

Perlindungan Hukum Data Pengguna E-Wallet Atas Kebocoran Data yang Disalahgunakan Oleh Pinjaman Online

¹Glory Sylviana, ²Dwiki Alif Setiawan, ³Carmelita Listyani, ⁴Elisya Karina Apriyanti, ⁵Linda Apriliana Peryoga Putri

^{1,2,3,4,5}Universitas Brawijaya
aprilianalinda1@student.ub.ac.id

ABSTRACT

E-wallet is a digital platform in the field of financial technology that makes online transactions easier for its users, where users will be asked to provide their personal data. As technology advances, there are leaks of e-wallet user data which may be misused for online loans. This type of research is normative juridical research with descriptive analysis to describe existing problems and support discussion of legal issues which are the focus of the research. The results of the discussion of legal issues in this research are that the main regulators involved in consumer protection in the fintech industry in Indonesia are the Otoritas Jasa Keuangan (OJK) and Bank Indonesia (BI) which are regulated in various related laws and regulations, whereas in Malaysia they are regulated in law. 709 Personal Data Protection Act 2010 and there is a Personal Data Protection Advisory Committee, meanwhile in Singapore it is regulated in The Personal Data Protection Act No. 26 of 2012 Singapore and there is a Personal Data Protection Commission institution. Apart from that, based on Law Number 27 of 2022 concerning Personal Data Protection, the concept of strict liability is considered to provide more justice, because e-wallet users will get the right to compensation, but this has not been regulated further in statutory regulations.

Keywords: E-Wallet, Legal Protection, Personal Data

ABSTRAK

*E-wallet adalah platform digital di bidang teknologi finansial memudahkan transaksi online penggunaannya, dimana pengguna akan diminta untuk memberikan data pribadinya. Seiring kemajuan teknologi, terdapat kebocoran data pengguna e-wallet yang kemungkinan disalahgunakan untuk pinjaman online. Jenis penelitian ini adalah penelitian yuridis normatif dengan sifat analisis deskriptif untuk menguraikan permasalahan yang ada dan mendukung pembahasan tentang persoalan hukum yang menjadi fokus penelitian. Hasil diskusi dari persoalan hukum dalam penelitian ini adalah regulator utama yang terlibat dalam perlindungan konsumen di industri fintech di Indonesia adalah Otoritas Jasa Keuangan (OJK) dan Bank Indonesia (BI) yang diatur dalam berbagai peraturan perundang-undangan terkait, sedangkan di Malaysia diatur dalam UU 709 Personal Data Protection Act 2010 dan terdapat lembaga Komite Penasihat Perlindungan Data Pribadi, sementara itu di Singapura diatur dalam The Personal Data Protection Act No. 26 of 2012 Singapore dan terdapat lembaga Personal Data Protection Commission. Selain itu, berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, konsep *strict liability* dinilai lebih memberikan keadilan, karena pengguna e-wallet akan mendapatkan hak ganti rugi, tetapi hal tersebut belum diatur dalam lebih lanjut dalam peraturan perundang-undangan.*

Kata Kunci: Data Pribadi, E-Wallet, Perlindungan Hukum

Pendahuluan

Perkembangan teknologi di sektor jasa keuangan telah mengalami transformasi signifikan dalam beberapa dekade terakhir, yang akhirnya memunculkan inovasi. Sejak akhir abad ke-20, kemajuan pesat dalam teknologi informasi dan komunikasi telah mengubah cara transaksi keuangan yang memungkinkan transaksi dilakukan secara elektronik, sehingga

menggantikan metode konvensional yang memerlukan kehadiran fisik. Akses yang semakin meluas ke internet berkecepatan tinggi dan peningkatan penetrasi *smartphone* menciptakan lingkungan kondusif untuk pengembangan solusi keuangan digital. Perkembangan keuangan digital tersebut menunjukkan bahwa saat ini kebutuhan masyarakat tidak hanya dapat dilayani sebatas tatap muka saja. Adanya tuntutan terhadap layanan atas kebutuhan masyarakat tersebut akhirnya menciptakan inovasi platform digital, seperti dompet elektronik atau *e-wallet*.

Electronic wallet (E-Wallet) merupakan produk berbasis perangkat lunak yang menggunakan sinyal internet. Di Indonesia, *e-wallet* atau dompet elektronik dikenal sebagai alat pembayaran digital yang memanfaatkan media elektronik berbasis server (Inggiharti, 2020). *E-wallet* adalah salah satu jenis dompet digital non-bank yang paling populer di Indonesia. Aplikasi *e-wallet* memungkinkan pengguna menyimpan uang elektronik dan melakukan berbagai transaksi digital seperti pembayaran tagihan, pembelian pulsa, pembelian tiket transportasi, dan lain-lain. Beberapa contoh *e-wallet* yang terkenal di Indonesia adalah GoPay, OVO, Dana, dan LinkAja (Dr. Suyanto, 2023). Untuk menggunakan *e-wallet* tersebut, pengguna seringkali diharuskan memasukkan data pribadi, seperti nama, usia, jenis kelamin, alamat, nomor telepon. Bahkan pada beberapa platform, meminta pengguna untuk memberikan identitas diri seperti contohnya Kartu Tanda Penduduk (KTP), Surat Izin Mengemudi (SIM), Nomor Pokok Wajib Pajak (NPWP), dan lain-lain.

Penggunaan *e-wallet* yang menawarkan kenyamanan dan kemudahan dalam melakukan transaksi keuangan juga membawa potensi risiko keamanan. Dimana penggunaan data pribadi menjadikan pengguna menjadi semakin rentan terhadap pelanggaran data pribadi. Adapun salah satu bentuk dari pelanggaran data pribadi adalah pencurian data. Sumber kebocoran data di Indonesia dapat berasal dari pihak luar (*malicious outsider*) dan pihak dalam (*malicious insider*), kebocoran yang tidak disengaja akibat sistem tidak aman, *ransomware*, *hacktivist*, dan berapa sumber yang tidak diketahui (Aswandi et al., 2020). Berdasarkan data BSSN telah terindikasi adanya 103 insiden kebocoran data pada tahun 2023. Yang mana sektor keuangan merupakan salah satu sektor yang terdampak dengan persentase 12% dari total insiden setelah sektor administrasi pemerintahan ((BSSN, 2024). Salah satu penyebab kebocoran data tersebut yaitu pelaku usaha jasa keuangan *online* yang menjual data penggunanya seperti nama, foto, NIK, foto KTP, dan nomor telepon kepada pihak ketiga. Hal tersebut terbukti dari adanya kasus kebocoran data pengguna *e-wallet* OVO yang diperjualbelikan ke pihak lain (Soemitra & Adlina, 2022).

