerugian yang mungkin terjadi.

Untuk mengatasi hal tersebut, maka penelitian ini menggunakan metode penelitian yuridis normatif yang meninjau dari sisi norma dan prinsip hukum serta doktrin-doktrin yang berkaitan dalam mengevaluasi perlindungan data pribadi nasabah dalam transaksi perbankan berbasis digital. Data Protection Authority (DPA) diangkat sebagai konsep perlindungan hukum terhadap data pribadi nasabah, yang memiliki peran penting dalam mencegah kejahatan cyber dan penyalahgunaan data pribadi. Dengan adanya DPA yang komprehensif, penegakan hukum terhadap pelanggaran dalam transaksi perbankan berbasis digital akan menjadi lebih efektif, mengamankan kebebasan berekspresi seseorang, dan mendukung misi pembangunan berkelanjutan.
Kata Kunci: *data protection authority, data pribadi, e-banking*

Diajukan: 30 Juli 2023 | Diterima: 29 Maret 2024 | Tersedia Online: 6 April 2024

Pendahuluan

Perkembangan teknologi masa kini terbilang sangat pesat yang menjadi momentum disruptif karena adanya perpindahan rantai suplai global ke dalam ruang digital dan virtual. Berbagai jenis kebutuhan sehari-hari tidak terlepas dari teknologi dan semacamnya, hal ini membuat posisi teknologi dalam kehidupan menjadi sangat fundamental. Teknologi yang canggih mampu mempermudah aktivitas manusia, baik di bidang industri, ekonomi, pemerintah, keuangan, dan lain sebagainya. Elemen-elemen dari kehidupan masyarakat telah dikuasai oleh teknologi yang semakin hari semakin memadai. Kemajuan teknologi dapat membuka peluang bisnis baru, terutama untuk layanan perbankan. Salah satu peluang tersebut adalah *e-banking*, yang memiliki potensi untuk mempengaruhi dan mengubah cara konsumen melakukan transaksi non-tunai (Aptika, 2021).

Pada awal tahun 2022, Bank Indonesia menunjukkan bahwa data pengguna transaksi *e-banking* telah mencapai 3,2 miliar dan mengalami peningkatan sebesar 67,87%, berbeda dengan tahun sebelumnya yang hanya berhasil memperoleh 1,90 miliar kali transaksi. Jenis transaksi yang paling banyak dilakukan adalah transfer antar bank yang mengalami pertumbuhan 76,06% menjadi 2,19 miliar kali, diikuti oleh transaksi pembayaran yang meningkat 57,20% menjadi 531,43 juta kali. Transaksi antar bank juga mengalami kenaikan 47,33% menjadi 474,58 juta kali. Dalam hal nilai, total transaksi *e-banking* dari awal tahun hingga Mei 2022 mencapai Rp 3.888,09 triliun, meningkat sebesar 43,76% dibandingkan tahun sebelumnya yang hanya Rp 2.704,61 triliun (Walfajri dkk., 2022).

Perubahan yang signifikan dalam bidang teknologi perbankan berbasis digital memicu masalah-masalah berisiko tinggi yang dapat mengakibatkan kerugian materiil dan immateriil. Salah satu masalah tersebut adalah, jika bank melanggar hak-hak nasabah, hak-hak tersebut cenderung terkikis. Dengan mengacu pada Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (Pemerintah Indonesia, 2022) dan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik atau yang dikenal dengan UU ITE (Pemerintah Indonesia, 2016), diketahui bahwa kedua undang-undang tersebut tidak secara tegas dan spesifik mengatur mengenai perlindungan hukum terhadap nasabah. Mengacu pada hal tersebut, maka perkembangan teknologi menjadi pisau bermata dua, berdampak positif apabila tujuan pembangunan nasional dapat tercapai, namun disisi lain menjadi tantangan yang dapat menghancurkan integrasi bangsa jika tidak mampu diakomodasi dengan baik sehingga setiap nasabah yang mengalami kerugian akibat kurangnya perlindungan hukum pada transaksi *e-banking* sewajarnya mendapatkan kompensasi atau jaminan (Sudaryanti dkk., 2021).

Selanjutnya, hal ini tidak terlepas dari Teori Interaktif Keadilan yang menyatakan bahwa kerangka konseptual yang membahas kebebasan negatif individu dalam konteks interaksi mereka dengan orang lain. Dalam pandangan Wright, Teori Interaktif Keadilan mengacu pada sebuah bentuk ganti rugi dimana merupakan alat dengan tujuan melindungi semua individu akibat adanya hubungan yang tidak menguntungkan, terutama diimplementasikan dalam bidang Hukum Perdata (*tort law*), Hukum Kontrak,

dan Hukum Pidana (Nurdinisari, 2013). Dalam teori ini, kompensasi berperan sebagai sarana untuk mengatasi dampak negatif dari interaksi yang merugikan dan memberikan jaminan bahwa individu akan dilindungi dari efek buruk yang mungkin timbul akibat tindakan atau perilaku orang lain (Nurdinisari, 2013). Maka dalam hal ini, berkaitan pula dengan konsep *Data Protection Authority* (DPA) yang dimana adanya tanggung jawab memberikan perlindungan hukum kepada nasabah dengan menyediakan fasilitas yang membantu jika terjadi kerugian akibat penggunaan layanan *e-banking*. Dalam situasi tersebut, apabila nasabah menghadapi kerugian, maka perlu adanya tanggung jawab mutlak (*strict liability*) berupa tuntutan ganti rugi melalui proses pengadilan atas pelanggaran hukum oleh bank atau lembaga keuangan terkait.