Informasi pribadi pengguna yang mengalami kebocoran data dari *e-wallet* dapat digunakan oleh pihak ketiga untuk mengajukan pinjaman *online* atas nama korban tanpa izin mereka. Dengan memiliki informasi pribadi lengkap, seperti nama, alamat, dan nomor identifikasi, pihak ketiga dapat membuat akun palsu dan mengajukan pinjaman dari layanan pinjaman *online*. Hal ini bisa menyebabkan korban mengalami dampak finansial yang serius, adanya persetujuan yang tepat dari para pengguna *e-wallet* terhadap pemrosesan datanya pada platform digital. Oleh karena itu, kasus kebocoran data dalam industri *e-wallet* menggarisbawahi pentingnya keamanan informasi pribadi dan perlindungan privasi pengguna dalam ekosistem digital saat ini. Bagaimana perbandingan hukum dan bentuk penyelesaian sengketa kebocoran data pengguna *e-wallet* atas kebocoran data yang digunakan

oleh pinjaman *online* menurut perspektif perlindungan data pribadi di Indonesia, Malaysia, dan Singapura? Bagaimana perlindungan hukum data konsumen ditinjau dari *Presumption Liability* dan *Strict Liability*?

Metode Penelitian

Penelitian ini menggunakan metode penelitian Yuridis Normatif karena pendekatan dalam penelitian ini menggunakan pendekatan perundang-undangan (*statue approach*) mengenai asas-asas dan aturan hukum yang berhubungan dengan perlindungan data pribadi, yakni Undang-Undang Nomor 27 tahun 2022 tentang Perlindungan Data Pribadi yang didukung oleh aturan-aturan pendukung lainnya seperti Peraturan Menteri (Permen) Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik. Selain itu, penelitian ini juga menggunakan pendekatan perbandingan (*comparative approach*) antara pengaturan perlindungan data pribadi di negara Indonesia, Malaysia, dan Singapura, dimana di negara Malaysia sendiri diatur dalam *Personal Data Protection Act 2010* dan di Singapura diatur dalam *The Personal Data Protection Act No 26 of 2012*. Dengan menggunakan pendekatan perundang-undangan dan pendekatan perbandingan, penelitian ini juga akan mengkaji bagaimana perlindungan hukum data konsumen *E-Wallet* atas kebocoran data yang digunakan untuk pinjaman online dengan melihat dari prinsip *Presumption Liability* dan *Strict Liability*.

Dalam melakukan penelitian yang menggabungkan pendekatan normatif-empiris, peneliti menggunakan tiga bahan hukum yang terbagi jadi tiga, yaitu primer, sekunder, dan tersier. Bahan hukum primer merupakan inti dari penelitian karena memiliki otoritas tertinggi, termasuk peraturan perundang-undangan dan dokumen resmi lainnya yang mengandung ketentuan hukum yang mengikat. Sementara itu, bahan hukum sekunder menyediakan dukungan dan penjelasan tambahan tentang sumber hukum primer, seperti buku, artikel, dan makalah. Selanjutnya terdapat bahan hukum tersier, yang merupakan pelengkap yang memberikan panduan dan penjelasan lebih lanjut tentang bahan hukum primer dan sekunder.

Dalam teknik pengumpulan data, peneliti menggunakan studi kepustakaan, di mana data sekunder dikumpulkan dari berbagai sumber terkait dengan topik penelitian. Data ini kemudian disusun dan dianalisis dengan menggunakan analisis deskriptif untuk menguraikan permasalahan yang ada dan mendukung pembahasan tentang persoalan hukum yang menjadi fokus penelitian.

Hasil Penelitian dan Pembahasan

Perbandingan Hukum dan Bentuk Penyelesaian Sengketa Kebocoran Data Pengguna *E-Wallet* Atas Kebocoran Data yang Digunakan Oleh Pinjaman Online Menurut Perspektif Perlindungan Data Pribadi di Indonesia, Malaysia, Dan Singapura

Fenomena Financial Technology (*Fintech*)

Teknologi finansial merupakan sebuah inovasi dari layanan jasa keuangan yang sebagian besar atau bahkan seluruh kegiatannya bertumpu pada kemajuan teknologi informasi, khususnya "*internet of things*" dimana inovasi tersebut berdampak pada

penghubung antara teknologi finansial (penyedia jasa *fintech*) dengan konsumen korporat atau bisnis (*business to business*) dan konsumen perorangan (*business to customer*) (Nurhasanah & Rahmatullah, 2020). Perkembangan teknologi digital, khususnya dalam industri *financial technology* (*fintech*), telah memunculkan berbagai inovasi seperti dompet elektronik (*e-wallet*). *E-wallet* atau dompet elektronik adalah sebuah platform digital yang menyediakan berbagai fitur untuk memudahkan dan mengamankan transaksi online penggunanya. Sebagai layanan yang semakin populer di era digital ini, *e-wallet* berfungsi sebagai tempat penyimpanan dan pengelolaan informasi penting terkait aktivitas belanja *online* para penggunanya (Bodhi & Tan, 2022). Ketika seseorang pengguna *e-wallet* mendaftar dan menggunakan layanan di dalam aplikasi tersebut, pengguna akan diminta untuk memberikan berbagai data pribadinya, seperti nama lengkap, kata sandi, alamat pengiriman, dan informasi terkait kartu kredit pengguna. Dengan demikian, setiap kali melakukan pembayaran *online*, pengguna tidak perlu lagi memasukkan informasi tersebut lagi secara manual, karena telah terdaftar pada *e-wallet*.

Banyaknya informasi pribadi yang tersimpan di dalam *e-wallet*, maka keamanan data menjadi hal yang prioritas. Namun, seiring dengan meningkatnya penggunaan platform ini, masalah keamanan dan perlindungan data pribadi pengguna menjadi perhatian utama. Perkembangan teknologi adalah pedang bermata dua, dimana menawarkan kemudahan dan manfaat bagi masyarakat, tetapi juga membuka peluang bagi pelaku kejahatan. Seiring waktu, jenis-jenis kejahatan berkembang seiring dengan kemajuan teknologi, terutama dengan munculnya internet yang mendorong lahirnya berbagai bentuk kejahatan baru seperti *cybercrime*. Pelaku kejahatan memanfaatkan teknologi untuk tindakan ilegal seperti pencurian data, penipuan *online*, peretasan, dan penyebaran *malware*. Kasus kebocoran data pengguna *e-wallet* yang digunakan oleh pinjaman *online* menimbulkan kekhawatiran serius dan memerlukan penyelesaian sengketa yang efektif.

Perlindungan Hukum Data Konsumen di Indonesia

Pada hakikatnya, perlindungan hukum merupakan wujud dari pemenuhan hak-hak yang seharusnya diterima oleh setiap konsumen. Dengan kata lain, perlindungan konsumen sejatinya merupakan cerminan dari perlindungan hukum terhadap hak-hak konsumen. Namun, tanggung jawab untuk melindungi konsumen tidak hanya terletak pada pundak pemerintah semata. Pelaku usaha juga memiliki peran penting dalam menjamin terpenuhinya hak-hak konsumen, sebagaimana diatur dalam Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen (Marcelliana & dkk, 2023). Pelaku usaha berkewajiban untuk mengambil langkah-langkah yang diperlukan guna memastikan bahwa hak-hak konsumen terjamin dan terlindungi sesuai dengan ketentuan peraturan perundang-undangan yang berlaku. Dengan demikian, perlindungan konsumen merupakan hasil dari sinergi antara upaya pemerintah dalam menegakkan hukum dan kesadaran pelaku usaha dalam memenuhi kewajibannya terhadap konsumen. Sebagaimana tertuang di dalam UU No. 8 Tahun 1999, perlindungan konsumen diartikan dalam hal segala upaya yang menjamin adanya kepastian hukum untuk memberikan bentuk perlindungan untuk konsumen.

Peraturan perundang-undangan di Indonesia yang mengatur terkait perlindungan data pribadi masyarakat Indonesia antara lain adalah Undang-Undang No. 11 Tahun 2008

tentang Informasi dan Transaksi Elektronik (UU ITE) berserta perubahannya, Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, Peraturan Pemerintah No. 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik, dan Peraturan Menteri Komunikasi dan Informatika No. 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik. Adapun aturan terkait perlindungan data pribadi yang telah disahkan oleh Presiden Republik Indonesia, yaitu pada 17 Oktober 2022 adalah Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) yang bertujuan untuk memberikan kepastian terkait perlindungan data pribadi masyarakat Indonesia dari penyalahgunaan yang tidak bertanggung jawab. Namun, setelah diundangkannya UU PDP, ternyata masih kerap ditemukan berbagai masalah terkait kebocoran data pribadi, khususnya data konsumen yang dicuri secara tidak dipertanggungjawabkan. Pertanggungjawaban pelaku usaha atas kebocoran data pribadi konsumen dalam bertransaksi di platform digital sebagai contoh kebocoran data di *e-wallet* yang disalahgunakan untuk pinjaman *online* masih belum diatur secara rinci di UU PDP.

Berbagai platform digital pada praktiknya telah mematuhi ketentuan kebijakan privasi konsumen, pada kasus kebocoran data dari platform *e-wallet* yang digunakan oleh pinjaman *online* pihak yang bertanggung jawab adalah pengendali dan prosesor data pribadi para konsumen. Sebagaimana diatur di dalam Bab IV UU PDP terkait kewajibannya dalam memproses data pribadi. Dalam konteks perlindungan data pribadi di Indonesia, Pasal 26 UU ITE memberikan hak kepada setiap individu untuk mengajukan gugatan atas tindakan perolehan data atau informasi pribadi tanpa persetujuan. Tindakan tersebut dapat dikategorikan sebagai perbuatan melawan hukum berdasarkan Pasal 1365 Kitab Undang-Undang Hukum Perdata (KUHPerdata) atau sebagai bentuk ketidakpatuhan atau kelalaian dalam melindungi data pribadi (Natha et al., 2022). Selain itu, Pasal 3 UU ITE juga menekankan adanya prinsip kehati-hatian dan pertanggungjawaban bagi setiap penyelenggara sistem elektronik, baik itu perusahaan maupun pemerintah, untuk menerapkan sistem elektronik yang andal dan aman.

Dalam proses penyelesaian sengketa terkait pelanggaran perlindungan data pribadi, pihak yang merasa dirugikan dapat mengajukan gugatan perdata ke pengadilan negeri setempat. Gugatan tersebut dapat didasarkan pada perbuatan melawan hukum (Pasal 1365 KUHPerdata) atau kelalaian (Pasal 1366 KUHPerdata). Penggugat harus dapat membuktikan adanya kerugian yang timbul akibat pelanggaran perlindungan data pribadi tersebut. Selain jalur pengadilan, penyelesaian sengketa juga dapat ditempuh melalui mekanisme alternatif, seperti mediasi atau arbitrase, sebagaimana diatur dalam Undang-Undang Nomor 30 Tahun 1999 tentang Arbitrase dan Alternatif Penyelesaian Sengketa. Melalui mediasi, para pihak yang bersengketa dapat mencapai kesepakatan dengan bantuan mediator yang netral. Sementara itu, arbitrase melibatkan pihak ketiga yang ditunjuk oleh para pihak untuk memberikan putusan yang mengikat.

Dalam kasus pelanggaran perlindungan data pribadi yang melibatkan perusahaan atau penyelenggara sistem elektronik, Kementerian Komunikasi dan Informatika (Kominfo) juga memiliki kewenangan untuk melakukan pengawasan dan penegakan hukum, mengingat di Indonesia belum adanya lembaga yang berwenang dalam menindaklanjuti

sengketa kebocoran data pribadi di Indonesia. Sehingga, Kominfo yang berwenang memberikan sanksi administratif, seperti peringatan tertulis, denda, atau pemblokiran akses, bagi penyelenggara sistem elektronik yang terbukti melanggar ketentuan perlindungan data pribadi. Dengan adanya berbagai mekanisme penyelesaian sengketa tersebut, diharapkan hak-hak individu terkait perlindungan data pribadi dapat terjamin dan pelaku pelanggaran dapat dimintai pertanggungjawaban sesuai dengan peraturan perundang-undangan yang berlaku di Indonesia.