Di Indonesia sendiri, salah satu ancaman serius yang mengaplikasikan metode rekayasa sosial dengan tujuan menipu pengguna atau pelanggan adalah *phising*. Seringkali, para penjahat menyamar sebagai pejabat bank dan mengirimkan penawaran menarik melalui email, pesan singkat, atau panggilan telepon untuk memancing nasabah memberikan data rahasia terkait akun bank mereka. Faktor utama yang memperkuat kejahatan *phising* pada bidang perbankan secara online yaitu minimnya kesadaran dari para pengguna terhadap taktik kejahatan semacam ini dan kurangnya langkah-langkah keamanan yang kuat oleh bank dan penyedia layanan perbankan online. Keadaan ini mengindikasikan bahwa jaminan perlindungan hukum kepada para nasabah pada konteks layanan *e-banking* di Indonesia saat ini belum memadai (Rahmadhani dkk., 2023). Akibatnya, masyarakat menghadapi kesulitan dalam upaya memperjuangkan hak-hak yang telah dilanggar sebagai konsumen pada bidang jasa keuangan.

Oleh karena itu, studi ini ditujukan pada telaah terhadap beberapa penelitian sebelumnya sebagai rujukan. Salah satunya adalah studi yang dilakukan oleh Rahman (2021) yang membahas keamanan dan perlindungan data secara umum atas sistem pemerintahan berbasis elektronik (SPBE). Selanjutnya, merujuk pada riset yang ditulis oleh Mahesa Jati Kusuma tahun 2013. Penelitian tersebut berkaitan terhadap kejahatan *cyber* serta upaya perlindungan hukum bagi para korban dari perspektif pidana (Kusuma, 2013). Sementara itu, penelitian yang sedang disusun oleh Tim Penulis berfokus pada perlindungan korban pengguna *e-banking* saat bertransaksi pada bidang perbankan, dengan mempertimbangkan aspek hukum perdata serta tanggung jawab pihak bank atas kerugian nasabah ketika menggunakan layanan tersebut, termasuk keterlibatan *Data Protection Authority* (DPA). Berangkat dari permasalahan tersebut, Tim Penulis mendasarkan tulisan ini pada inti argumen terkait bagaimana implementasi perlindungan terhadap hak-hak dan privasi data pribadi nasabah dalam penggunaan *e-banking* di Indonesia dan apa urgensi penerapan *Data Protection Authority* (DPA) yang sifatnya krusial dan komprehensif sebagai bentuk penegakan hukum terhadap nasabah saat proses transaksi perbankan berbasis digital (Kusnadi dkk., 2021).

Metode Penelitian

Dengan menggunakan sebuah pendekatan yuridis normatif, penelitian ini mengkaji doktrin, norma, dan asas-asas hukum yang relevan untuk menilai perlindungan data pribadi di bawah UU Perlindungan Data Pribadi dan UU ITE. Pendekatan ini digunakan untuk menganalisis dan merumuskan perlindungan hukum yang sesuai pada permasalahan perlindungan data pribadi dalam layanan *e-banking*. Data-data yang digunakan berupa bahan hukum yang dikumpulkan secara sistematis melalui teknik pengumpulan data studi dokumenter atau studi kepustakaan. Oleh karena itu, penelitian ini menggunakan tiga jenis bahan hukum, yaitu bahan hukum primer yang berupa norma-norma hukum yang relevan, bahan hukum sekunder yang berupa buku-buku, jurnal, karya ilmiah, dan literatur hukum lainnya, serta bahan hukum tersier yang merupakan pelengkap dari bahan hukum primer dan sekunder. Pengecekan validitas data dalam penelitian diuji dilakukan melalui triangulasi sumber, yaitu dengan memverifikasi data menggunakan beberapa sumber untuk menentukan kebenaran dan kredibilitasnya. Penelitian ini diharapkan menghasilkan referensi hukum berupa konsep perlindungan hukum terhadap data pribadi nasabah melalui *Data Protection Authority* (DPA).

Hasil dan Pembahasan

Implementasi Perlindungan Terhadap Hak-Hak dan Privasi Data Pribadi Nasabah dalam Penggunaan E-Banking di Indonesia

Berkorelasi dengan gagasan *"the rule of Law, and not of Man"* diperkuat oleh undang-undang dan peraturan tertentu yang signifikan. Paradigma *"the rule of law"* sepenuhnya mengatur jaminan bahwa hukum adalah yang tertinggi (supremasi hukum), bahwa kesetaraan berlaku baik dalam pemerintahan maupun hukum (kesetaraan di hadapan hukum), dan bahwa diskriminasi tidak ada dengan memberikan prioritas utama pada hak asasi manusia (HAM) (Greenleaf, 2021). Perlindungan privasi dan data pribadi adalah isu global yang mendapat perhatian serius dari berbagai negara dan lembaga internasional. Uni Eropa telah memimpin upaya harmonisasi regulasi dengan *European Union General Data Protection Regulation* (EU GPRD) yang kuat. Begitu pula penerapan di Hong Kong, Malaysia, dan Singapura yang telah mengadopsi langkah-langkah untuk melindungi privasi dan data pribadi dengan masing-masing peraturan perundang-undangan yang relevan. Upaya ini menunjukkan kesadaran akan pentingnya melindungi informasi pribadi individu dan memberikan landasan hukum bagi pencegahan penyalahgunaan data serta menjaga kepercayaan masyarakat terhadap layanan digital. Perlindungan privasi dan data pribadi adalah komponen penting dalam era teknologi digital yang semakin canggih, dan tantangan ini terus menghadirkan perdebatan dan penyesuaian kebijakan di tingkat nasional dan internasional.