Indonesia memiliki Badan Perlindungan Konsumen Nasional (BPKN), tetapi badan ini tidak memiliki peran yang besar dalam melindungi konsumen di industri teknologi finansial. Regulator utama yang terlibat dalam perlindungan konsumen di industri *fintech* adalah Otoritas Jasa Keuangan (OJK) dan Bank Indonesia (BI). Berdasarkan Peraturan OJK No. 1 tahun 2013 tentang Perlindungan Konsumen di Sektor Jasa Keuangan menyatakan bahwa penyedia jasa keuangan wajib menerapkan transparansi, perlakuan yang tidak memihak, dapat dipercaya, privasi dan keamanan data/informasi konsumen, dan perlakuan yang sederhana dalam menangani keluhan dan penyelesaian sengketa konsumen ke dalam operasi mereka, serta biaya yang cepat dan murah. BI juga memiliki fungsi perlindungan konsumen yang memungkinkan nasabah untuk melaporkan keluhan yang berkaitan dengan sistem pembayaran. Peraturan OJK No. 13 Tahun 2018 mewajibkan perusahaan tekfin digital untuk bertanggung jawab dan aman serta memprioritaskan perlindungan dan tata kelola konsumen. Masalah ini juga dibahas dalam Peraturan Bank Indonesia No. 18 Tahun 2016 dan Peraturan OJK No. 77 tahun 2016.

Perlindungan Hukum Data Konsumen di Malaysia

Di Malaysia, data adalah komoditas yang berharga dan oleh karena itu penting untuk dilindungi. Malaysia memiliki Undang-Undang Perlindungan Data Pribadi (UU 709 *Personal Data Protection Act* 2010) atau disebut PDPA, yang berlaku efektif sejak tahun 2013. Ini adalah undang-undang perlindungan data pribadi pertama di ASEAN pada saat itu. Rancangan PDPA dimulai pada tahun 2001. PDPA merupakan pedoman yang komprehensif bagi semua sektor yang menggunakan transaksi elektronik untuk memberikan perlindungan keamanan bagi konsumen dari penipuan kartu kredit, identitas atau data dan penjualan atau penyebaran data pribadi tanpa persetujuan konsumen (Nurhasanah & Rahmatullah, 2020). PDPA hadir untuk merespon maraknya regulasi data pribadi di berbagai bidang. Ruang lingkup PDPA sangat luas sehingga mencakup banyak bidang antara lain: perbankan dan keuangan, asuransi, telekomunikasi, kesehatan, rumah sakit dan pariwisata, pendidikan, *real estate* dan properti, penjualan langsung, jasa (hukum, akuntansi, konsultan bisnis, teknik, arsitektur, ketenagakerjaan) agen, transportasi dan ritel.

Dalam beberapa tahun terakhir, Malaysia telah membuat kemajuan yang signifikan sebagai pusat *fintech* global. Menurut Malaysia Fintech Report 2019, Malaysia memiliki 198 *Fintech* yang beroperasi di berbagai bidang termasuk pembayaran (19%), dompet (*wallet*) (19%), regtech (6%), insurtech (8%), crowdfunding (6%), pasar (3%), pinjaman (7%), *blockchain* (7%), *wealthtech* (7%), pengiriman uang (7%), *AI/Big Data* (4%), *fintech* syariah (3%), dan proptech (3%). Pembayaran dan dompet merupakan area yang paling banyak menggunakan solusi teknologi finansial. Dengan 95% penduduk Malaysia memiliki rekening

bank dan 86% penetrasi internet, solusi teknologi finansial diperkirakan akan terus berkembang di tahun-tahun berikutnya. Pertumbuhan ini ditunjukkan dengan meningkatnya nilai transaksi internet banking dari 920,9 juta di tahun 2018, menjadi 734,9 miliar di tahun 2019. Untuk mendukung pertumbuhan ini, Asosiasi Fintech Malaysia (FAOM) dibentuk pada tahun 2016, dengan tujuan untuk melibatkan para pelaku industri dan mendukung pengembangan fintech serta untuk terhubung dengan para pemangku kepentingan baik secara lokal maupun global (Financial Technology Regulation in Malaysia and Indonesia: A Comparative Study, 2020). Internet banking di Malaysia telah meningkat empat kali lipat dalam beberapa tahun terakhir, mencapai puncaknya pada penggunaan 90% pada tahun 2018. Mobile banking juga menjadi populer dengan dukungan cakupan jaringan 4G, data yang terjangkau, dan proyeksi teknologi 5G. Malaysia telah menduduki peringkat pertama dalam Indeks Kesiapan Jaringan World Economic Forum 2019 dan menjadi yang pertama di antara negara-negara di Asia yang sedang berkembang. Untuk mendukung pengembangan dan meningkatkan kualitas fintech di Malaysia, Financial Technology Enabler Group (FTEG) didirikan oleh Bank Negara Malaysia (BNM) pada bulan Juni 2016. Terdiri dari kelompok lintas fungsi di dalam BNM, FTEG memiliki tanggung jawab untuk merumuskan dan meningkatkan kebijakan regulasi untuk memfasilitasi adopsi inovasi teknologi di industri jasa keuangan Malaysia.

Penyelesaian sengketa di Malaysia terkait kebocoran data pribadi dari *e-wallet* yang digunakan untuk pinjaman online diatur dalam beberapa peraturan perundang-undangan, termasuk *Personal Data Protection Act 2010* (PDPA) dan *Financial Services Act 2013* (FSA). Berdasarkan PDPA, setiap individu yang data pribadinya bocor atau disalahgunakan oleh pihak lain, termasuk penyedia layanan *e-wallet* atau pinjaman online ilegal, berhak mengajukan keluhan kepada Jabatan Perlindungan Data Pribadi (JPDP) di bawah Kementerian Komunikasi dan Multimedia Malaysia. JPDP akan melakukan investigasi terhadap keluhan tersebut dan dapat menjatuhkan sanksi administratif kepada pihak yang terbukti melanggar ketentuan perlindungan data pribadi, seperti denda atau perintah untuk menghentikan pemrosesan data pribadi. Selain itu, individu yang dirugikan juga dapat mengajukan gugatan perdata ke Mahkamah Tinggi (*High Court*) atas dasar pelanggaran kewajiban berdasarkan kontrak (*breach of contract*) atau perbuatan melawan hukum (*tort of negligence*). Penggugat harus dapat membuktikan adanya kerugian yang timbul akibat kebocoran data pribadi tersebut.