Nasabah yang menggunakan layanan e-banking dilindungi oleh perlindungan hukum pidana dan perdata. Dalam perspektif hukum perdata, nasabah dapat mengandalkan ketentuan hukum positif yang mengatur permasalahan tersebut. Di sisi lain, dalam perspektif hukum pidana, perlindungan hukum

berdasarkan Undang-Undang Nomor 8 Tahun 1981 tentang Kitab Undang-Undang Hukum Pidana juga tersedia (Pemerintah Indonesia, 1981). Jika seorang nasabah menjadi korban dalam transaksi *e-banking*, maka dapat menyelesaikan masalahnya melalui dua cara, yakni melalui proses litigasi atau non-litigasi, dan bergantung pada kasus yang dihadapinya, bisa meminta ganti rugi atau memulihkan kredibilitasnya. Tujuan dari layanan *e-banking* adalah untuk memungkinkan sistem layanan bank yang lebih cepat dan efektif. Namun, layanan ini harus ditangani dengan hati-hati agar tidak menimbulkan lebih banyak konsekuensi yang merugikan daripada menguntungkan. Hal ini disebabkan oleh fitur-fitur unik dari layanan *e-banking*, yang menimbulkan bahaya spesifik platform tertentu. Beberapa di antaranya adalah:

1. *Technology risk*: Terkait dengan kapabilitas dan keamanan sistem. Tingkat risiko teknologi yang harus dihadapi oleh bank yang menawarkan layanan *internet banking* sebagian besar ditentukan oleh kecanggihan teknologi dan perangkat lunak yang mereka gunakan.
2. *Reputational risk*: Hal ini berdampak langsung pada reputasi atau citra bank. Kepercayaan nasabah terhadap layanan *e-banking* sebagian besar bergantung pada reputasi bank yang menyelenggarakan perbankan online.
3. *Outsourcing risk*: Mayoritas bank yang menyediakan layanan perbankan online bergantung pada pihak lain untuk mengoperasikan dan memelihara data mereka, seperti *internet service provider* (ISP) atau operator data. Risiko yang mungkin timbul dari *outsourcing* ini termasuk kebangkrutan ISP yang menyebabkan layanan tertutup, kebocoran data karena keamanan ISP yang lemah, atau keterbatasan kapabilitas ISP.
4. *Legal risk*: Masalah hukum *e-banking* masih belum sepenuhnya terselesaikan dan dalam banyak kasus tidak diatur secara tegas.
5. *Transaction risk*: Terdiri dari bahaya yang terkait dengan penipuan, kesalahan, dan ketidakmampuan untuk menawarkan barang dan jasa, menjaga keunggulan kompetitif, dan menangani informasi baik saat ini maupun di masa depan. Para penyedia layanan *e-banking* perlu mengidentifikasi, memahami, dan mengelola risiko-risiko ini dengan baik untuk menjaga kualitas dan keamanan layanan yang diberikan kepada nasabah, serta untuk memitigasi potensi kerugian reputasi dan keuangan yang dapat timbul akibat dari risiko-risiko tersebut.

Di Indonesia terdapat beberapa risiko terkait penggunaan layanan *e-banking* seperti halnya yang tertera pada Gambar 1. Namun, pada kenyataannya dalam hal mengatasi risiko tersebut belum didukung peraturan hukum yang secara khusus mengatur perlindungan data pribadi pengguna layanan *e-banking*. UU Perlindungan Data Pribadi tidak secara khusus mengatur perlindungan hukum bagi nasabah *e-banking*, namun hanya menguraikan upaya-upaya umum untuk melindungi data pribadi, baik secara langsung maupun tidak langsung, melalui sistem elektronik maupun non-elektronik dalam proses pengolahan data pribadi untuk menjamin hak-hak konstitusional subjek data pribadi. Meskipun demikian,

terdapat sejumlah peraturan terkait yang berisi pedoman untuk menjaga privasi informasi pribadi konsumen. Seperti halnya, Peraturan Bank Indonesia Nomor 7/6/PBI/2005 mengenai transparansi informasi produk bank dan penggunaan data pribadi nasabah mengharuskan bank untuk memberikan informasi transparan tentang produk bank dan penggunaan data pribadi nasabah (Pemerintah Indonesia, 2005). Selain itu, Undang-undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen memberikan hak konsumen terhadap kenyamanan, keamanan, dan keselamatan dalam menggunakan barang dan jasa (Pemerintah Indonesia, 1999). Dengan demikian, meskipun belum ada peraturan yang secara spesifik mengatur perlindungan data pribadi pengguna layanan *e-banking*, sejumlah peraturan dan undang-undang yang terkait memberikan kerangka kerja untuk perlindungan nasabah dan pengguna layanan perbankan secara umum.

Gambar 1. Hasil Analisis Risiko Layanan E-Banking

Berdasarkan Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan, Pasal 29 ayat 4 mengamanatkan bank untuk mengungkapkan setiap kemungkinan risiko kerugian yang terkait dengan transaksi konsumen (Pemerintah Indonesia, 1998). Dalam situasi ini, bank harus bertanggung jawab untuk memberikan perlindungan hukum kepada nasabah dengan menawarkan sumber daya untuk membantu jika nasabah mengalami kerugian akibat penggunaan layanan *e-banking*. Dalam situasi tersebut, bank akan memfasilitasi nasabah dengan memberikan bantuan hukum, baik melalui proses litigasi maupun non-litigasi, dengan tujuan utama untuk melindungi hak-hak nasabah dan mencapai keadilan, manfaat, serta kepastian hukum. Dalam upaya menegakkan salah satu hak konsumen yang diuraikan dalam Undang-Undang Perlindungan Konsumen, yaitu hak untuk mendapatkan penggantian atau kompensasi apabila barang dan/atau jasa yang diterima tidak sesuai dengan perjanjian atau tidak memenuhi standar yang semestinya, maka Bank memikul tanggung jawab untuk menangani kerugian. Hal ini tidak terlepas pula pada Teori Keadilan Interaktif yang

menyebutkan bahwasanya kompensasi berperan sebagai sarana untuk mengatasi dampak negatif dari interaksi yang merugikan yang berarti juga memberikan jaminan nasabah agar dilindungi dari efek buruk yang timbul.

Mengingat belum adanya pedoman yang tegas tentang layanan *e-banking*, maka lembaga keuangan harus merancang regulasi khusus yang mengatur layanan tersebut serta tetap memastikan bahwa regulasi yang dibuat senantiasa sejalan dengan peraturan-peraturan yang sudah ada sebelumnya (Hanafittya, 2021). Hal ini terkait dengan berbagai perlindungan hukum terhadap data pribadi nasabah yang harus dijaga oleh undang-undang atau lembaga perbankan. Informasi pribadi yang harus diungkapkan meliputi nama, nomor identitas, tempat dan tanggal lahir, nomor telepon, alamat, dan nama orang tua kandung. Terlihat pula dalam aspek perlindungan privasi data, data pribadi dibagi menjadi dua kategori yaitu data pribadi yang bersifat umum dan data pribadi yang bersifat khusus. Dalam hal ini agama, jenis kelamin, kewarganegaraan, nama lengkap, dan data pribadi yang bersifat umum perlu dilengkapi untuk mengidentifikasi seseorang. Sebaliknya, data pribadi yang bersifat khusus meliputi informasi kesehatan, data biometrik, data genetik, orientasi seksual, masalah politik, data yang berhubungan dengan kesehatan, informasi mengenai anak-anak, informasi keuangan pribadi, dan data lainnya sesuai dengan hukum yang berlaku. Selain data pribadi, ada fitur keamanan lain yang perlu dipantau, seperti nomor rekening, kode verifikasi OTP, PIN ATM, kode CVV/CVC dari kartu kredit, serta nomor kartu kredit serta tanggal kadaluarsanya baik untuk kartu debit maupun kredit.

Urgensi Penerapan Data Protection Authority (DPA) yang Sifatnya Krusial dan Komprehensif Sebagai Bentuk Penegakan Hukum Terhadap Nasabah dalam Transaksi Perbankan Berbasis Digital

Orientasi dari penerapan *Data Protection Authority* (DPA) menjadi hal krusial yang menyangkut harkat martabat manusia serta sebagai wujud kebebasan berekspresi seseorang (Prasetyo, 2018). *Data Protection Authority* (DPA) merupakan sebuah lembaga pengawas yang bertugas menjaga keamanan data dengan fokus utama pada mencegah kejahatan *cyber* terutama dalam hal penyalahgunaan data dan informasi pribadi (Rosadi dkk., 2020). Dengan kata lain, sistem *Data Protection Authority* (DPA) merupakan instrumen dengan sifat fundamental dalam perlindungan data pribadi. Perlindungan privasi dan data pribadi bukanlah isu yang terbatas hanya di Indonesia, tetapi juga menjadi perhatian global di berbagai negara dan organisasi internasional. *European Union General Data Protection Regulation* (EU GDPR) mengungkapkan bahwa Perlindungan Data Pribadi diatur secara terperinci serta jelas pada setiap pasal yang ada didalamnya. Pada Bab III EU GDPR terdapat peraturan yang menyangkut terkait dengan hak-hak atas kepemilikan data pribadi, di mana subjek data memiliki hak dalam pandangan informasi terkait pengolahan data pribadi mereka. Hal yang sama juga berlaku untuk pengaturan mengenai kompensasi, tanggung jawab, dan sanksi yang diuraikan dalam Bab VIII EU GDPR. Di bagian ini dijelaskan terkait individu pemilik data pribadi yang mempunyai hak dalam meminta kompensasi dari entitas yang

mengendalikan atau mengolah data jika terjadi penyalahgunaan atau pengolahan yang tidak berhubungan terhadap tujuan, ataupun jika terjadi pelanggaran (Mahendra dkk., 2022). Hong Kong memiliki *Personal Data Privacy Ordinance of* 1995 (PDPO) yang merupakan undang-undang nasional pertama di mana secara komprehensif mengatur permasalahan privasi serta data pribadi. Di Malaysia, privasi data pribadi masyarakat dilindungi oleh *The Personal Data Protection Act No.* 709 of 2010 (PDPA Malaysia). Sementara itu, Singapura melindungi privasi dan data pribadi dengan pendekatan sektoral melalui *The Personal Data Protection Act* 12 Nomor 26 of 2012.

Tabel 1. Hasil Analisis Perbedaan Perlindungan Data Pribadi di Negara Lain

Negara	Peraturan Perundang-undangan	Keterangan
Eropa	*European Union General Data Protection Regulation* (EU GDPR)	Undang-undang Eropa yang menetapkan perlindungan privasi dan keamanan data pribadi tentang individu. Dalam EU GDPR terdapat prinsip transparansi yang dimana masyarakat memiliki hak untuk mengakses, mengubah, dan menghapus data pribadi mereka yang disimpan oleh perusahaan. Perlindungan Data di Uni Eropa telah diterapkan secara efektif dan tegas untuk mengatur hubungan hukum antara pemilik data pribadi dan pengendali data.
Hongkong	*Personal Data Privacy Ordinance of* 1995 (PDPO)	PDPO sebagai peraturan perundang-undangan nasional pertama yang mengatur masalah privasi dan data pribadi masyarakat. Prinsip-prinsip perlindungan privasi data pribadi di Hongkong mencakup pembatasan pengumpulan data yang sesuai dengan maksudnya, penggunaan dan pengungkapan data yang telah disetujui oleh pemiliknya, keakuratan data, penyimpanan data oleh pihak ketiga dengan waktu tertentu, perlindungan data dari akses yang tidak sah, serta kewajiban pihak ketiga untuk menyampaikan kebijakan privasi dan sanksi dari pemerintah dalam kasus pelanggaran.
Malaysia	*The Personal Data Protection Act No.* 709 of 2010 (PDPA Malaysia)	Undang-undang ini secara tegas bertujuan untuk melindungi data pribadi dengan mengharuskan pengguna data untuk mematuhi ketentuan yang telah ditetapkan, termasuk larangan melakukan transfer data pribadi ke luar Malaysia tanpa izin resmi dari Menteri Informasi, Kebudayaan, dan Komunikasi, serta memastikan bahwa negara atau tempat tujuan transfer data pribadi menyediakan perlindungan data