Dalam konteks pinjaman online ilegal, Bank Negara Malaysia (BNM) selaku regulator keuangan juga memiliki kewenangan untuk mengambil tindakan terhadap pihak-pihak yang terlibat. Berdasarkan FSA, BNM dapat melakukan investigasi dan menjatuhkan sanksi, termasuk denda dan pencabutan izin usaha, kepada penyedia layanan keuangan yang melanggar ketentuan, termasuk dalam hal perlindungan data pribadi nasabah. Selain itu, BNM juga mendorong penyelesaian sengketa melalui mekanisme alternatif, seperti mediasi atau ajudikasi, melalui Pusat Penyelesaian Pertikaian Kewangan (*Financial Mediation Bureau*) yang didirikan oleh BNM. Melalui mekanisme ini, nasabah yang dirugikan dapat mengajukan pengaduan dan mencapai kesepakatan dengan penyedia layanan keuangan tanpa harus melalui proses pengadilan.

Secara keseluruhan, Malaysia telah memiliki kerangka hukum yang cukup komprehensif untuk menangani sengketa terkait kebocoran data pribadi dari *e-wallet* yang digunakan untuk pinjaman *online* ilegal. Melalui kombinasi antara penegakan hukum oleh regulator, mekanisme pengaduan, dan penyelesaian sengketa alternatif, diharapkan hak-hak konsumen dapat terlindungi dan pelaku pelanggaran dapat dimintai pertanggungjawaban. Malaysia membentuk Komite Penasihat Perlindungan Data Pribadi di bawah *Personal Data Protection Act* 2010 untuk menerima tuduhan penyalahgunaan data pribadi dan transfer yang tidak sah. Pada saat yang sama, pengadilan banding terlibat dalam penyelesaian yudisial. Undang-undang ini tidak hanya menjamin kebebasan untuk berdemonstrasi, tetapi juga memberikan konsekuensi pidana bagi mereka yang melanggar peraturan yang melindungi data publik. Sanksi dapat dijatuhkan kepada orang-orang yang secara ilegal mengakses atau mengumpulkan data pribadi, yang berujung pada vonis bersalah dan hukuman penjara. Secara tidak sah, pelaku dapat dihukum dengan denda maksimum lima ratus ribu ringgit Malaysia dan atau hukuman penjara hingga tiga tahun (Rizal, 2019).

Perlindungan Hukum Data Konsumen di Singapura

Perlindungan hukum data pribadi konsumen di Singapura diatur di dalam *The Personal Data Protection Act* No. 26 of 2012 Singapore (PDPA 2012 Singapura). Singapura telah memberlakukan peraturan yang komprehensif terkait perlindungan data pribadi sejak tahun 2014. Aturan yang dimiliki oleh Singapura dan Malaysia memiliki banyak kesamaan, karena keduanya mengadopsi prinsip-prinsip yang terdapat dalam *European Data Protective Directive* (EUDP). Namun, terdapat satu perbedaan mendasar antara aturan perlindungan data pribadi di Singapura dan Malaysia. Singapura memiliki sebuah badan khusus yang bernama *Do Not Call* (DNC) *Registry*, yang merupakan bagian integral dari *Personal Data Protection Act* (PDPA) 2012 (Priscyllia, 2019). Melalui *DNC Registry*, masyarakat Singapura diberikan hak untuk memilih apakah mereka ingin menerima atau menolak pesan singkat (SMS atau MMS) yang berasal dari pihak atau organisasi pemasaran yang tidak mereka kehendaki. Dengan adanya mekanisme ini, masyarakat Singapura memiliki kontrol yang lebih besar atas data pribadi mereka, terutama dalam konteks komunikasi pemasaran. Sebaliknya, Malaysia belum memiliki sistem serupa yang terintegrasi dengan peraturan perlindungan data pribadinya.

Undang-Undang perlindungan data pribadi di Singapura memperkenalkan beberapa konsep fundamental yang dapat dijadikan acuan bagi Indonesia dalam mengembangkan kerangka hukum serupa. Tiga konsep utama yang patut dipertimbangkan adalah persetujuan (*consent*), tujuan (*purpose*), dan kewajaran (*reasonableness*) (Wiranata, 2021). Pertama, konsep persetujuan menekankan bahwa organisasi hanya boleh mengumpulkan, menggunakan, atau mengungkapkan data pribadi setelah mendapatkan persetujuan yang jelas dari pemilik data tersebut. Pendekatan ini sangat penting untuk melindungi hak-hak individu atas data pribadi mereka. Kedua, konsep tujuan mengharuskan organisasi untuk secara eksplisit menyatakan maksud dan tujuan dari pengumpulan data pribadi. Organisasi wajib menginformasikan kepada individu mengenai bagaimana data pribadi mereka akan digunakan dan untuk keperluan apa. Terakhir, konsep kewajaran mensyaratkan agar organisasi hanya mengumpulkan, menggunakan, atau mengungkapkan data pribadi untuk tujuan-tujuan

yang dianggap wajar dan tidak berlebihan. Hal ini bertujuan untuk mencegah penyalahgunaan data pribadi oleh organisasi.

Singapura telah menerapkan sanksi yang tertuang di dalam PDPA 2012 Singapura, yaitu terdiri dari sanksi pidana dan denda terhadap pelanggaran data pribadi. Selain itu, di Singapura terdapat *Data Protection Officer*. Kehadiran *Data Protection Officer* di Singapura merupakan kewajiban bagi setiap organisasi yang kecil maupun menengah. Singapura mewajibkan setiap organisasi, terlepas dari ukurannya, untuk memiliki seorang petugas perlindungan data (*data protection officer* atau DPO). Meskipun organisasi dengan sumber daya terbatas diperbolehkan untuk mengalihdayakan tugas-tugas operasional DPO kepada pihak ketiga, tanggung jawab utama atas perlindungan data pribadi tetap berada pada organisasi itu sendiri. Sebagai alternatif, organisasi dapat memanfaatkan layanan DPO *as a Service* (DPOaS) yang terdaftar pada *Infocomm Media Development Authority* (IMDA) (Yuniarti, 2022). DPOaS memungkinkan organisasi untuk menyerahkan fungsi perlindungan data pribadi mereka kepada penyedia layanan eksternal yang kompeten. IMDA, sebagai lembaga di bawah Kementerian Komunikasi dan Informasi Singapura (MCI), memiliki mandat untuk mengembangkan dan mengatur sektor informasi, komunikasi, dan media, termasuk aspek perlindungan data. Dengan menggunakan layanan DPOaS yang terdaftar pada IMDA, organisasi dapat memastikan bahwa mereka mematuhi kewajiban perlindungan data pribadi sesuai dengan peraturan yang berlaku, sambil tetap dapat fokus pada kegiatan inti bisnis mereka.