Negara	Peraturan Perundang-undangan	Keterangan
		pribadi yang setara dengan standar yang diberlakukan oleh PDPA.
Singapura	*The Personal Data Protection Act* 2012 (No. 26 of 2012) (PDPA Singapore)	Undang-undang ini mengatur pengumpulan, penggunaan, dan pengungkapan data pribadi individu oleh pemerintah dengan cara yang mengakui hak individu untuk melindungi data pribadi masyarakatnya. PDPA Singapura mencakup penyediaan sebuah badan registrasi khusus yang disebut *Do Not Call* (DNC) *Registry*, yang memberikan masyarakat hak untuk menerima atau menolak pesan singkat (SMS atau MMS) dari pihak yang tidak diinginkan.

Maka, dapat dilihat dari Tabel 1 di atas bahwa terdapat perbedaan pengaturan atau regulasi perlindungan data pribadi di negara lain. Sementara itu, perlindungan data pribadi di Indonesia melalui penerapan *Data Protection Authority* (DPA) sendiri merupakan sebuah lembaga pengawasan yang dengan kemampuan untuk menangkal kejahatan *cyber* terlebih berkaitan terhadap penyalahgunaan data serta informasi pribadi. Lembaga ini memastikan bahwa data pribadi seseorang aman di pusat pengumpulan data yang dikelola oleh Kominfo. Pengelolaan data yang dijalankan oleh Kementerian Komunikasi dan Informatika (Kominfo) merupakan salah satu unsur dari implementasi *Data Protection Authority* (DPA) menjadi suatu kebutuhan yang sangat penting untuk mencapai tujuan yang mendesak, yaitu memastikan adanya sistem pengamanan *cyber* yang tangguh dan kokoh dalam menghadapi berbagai ancaman. Dalam era digital yang semakin kompleks ini, perlindungan data pribadi dan keamanan *cyber* menjadi perhatian utama untuk menjaga integritas, kerahasiaan, dan ketersediaan data, serta melindungi masyarakat dari potensi risiko dan kerugian akibat kejahatan *cyber* (Latumahina, 2022). Dengan kata lain, *Data Protection Authority* (DPA) menjadi instrumen yang sangat penting dan mendasar dalam upaya melindungi data pribadi. Pada lingkup teknologi informasi dan komunikasi yang semakin maju, perlindungan terhadap data pribadi menjadi isu yang krusial dan kian relevan. *Data Protection Authority* (DPA) bertindak sebagai landasan hukum dan pengawas yang memastikan terhadap data pribadi individu dijaga secara baik serta tidak disalahgunakan oleh para pihak yang di mana tidak memiliki kewenangan (Hartono, 2010).

Adanya lembaga untuk melindungi data merupakan kemajuan besar dalam pengelolaan data, terutama dalam hal *Big Data*. Dengan semakin berkembangnya teknologi dan kemampuan kita untuk mengumpulkan, menyimpan, dan menganalisis data yang sangat besar, keamanan dan privasi data pribadi menjadi semakin penting. *Data Protection Authority* (DPA) berfungsi sebagai lembaga pengawas dalam kerangka hukum yang memberikan suatu perlindungan (Greenleaf, 2022). Penerapan *Data Protection Authority* (DPA) sejatinya wajib dilakukan secara konsisten di Indonesia, melihat terhadap langkah ini sesuai dengan misi pemerintah Indonesia untuk mencapai pembangunan yang berkelanjutan *(sustainable development goals)*. Metode ini memberikan jaminan terkait keamanan data pengguna internet, karena

beroperasi melalui sistem yang terintegrasi dengan Kementerian Komunikasi dan Informatika (Kominfo), dimana memiliki tanggung jawab atas tata kelola data para pengguna internet. Dengan demikian, penggunaan *Data Protection Authority* (DPA) menjadi instrumen yang vital untuk melindungi privasi dan keamanan data di era teknologi digital, dan mendukung visi pemerintah dalam mencapai tujuan pembangunan berkelanjutan secara holistik.

Lembaga yang dicanangkan berjalan secara independen ini, nyatanya memiliki tugas pokok serta fungsi (Tupoksi) dalam mengawasi setiap pemrosesan data pribadi. Sederhananya tugas pokok *Data Protection Authority* (DPA) melibatkan penerapan hukum perlindungan data pribadi. Untuk menjalankan instruksi ini, badan yang diberikan perlu diperkuat melalui fungsi investigasi, yang mencakup seperti halnya melakukan penyelidikan serta penyidikan terhadap setiap *complain* dan mengeluarkan berbagai kebijakan yang mengikat maupun menetapkan hukuman saat ditemukan adanya pelanggaran hukum yang dilakukan oleh suatu lembaga. Dalam hal tersebut, *Data Protection Authority* (DPA) memiliki fungsi meminta informasi atas pemrosesan data, melaksanakan pemeriksaan, dan dapat mengakses segala keterangan dimana diperlukan dalam penyelidikan, baik terkait dengan akses fisik ke gedung ataupun peralatan yang berguna dalam pemrosesan. Selain itu, lembaga ini memiliki tanggung jawab untuk mendapatkan serta merespon setiap *complain* dari individu maupun asosiasi kepentingan/privasi publik, serta menerima pengaduan dari organisasi yang memiliki bukti terkait praktik buruk sebelum terjadinya pelanggaran.

Dalam rangka mewujudkan *Data Protection Authority* (DPA) bagi nasabah dan memulihkan kedudukan mereka, salah satu upaya yang dapat dilakukan adalah penerapan asas tanggung jawab mutlak (*strict liability*) dan menuntut ganti rugi melalui proses pengadilan atas perbuatan melawan hukum oleh pihak bank atau lembaga keuangan terkait (Cahyani dkk., 2022). *Strict liability*, dalam konteks hukum, merujuk pada jenis tanggung jawab di mana seseorang atau perusahaan dapat dianggap bertanggung jawab atas suatu tindakan atau hasil tanpa memerlukan bukti kesalahan atau unsur bersalah. Dalam kasus-kasus *strict liability*, fokusnya lebih pada hasil atau akibat dari suatu tindakan daripada mencari bukti niat jahat atau kelalaian. Melalui penerapan *strict liability*, pihak perbankan memiliki tanggung jawab sepenuhnya ketika nasabah dapat membuktikan bahwa bank telah lalai dalam menjamin keamanan *e-banking*, yang mengakibatkan kegagalan transaksi dan kerugian material. Dalam hal ini, secara yuridis pada Pasal 29 ayat (2) Undang-Undang Nomor 10 Tahun 1998 Tentang Perubahan atas Undang-Undang Nomor 7 Tahun 1992 Tentang Perbankan menegaskan bahwa pihak bank memiliki kewajiban dalam penerapan asas kehati-hatian terhadap kegiatan usaha (Pemerintah Indonesia, 1998). Penerapan asas kehati-hatian ini bertujuan dalam meningkatkan kewaspadaan pihak bank maupun nasabah terhadap risiko yang dapat terjadi sewaktu-waktu.

Penerapan *Data Protection Authorit*y (DPA) di Indonesia bertujuan untuk mencapai kemajuan peradaban di masa depan, dengan menghindari diskriminasi dan mengutamakan prinsip-prinsip Hak Asasi

Manusia (Niffari, 2020). Hal tersebut memiliki tujuan dalam menjaga kebebasan serta keamanan maupun meminimalisir risiko pemerasan dan pencurian data pengguna internet melalui pendekatan cerdas dalam pengurangan risiko. Melalui perlindungan data pribadi dalam sistem pengamanan *cyber*, pembentukan *Data Protection Authority* (DPA) dianggap sebagai benteng pertahanan, terutama di tengah era disrupsi teknologi. Penerapan *Data Protection Authority* (DPA) yang sifatnya krusial dan komprehensif sangatlah penting dalam penegakan hukum terhadap nasabah dalam transaksi perbankan berbasis digital (Putra, 2020).

Berikut merupakan tugas pokok dan fungsi dari *Data Protection Authority* (DPA) sehingga penting untuk diimplementasikan di Indonesia:

1. *Data Protection Authority* (DPA) yang kuat akan memberikan keamanan dan perlindungan bagi nasabah terhadap risiko kebocoran data pribadi, penipuan, dan akses yang tidak sah. Saat ini, kasus kebocoran data dan penyalahgunaan informasi pribadi semakin meningkat, dan seringkali menimbulkan dampak yang merugikan bagi nasabah. Dengan adanya *Data Protection Authority* (DPA) yang kuat, perusahaan perbankan berbasis digital diwajibkan untuk mengimplementasikan langkah-langkah keamanan dan privasi data yang tinggi. *Data Protection Authority* (DPA) juga mengatur bagaimana data nasabah harus ditangani, disimpan, dan diakses oleh pihak-pihak tertentu, sehingga meminimalkan risiko data pribadi nasabah jatuh ke tangan yang tidak berwenang.
2. *Data Protection Authority* (DPA) mendorong pihak bank untuk bertanggung jawab terhadap tindakan mereka. Jika ada pelanggaran atau kesalahan yang merugikan nasabah, nasabah memiliki dasar hukum untuk menuntut ganti rugi dan memastikan pihak bank bertanggung jawab atas kerugian yang terjadi (Sautunnida, 2020). Jika ada pelanggaran atau kesalahan yang merugikan nasabah, nasabah memiliki dasar hukum untuk menuntut ganti rugi dan memastikan pihak bank bertanggung jawab atas kerugian yang terjadi. Dengan *Data Protection Authority* (DPA) yang efektif, pihak bank tidak dapat mengabaikan perlindungan data nasabah sebagai prioritas dan harus memastikan bahwa setiap tindakan mereka sesuai dengan standar keamanan yang telah ditetapkan. Ini menciptakan tanggung jawab yang lebih besar dan lebih akuntabel bagi pihak bank dalam mengelola data nasabah.
3. *Data Protection Authority* (DPA) merupakan langkah yang penting bagi perusahaan perbankan berbasis digital untuk memastikan bahwa mereka mematuhi aturan dan regulasi terkait perlindungan data pribadi. Dengan mengikuti *Data Protection Authority* (DPA), perusahaan dapat menjaga kredibilitas mereka dan menghindari sanksi hukum yang dapat merusak reputasi dan keuangan perusahaan. Dengan demikian, *Data Protection Authority* (DPA) menjadi sarana penting dalam upaya perlindungan data pribadi nasabah dan menjaga integritas perusahaan di era perbankan digital.

4. Dengan adanya *Data Protection Authority* (DPA) yang komprehensif, penegakan hukum terhadap pelanggaran dalam transaksi perbankan berbasis digital atau *e-banking* akan menjadi lebih efektif (Inggarwati dkk., 2020). *Data Protection Authority* (DPA) memberikan kekuatan hukum kepada otoritas untuk menyelidiki, mengawasi, dan menindak pelanggaran yang terkait dengan perlindungan data nasabah. Ini menciptakan sistem hukum yang lebih kuat untuk menangani pelanggaran dan memberikan keadilan bagi nasabah yang mungkin menjadi korban tindakan ilegal.