Dalam konteks pinjaman *online* ilegal yang datanya dibocorkan dari platform *e-wallet*, lembaga yang menaungi terkait perlindungan data pribadi konsumen berada di bawah Personal Data Protection Commission (PDPC) secara kelembagaan berada dibawah naungan *Ministry of Communications and Information* (MCI) (Faizah, A. F., Rosadi, S. D., Pratama, G. G., & Dharmawan, 2023). Posisi kelembagaan Personal Data Protection Commission (PDPC) di Singapura adalah sebagai otoritas pemerintah yang berada di bawah naungan kementerian, bukan sebagai lembaga independen. Hal ini dikarenakan oleh lingkup kerja PDPC yang terbatas hanya pada sektor swasta dan tidak mencakup sektor publik. Selain itu, model berbasis kementerian juga dapat membatasi kemampuan PDPC untuk bertindak sebagai pengawas yang efektif atas praktik perlindungan data pribadi di sektor publik. Hal ini dapat menciptakan celah dalam perlindungan data pribadi secara keseluruhan, mengingat bahwa lembaga publik juga mengelola sejumlah besar data pribadi warga negara.

Perlindungan Hukum Data Konsumen Ditinjau dari *Presumption Liability* dan *Strict Liability*

Undang-Undang Nomor 27 Tahun 2022 (UU PDP) menyebutkan bahwasannya subjek data pribadi dalam hal ini pengguna *e-wallet* berdasarkan Pasal 12, dapat mengajukan gugatan dan menerima ganti rugi atas pelanggaran yang dilakukan oleh pemrosesan data pribadi dirinya (Pasal 12 Undang-Undang Nomor 27 Tahun 2022). Dalam kasus terjadinya kebocoran data pribadi pengguna *e-wallet*, maka dasar gugatan yang dapat diajukan oleh mereka adalah dalih telah terjadinya perbuatan melawan hukum yang dilakukan oleh perusahaan *e-wallet*. Kemudian, perbuatan melawan hukum juga didasarkan pada Pasal 1365

KUHPerdata, karena ketika terjadinya kebocoran data pengguna *e-wallet*, maka adanya kemungkinan hak privasi dari pengguna tersebut yang dilanggar. Padahal, kalau melihat Pasal 36 UU PDP, seharusnya perusahaan *e-wallet* sebagai pengendali data pribadi memiliki kewajiban terhadap keamanan data penggunanya yang meliputi (Suriaatmadja, 2023):

- a. Penyusunan dan penerapan langkah teknis 'operasional untuk melindungi Data Pribadi dari gangguan pemrosesan Data Pribadi yang bertentangan dengan ketentuan peraturan perundang-undangan; dan
- b. Penentuan tingkat keamanan Data Pribadi dengan memperhatikan sifat dan risiko dari Data Pribadi yang harus dilindungi dalam pemrosesan Data Pribadi.

Menjadi kewajiban suatu pengendali data pribadi dalam hal perusahaan *e-wallet* untuk dapat mencegah terjadinya pelanggaran terhadap data pribadi pengguna dengan merujuk pasal tersebut, tetapi ketika perusahaan *e-wallet* gagal melakukan kewajibannya tersebut maka kelalaian yang dilakukan perusahaan *e-wallet* telah tergolong sebagai perbuatan yang melanggar hukum, karena kelalaian yang dilakukan oleh perusahaan *e-wallet* maka kemungkinan besar akan menyebabkan kerugian dari sisi penggunanya, apalagi ditambah ketika data pengguna yang bocor tersebut disalahgunakan untuk kejahatan lain seperti penyalahgunaan pinjaman online. Jika melihat UU PDP, sanksi yang dijelaskan secara tegas berupa sanksi administratif saja berkaitan dengan adanya pelanggaran data pribadi, mulai dari peringatan tertulis, penghentian sementara kegiatan pemrosesan data pribadi, penghapusan atau pemusnahan data pribadi sampai dengan denda administratif. Dalam hal jika pengguna *e-wallet* ingin meminta ganti rugi dari perusahaan *e-wallet*, maka aturan yang berkaitan dengan ganti rugi merujuk pada Peraturan Pemerintah. Namun, untuk saat ini belum ada peraturan pemerintah yang terbaru yang mengatur tata cara pengenaan ganti rugi.

Pengguna *e-wallet* juga dapat dikategorikan sebagai konsumen jasa, maka penulis juga melihat tanggung jawab yang diakomodir dalam Undang-undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen (UUPK). UUPK sendiri lebih mengadopsi konsep *presumption of liability*. Pada konsep tanggung jawab tersebut, perusahaan atau penyedia barang/jasa selalu dianggap bertanggung jawab atas perbuatan baik kesalahan atau kelalaian yang diperbuatannya, sampai perusahaan tersebut dapat membuktikan sebaliknya bahwa kerugian yang timbul bukan karena perbuatannya atau bisa disebut juga sebagai pembuktian terbalik (Delpiero, 2021). Adapun konsep tanggung jawab tersebut dapat dilihat dalam Pasal 19, 22, dan 23 UUPK. Namun, jika melihat konsep tersebut, menurut penulis kurang dapat memberikan keadilan bagi para konsumen khususnya konsumen yang data pribadinya digunakan untuk layanan jasa, karena kemungkinan perusahaan akan terbebas dari tanggung jawabnya apabila memang mereka membuktikan tidak melakukan kesalahan atau mereka telah melakukan kelalaian tapi sudah berusaha sebisa mungkin mengatasi untuk tidak terjadi kerugian atau karena keadaan *force majeure*, mereka terbebas dari tanggung jawab. Ditambah lagi kalau melihat Peraturan Menteri Komunikasi Dan Informatika Republik Indonesia Nomor 5 Tahun 2020 Tentang Penyelenggara Sistem Elektronik Lingkup Privat, dalam Pasal 11 dapat dilihat bahwa suatu perusahaan dapat dibebaskan dari tanggung jawab hukum mengenai Informasi Elektronik dan/atau Dokumen Elektronik yang dilarang yang ditransmisikan atau didistribusikan melalui Sistem Elektroniknya, meliputi:

- a. telah melakukan kewajiban sebagaimana dimaksud dalam Pasal 9 ayat (3) dan Pasal 10;
- b. memberikan Informasi Pengguna Sistem Elektronik (*Subscriber Information*) yang mengunggah Informasi Elektronik dan/atau Dokumen Elektronik yang dilarang dalam rangka pengawasan dan/atau penegakan hukum; dan
- c. melakukan Pemutusan Akses (*take down*) terhadap Informasi Elektronik dan/atau Dokumen Elektronik yang dilarang.