Secara keseluruhan, penerapan *Data Protection Authority* (DPA) yang krusial dan komprehensif akan memberikan perlindungan yang kuat terhadap data nasabah dalam transaksi perbankan berbasis digital. Hal ini tidak hanya melindungi nasabah dari risiko kejahatan *cyber*, tetapi juga membangun kepercayaan dan memperkuat sektor perbankan digital secara keseluruhan. Artinya dengan adanya penerapan *Data Protection Authority* (DPA) yang kuat akan memberikan manfaat yang signifikan bagi keamanan dan perlindungan nasabah dalam transaksi perbankan berbasis *digital*. Selain melindungi data pribadi nasabah, *Data Protection Authority* (DPA) juga mendorong tanggung jawab pihak bank, memastikan kepatuhan terhadap regulasi, dan meningkatkan efektivitas penegakan hukum. Dengan dukungan dari adanya penerapan *Data Protection Authority* (DPA), sektor perbankan *digital* dapat beroperasi dengan lebih aman bagi nasabahnya, serta menjaga integritas industri di tengah perkembangan teknologi yang terus berlanjut.

Simpulan

Berdasarkan uraian pembahasan di atas dan hasil analisis, dapat disimpulkan bahwa perlindungan terhadap hak-hak dan privasi data pribadi nasabah pada penggunaan layanan e-banking di Indonesia sangat penting. Perlindungan hukum bagi nasabah mencakup tanggung jawab mutlak (*strict liability*) berupa tuntutan ganti rugi melalui proses pengadilan atas pelanggaran hukum oleh bank atau lembaga keuangan terkait. Selain itu, penerapan *Data* Protection Authority (DPA) merupakan langkah krusial dan komprehensif untuk memastikan keamanan dan perlindungan data pribadi nasabah dalam transaksi perbankan berbasis digital. DPA membantu mengatur dan memastikan keamanan serta privasi data pribadi nasabah, mendorong bank untuk bertanggung jawab atas tindakan mereka, mematuhi aturan dan regulasi, serta memberikan dasar hukum bagi nasabah untuk menuntut ganti rugi jika terjadi pelanggaran. Dengan adanya *Data Protection Authority* (DPA) penegakan hukum terhadap pelanggaran dalam transaksi perbankan digital menjadi lebih efektif, menciptakan sistem hukum yang kuat, dan memperkuat sektor perbankan digital secara keseluruhan. Secara keseluruhan, penerapan DPA menjadi langkah penting dalam menjaga keamanan data pribadi nasabah, membangun kepercayaan, dan mendukung perkembangan sektor perbankan digital di era teknologi yang terus berkembang. Dengan demikian, penerapan *Data Protection Authority* (DPA) memiliki urgensi yang tinggi untuk menjaga keamanan data

pribadi nasabah, memastikan tanggung jawab pihak bank, dan memenuhi standar keamanan pada transaksi perbankan berbasis digital.

Maka dari itu, perlunya diimplementasikan terkait dengan pembentukan regulasi perlindungan hukum yang memadai bagi nasabah pengguna layanan *e-banking*. Regulasi ini dapat berbentuk *self-regulation* yang disusun oleh bank untuk mencegah terjadinya kekosongan hukum. *Self-regulation* tersebut perlu disusun dengan lebih mengedepankan *prudential banking principle* dalam menjalankan bisnis usahanya. Selain itu, juga penting adanya *government regulation* yang ditetapkan oleh pemerintah dengan tujuan dalam memastikan adanya suatu perlindungan hukum yang jelas diberikan kepada khalayak umum untuk memberikan kemudahan transaksi melalui layanan *e-banking*. Sebagai penutup, Tim Penulis ingin mengatakan bahwa *Data Protection Authority* (DPA) menjadi instrumen yang bersifat fundamental dalam perlindungan data pribadi. Dengan demikian, diharapkan pembentukan *Data Protection Authority* (DPA) tidak hanya menjadi retorika semata tetapi benar-benar diaktualisasikan agar penyalahgunaan data pribadi tidak lagi menjadi momok yang menakutkan bagi nasabah *e-banking*.

Daftar Pustaka

Aptika, Ditjen. (2021, Oktober 17). *Pentingnya Perlindungan Data Pribadi di Era Digital*. Kominfo. https://aptika.kominfo.go.id/2021/10/pentingnya-pelindungan-data-pribadi-di-era-digital/

Cahyani, N. M. M. F. S. D.; Budiartha, I. N.P.; Astiti, N. G. K. S. (2022). Perlindungan Hukum Bagi Nasabah Bank yang Dirugikan Dalam Transaksi Layanan *E-Banking*. *Jurnal Interpretasi Hukum*, *3*(1), 86. https://doi.org/10.22225/juinhum.3.1.4643.83-88

Elnizar, N. E. (2019, Juli 3). *Perlindungan Data Pribadi Tersebar di 32 UU, Indonesia Perlu Regulasi Khusus*. Hukum Online. https://www.hukumonline.com/berita/a/perlindungan-data-pribadi-tersebar-di-32-uu-indonesia-perlu-regulasi-khusus-lt5d1c3962e01a4

Greenleaf, G. W. (2021). *India's U-turns on Data Privacy*. Privacy Laws & Business International Report.

Greenleaf, G. W. (2022). *Asian Data Privacy Laws-Trade and Human Rights Perspectives*. New York: Oxford University Press.

Hanafittya, S. W. R. (2021). Analisis Perlindungan Kerahasiaan Data Pribadi pada Nasabah Pengguna Produk Layanan Mobile Banking Milik Pemerintah Daerah Aceh. *Jurnal Ilmiah Mahasiswa Bidang Hukum Keperdataan*, *5*(2), 329.

Hartono. (2010). *Penyidikan dan Penegakan Hukum Pidana Melalui Pendekatan Hukum Progresif*. Jakarta: Sinar grafika.