Menjadi sebuah ketidakadilan bagi konsumen dalam hal ini pengguna data *e-wallet* kalau misalnya ternyata perusahaan *e-wallet* memang telah melakukan kesalahan atau kelalaian, tetapi mereka telah melakukan suatu perbuatan yang baik untuk menanggulangnya sehingga mereka terbebas dari tanggung jawab mereka ketika adanya kebocoran data pengguna *e-wallet*. Padahal kalau melihat UU PDP salah satunya dilandasi oleh asas kehati-hatian. Ketidakhati-hatian suatu perusahaan terhadap suatu pengolahan data pribadi, meskipun sudah melakukan tindakan yang baik untuk menanggulangnya harusnya tidaklah dapat untuk menghilangkan tanggung jawab perusahaan tersebut. Dengan demikian, pengguna *e-wallet* bisa saja tidak mendapatkan ganti rugi jika melihat penjelasan sebelumnya dan tidak memberikan keadilan bagi pengguna *e-wallet*, istilah *strict liability* (tanggung jawab mutlak). Konsep ini menekankan bahwa perusahaan dianggap selalu bertanggung jawab tanpa melihat apakah suatu perbuatan dilakukan karena kesalahan atau tidak melihat siapa yang melakukan kesalahan (Priliasari, 2023). Jika melihat dari hal tersebut, maka konsep tanggung jawab tersebut akan menjadi *a contrario* dari Pasal 11 Peraturan Menteri Komunikasi Dan Informatika Republik Indonesia Nomor 5 Tahun 2020 Tentang Penyelenggara Sistem Elektronik Lingkup Privat. Karena meskipun perusahaan *e-wallet* telah melakukan serangkain tindakan baik pencegahan maupun penanggulangan, tetap saja mereka akan bertanggung jawab atas segala kerugian yang diderita oleh pengguna *e-wallet*. Tentunya menurut penulis konsep tanggung jawab lebih memberikan rasa keadilan, karena tentunya pengguna *e-wallet* akan mendapatkan hak ganti ruginya. Jika melihat Pasal 47 UU PDP yang menyatakan bahwa Pengendali Data Pribadi wajib bertanggung jawab atas pemrosesan Data Pribadi dan menunjukkan pertanggungjawaban dalam kewajiban pelaksanaan prinsip Perlindungan Data Pribadi. Dari Pasal tersebut dapat dilihat bahwa UU PDP rasanya lebih menganut konsep *strict liability*, ditambah lagi hal tersebut sangat mendukung adanya penerapan asas kehati-hatian yang mengharuskan perusahaan untuk selalu memperhatikan segenap aspek yang berpotensi mendatangkan kerugian, karena mereka akan selalu bertanggung jawab atas kerugian yang timbul meskipun kerugian tersebut karena kelalaian perusahaan.

Adapun yang menjadi perhatian dari penulis di sini adalah UU PDP memang sudah menjadi *lex posterior* bagi peraturan lain, tetapi memang penulis masih melihat satu kelemahan di dalam UU PDP, belum ada peraturan pemerintah terbaru sebagai peraturan pelaksana berkaitan dengan tata cara pengenaan ganti rugi atas pelanggaran pemrosesan data pribadi, sehingga menurut penulis perlu adanya aturan terbaru yang mengatur hal tersebut ditambah lagi perlu adanya penambahan segmentasi besaran kesalahan dan kerugian atau bisa dibilang kualifikasi yang dapat dikenakan terhadap pengendali atau prosesor data pribadi.

Penutup

E-wallet adalah platform digital yang memudahkan transaksi *online* penggunanya, dimana pengguna akan diminta untuk memberikan data pribadinya. Seiring kemajuan teknologi, salah satu kejahatan yang berkembang adalah kebocoran data pengguna *e-wallet* yang digunakan oleh pinjaman *online*. Di Indonesia, perlindungan hukum dan penyelesaian sengketa mengenai data pribadi diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), Peraturan OJK No. 1 tahun 2013, Peraturan OJK No. 13 Tahun 2018, dan Peraturan OJK No. 77 tahun 2016, dan Peraturan Bank Indonesia No. 18 Tahun 2016, sedangkan di Malaysia diatur dalam Undang-Undang Perlindungan Data Pribadi (UU 709 *Personal Data Protection Act* 2010) dan terdapat lembaga Komite Penasihat Perlindungan Data Pribadi, sementara itu, di Singapura diatur dalam *The Personal Data Protection Act* No. 26 of 2012 Singapore dan terdapat lembaga Personal Data Protection Commission.

Terkait kebocoran data pribadi, pengguna *e-wallet* dapat mengajukan gugatan dan menerima ganti rugi dengan dasar gugatan perbuatan melawan hukum yang dilakukan oleh perusahaan *e-wallet*. Pengguna *e-wallet* termasuk konsumen jasa, sehingga berdasarkan konsep *presumption of liability* yang diatur dalam Undang-Undang Perlindungan Konsumen, perusahaan selalu dianggap bertanggung jawab atas perbuatan sampai perusahaan tersebut dapat membuktikan sebaliknya (pembuktian terbalik). Konsep tersebut kurang memberikan keadilan bagi para konsumen karena perusahaan dapat terbebas dari tanggung jawabnya jika mereka membuktikan tidak melakukan kesalahan atau mereka telah melakukan kelalaian tetapi sudah berusaha sebisa mungkin mengatasinya atau karena keadaan *force majeure*. Berdasarkan konsep *strict liability*, dimana perusahaan dianggap selalu bertanggung jawab tanpa melihat perbuatan dilakukan karena kesalahan atau tidak melihat siapa yang melakukan kesalahan, dinilai lebih memberikan keadilan, karena pengguna *e-wallet* akan mendapatkan hak ganti ruginya.