Inggarwati, M. P.; Celia, O.; Arthanti, B. W. (2020). Online Single Submission for Cyber Defense and Security in Indonesia. *Lex Scientia Law Review Journal*, *4*(1), 83-92. https://doi.org/10.15294/lesrev.v4i1.37709

Kusnadi, S. A.; Wijaya, A. U. (2021). Perlindungan Hukum Data Pribadi Sebagai Hak Privasi. *Jurnal Al-Wasath*, *2*(1), 24.

Kusuma, M. J. (2013). Perlindungan Hukum Terhadap Nasabah Bank yang Menjadi Korban Kejahatan ITE di Bidang Perbankan. *Al 'Adl Jurnal Hukum*, *5*(9), 32-55.

Latumahina, R. E. (2022). Aspek Hukum Perlindungan Data Pribadi di Dunia Maya. *Jurnal Gema Aktualita*, *3*(2), 15.

Mahendra, R.; Rosra, D. (2022). Kajian Yuridis tentang Perlindungan Data Pribadi Menurut European Union General Data Protection Regulation (EU GDPR) Tahun 2018 Ditinjau dari Hukum Internasional. *Jurnal Bung Hatta*, *13*(2), 2-3.

Niffari, H. (2020). Perlindungan Data Pribadi Sebagai Bagian Dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi (Suatu Tinjauan Komparatif Dengan Peraturan Perundang-Undangan Di Negara Lain). *Jurnal Yuridis*, *7*(1), 110.

Nurdinisari, R. (2013). *Perlindungan Hukum Terhadap Privasi dan Data Pribadi Pengguna Telekomunikasi Dalam Penyelenggaraan Telekomunikasi Khususnya Dalam Menerima Informasi Promosi yang Merugikan (Spamming)* (Publikasi No. T32602) [Tesis S-2, Fakultas Hukum Program Pasca Sarjana Universitas Indonesia]. Universitas Indonesia Library.

Pemerintah Indonesia. 2005. Peraturan Bank Indonesia Nomor 7/6/PBI/2005 tentang Transparansi Informasi Produk Bank dan Penggunaan Data Pribadi Nasabah. Lembaran Negara Republik Indonesia Tahun 2005, No. 1. Sekretariat Negara. Jakarta.

Pemerintah Indonesia.1998. Undang-Undang Nomor 10 Tahun 1998 Tentang Perubahan atas Undang-Undang Nomor 7 Tahun 1992 Tentang Perbankan. Lembaran Negara Republik Indonesia Tahun 1998, No. 182. Sekretariat Negara. Jakarta.

Pemerintah Indonesia. 2016. Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik (ITE). Lembaran Negara Republik Indonesia Tahun 2016, No. 58. Sekretariat Negara. Jakarta.

Pemerintah Indonesia. 2022. Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi. Lembaran Negara Republik Indonesia Tahun 2022, No. 196. Sekretariat Negara. Jakarta.

Pemerintah Indonesia. 1981. Undang-Undang Nomor 8 Tahun 1981 Tentang Kitab Undang-Undang Hukum Pidana. Lembaran Negara Republik Indonesia, No. 3209. Sekretariat Negara. Jakarta.

Pemerintah Indonesia. 1999. Undang-undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen. Lembaran Negara Republik Indonesia Tahun 1999, No. 8. Sekretariat Negara. Jakarta.

Prasetyo, T. (2018). *Keadilan Bermartabat: Perspektif Teori Hukum*. Bandung: Raja Grafindo Persada.

Pratama, G. Y. (2016). Perlindungan Hukum Terhadap Data Pribadi Pengguna Jasa Transportasi Online Dari Tindakan Penyalahgunaan Pihak Penyedia Jasa Berdasarkan Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen. *Jurnal Hukum*, *5*(3), 9.

Putra, I. M. A. M. (2020). Tanggung Jawab Hukum Bank Terhadap Nasabah dalam Hal Terjadinya Kegagalan Transaksi pada Sistem Mobile Banking. *Jurnal Kertha Wicaksana: Sarana Komunikasi Dosen dan Mahasiswa*, *14*(2), 135. https://doi.org/10.22225/kw.14.2.1921.132-138,

Rahmadhani, D. V.; Nasution, M. I. P.; Sundari, S. S. (2023). Perlindungan Data Privasi Yang Dilakukan Perbankan Terhadap Penggunaan Layanan Mobile Banking. *JUEB: Jurnal Ekonomi dan Bisnis*, *2*(2), 7.

Rahman, F. (2021). Kerangka Hukum Perlindungan Data Pribadi dalam Penerapan Sistem Pemerintahan Berbasis Elektronik di Indonesia. *Jurnal Legislasi Indonesia*, *18*(1), 81-99.

Rosadi, S. D.; Pratama, G. G. (2020). Urgensi Perlindungan Data Privasi dalam Era Ekonomi Digital di Indonesia. *Veritas et Justitia Journal, 4*(1), 105.

Sautunnida, L. (2020). Urgensi Undang-Undang Perlindungan Data Pribadi di Indonesia: Studi Perbandingan Hukum Inggris dan Malaysia. *Kanun Jurnal Ilmu Hukum*, *20*(2), 369-384.

Sudaryanti, k. d.; Dharmawan, N. K. S.; Purwanti, N. P. (2013). Perlindungan Hukum Terhadap Investor dalam Perdagangan Obligasi Secara Elektronik. *Jurnal Kertha Wicara, 2*(1), 1.

Walfajri, M.; Perwitasari, A. S. (2022, Agustus 11). BI Catat Transaksi Mobile Banking Tembus Rp 3.888,09 Triliun hingga Mei 2022. Kontan. https://keuangan.kontan.co.id/news/bi-catat-transaksi-mobile-banking-tembus-rp-388809-triliun-hingga-mei-2022.