Sebaiknya Indonesia dapat membentuk lembaga pengawas terkait perlindungan data pribadi, supaya dapat mencegah kasus-kasus kebocoran data pribadi; dan Sebaiknya lembaga legislatif dapat mengatur lebih rinci mengenai tata cara pengenaan ganti rugi bagi pengguna *e-wallet* yang ingin meminta ganti rugi dari perusahaan *e-wallet* dalam peraturan pelaksana Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

Daftar Pustaka

- Aswandi, R., Putri, M., & Sultan, M. (2020). Perlindungan Data dan Informasi Pribadi Melalui Indon-987sia Data Protrction System (IDPS). *Legislatif*, 3(2), 167-190.\
- Bodhi, S., & Tan, D. (2022). KEAMANAN DATA PRIBADI DALAM SISTEM PEMBAYARAN E-WALLET TERHADAP ANCAMAN PENIPUAN DAN PENGELABUAN (CYBERCRIME). *UNES Law Review*, 4(3), 297-308. <https://doi.org/10.31933/unesrev.v4i3.236>
- BSSN, B. S. dan S. N. (2024). *Lanskap Keamanan Siber Indonesia 2023*.
- Delpiero, M. (2021). Analisis Yuridis Kebijakan Privasi dan Pertanggungjawaban Online

- Marketplace Dalam Perlindungan Data Pribadi Pengguna Pada Kasus Kebocoran Data. *Padjadjaran Law Review*, 9(1), 1–22. <https://doi.org/http://jurnal.fh.unpad.ac.id/index.php/plr/article/view/509>.
- Dr. Suyanto, S. S. (2023). *Mengenal Dompot Digital Di Indonesia*. CV AA Rizky.
- Faizah, A. F., Rosadi, S. D., Pratama, G. G., & Dharmawan, A. F. (2023). *Penguatan Perlindungan Data Pribadi Melalui Otoritas Pengawas Di Indonesia Berdasarkan Perbandingan Hukum Hong Kong Dan Singapura*. *Hakim*, 1(3), 2023, Hal. 14. 1(3), 2023.
- Financial Technology Regulation in Malaysia and Indonesia: A Comparative Study, 3 Ihtifaz: Journal of Islamic Economics, Finance, and Banking, 74 (2020).
- Inggiharti, N. (2020). Pengaruh Electronic Wallet terhadap Kegiatan Keuangan Indonesia (Perbandingan Aplikasi Electronic Wallet Milik Perusahaan Financial Technology terhadap Aplikasi Electronic Wallet Milik BUMN). *University Of Bengkulu Law Journal*, 5(1), 74–88. <https://doi.org/10.33369/ubelaj.5.1.74-88>
- Marcelliana, V., & dkk. (2023). Penerapan Perlindungan Konsumen Terhadap Nasabah PT. Bank Syariah Indonesia Dalam Kasus Kebocoran Data Nasabah. *Depositi: Jurnal Publikasi Ilmu Hukum*, 1(2), 180–194. <https://journal.widyakarya.ac.id/index.php/Depositi-widyakarya/article/view/577>
- Natha, K. D. R., Budiarta, I. N. P., & Astiti, N. G. K. S. (2022). Perlindungan Hukum Atas Kebocoran Data Pribadi Konsumen Pada Perdagangan Elektronik Lokapasar (Marketplace) (Legal Protection for Leaks of Consumer Personal Data in Marketplace Electronic Commerce). *Jurnal Preferensi Hukum*, 3(1), 143–148.
- Nurhasanah, & Rahmatullah, I. (2020). FINANCIAL TECHNOLOGY AND THE LEGAL PROTECTION OF PERSONAL DATA: The Case of Malaysia and Indonesia. *Al-Risalah: Forum Kajian Hukum Dan Sosial Kemasyarakatan*, 20(2), 197–214. <https://doi.org/10.30631/alrisalah.v20i2.602>
- Pasal 12 Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi.
- Priliasari, E. (2023). PERLINDUNGAN DATA PRIBADI KONSUMEN DALAM TRANSAKSI E-COMMERCE MENURUT PERATURAN PERUNDANG-UNDANGAN DI INDONESIA (Legal Protection of Consumer Personal Data in E- Commerce According To Laws dan Regulations in Indonesia). *Jurnal Rechts Vinding*, 12(2), 61–79. <https://www.ncbi.nlm.nih.gov/books/NBK558907/>
- Priscyllia, F. (2019). Perlindungan Privasi Data Pribadi Perspektif Perbandingan Hukum. *JATISWARA*, 34(3), 239–249. <https://doi.org/10.29303/jtsw.v34i3.218>
- Rizal, M. S. (2019). Perbandingan Perlindungan Data Pribadi Indonesia dan Malaysia. *Jurnal Cakrawala Hukum*, 10(2), 2019. <https://doi.org/10.26905/idjch.v10i2.3349>
- Soemitra, A., & Adlina. (2022). Perlindungan Konsumen Terhadap Kebocoran Data Pada Jasa Keuangan Di Indonesia. *Jurnal Insitusi Politeknik Ganesha Medan Juripol*, 5(1), 288–303.
- Suriaatmadja, G. A. R. dan T. T. (2023). Perlindungan Hukum Atas Kebocoran Data Pribadi Konsumen PT PLN Dihubungkan Dengan Hak Atas Keamanan Pribadi Ditinjau Dari Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi,”. *Bandung Conference Series: Law Studies* 3, 3(1).

<https://www.ncbi.nlm.nih.gov/books/NBK558907/>

Wiranata, A. (2021). Analogi Sistem Perlindungan Hak Atas Data Pribadi Antara Indonesia Dengan Singapura. *Jurnal Ilmiah Mahasiswa Hukum (JIMHUM)*, 1(November), 1-12.

Yuniarti, S. (2022). Petugas/Pejabat Pelindungan Data Pribadi dalam Ekosistem Perlindungan Data Pribadi: Indonesia, Uni Eropa dan Singapura. *Business Economic, Communication, and Social Sciences (BECOSS) Journal*, 4(2), 111-120.
<https://doi.org/10.21512/becossjournal.v4i2.8377>